El Peruano
Signed by: Editora Peru
Date: 13/10/2023 01:58

DIARIO OFICIAL DEL BICENTENARIO

El Peruano

FOUNDED ON OCTOBER 22, 1825 BY THE LIBERATOR SIMÓN BOLÍVAR

"YEAR OF UNITY, PEACE AND DEVELOPMENT".

Friday, October 13, 2023

MINISTRY OF FOREIGN TRADE AND TOURISM

SUPREME DECREE Nº 005-2023-MINCETUR

Regulation of Law No. 31557, which regulates remote gaming and sports betting at a distance.

distance, as amended by Law No. 31806

LEGAL STANDARDS

SUPREME DECREE Nº 005-2023-MINCETUR

SUPREME DECREE APPROVING THE REGULATION OF LAW NO. 31557, LAW REGULATING THE EXPLOITATION OF REMOTE GAMING AND REMOTE SPORTS BETTING

THE PRESIDENT OF THE REPUBLIC CONSIDERING:

Law No. 31557, Law which regulates the exploitation of remote gaming and remote sports betting, modified by Law No. 31806, has the purpose of guaranteeing that the exploitation of remote gaming and remote sports betting is conducted with integrity, honesty, transparency and equal treatment; to protect the vulnerable sectors of the population by means of access controls for minors and the execution of responsible gaming policies aimed at preventing the development of addictive behaviors; and, to prevent the exploitation of remote gaming and remote sports betting from being used for the commission of crimes related to money laundering and financing of terrorism or for the commission of fraud, computer crimes and any other illicit purpose;

That the Second Final Complementary Provision of said Law provides that MINCETUR shall regulate it by means of a Supreme Decree;

Consequently, it is necessary to dictate the Regulation of Law No. 31557, Law that regulates the exploitation of remote gaming and remote sports betting, modified by Law No. 31806, with the purpose of developing its provisions, in order to guarantee that the exploitation of remote gaming and remote sports betting is conducted with integrity, honesty, transparency and equal treatment, as well as to protect the vulnerable sectors of the population through access controls for minors and the execution of responsible gaming policies aimed at preventing the development of addictive behaviors;

Pursuant to numeral 8) of Article 118 of the Political Constitution of Peru; and Law No. 31557, Law that regulates the exploitation of remote gaming and remote sports betting, modified by Law No. 31806;

DECREES:

Article 1. Approval
Approve the Regulation of Law No. 31557, Law that regulates the exploitation of remote gaming and remote sports betting, composed of seven (7) Titles, fifty seven (57) articles, three (3) Transitory Complementary Provisions, three (3) Final Complementary Provisions, two (2) Annexes and the Technical Standards described in the following article.

Article 2. Technical Standards
The Technical Standards that are part of the Regulations approved in the previous article are the following:

- Technical Standards I for Distance Gaming Technology Platforms.
- Technical Standards II for Remote Sports Betting Technology Platforms.
- Technical Standards III for operational auditing of technological platforms.
- Technical Standards IV for economic data that the technological platform must transmit to MINCETUR's Data Center.

Article 3. Financing
The implementation of the actions derived from this Supreme Decree is financed from the institutional budget of the public entities involved, without requiring additional resources from the Public Treasury.

Article 4. Publication
This Supreme Decree and the Regulations approved in Article 1 shall be published in the Single Digital Platform of the Peruvian State for Citizen Orientation (www.gob.pe), as well as in the Institutional Web Portal of the Ministry of Commerce and Tourism (www.gob.pe/mincetur), on the same day of its publication in the Official Gazette "El Peruano".

Article 5.- Endorsement
This Supreme Decree is countersigned by the Minister of Foreign Trade and Tourism.

Given at the Government House, in Lima, on the tenth day of the month of October of the year two thousand and twenty-three.

DINA ERCILIA BOLUARTE ZEGARRA
President of the Republic

JUAN CARLOS MATHEWS SALAZAR
Minister of Foreign Trade and Tourism

REGULATION OF LAW NO. 31557, LAW REGULATING THE EXPLOITATION OF REMOTE GAMING AND REMOTE SPORTS BETTING

TITLE I GENERAL

PROVISIONS

Article 1.- Abbreviations and Definitions

For the purposes of these Regulations, the following definitions shall apply:

1.1 Balance adjustment: Manual correction made by the Account Holder in the gaming account on deposits made by the player or prizes won.

1.2 Algorithm: A finite set of unambiguous instructions performed in a defined sequence to achieve a goal, especially a mathematical rule or procedure used in the calculation of a desired result.

1.3 Hash Algorithm: A function that converts a sequence of data resulting in an alphanumeric sequence of fixed length and is a variant of the SHA-1 algorithm.

1.4 SHA-1 Algorithm: Variant of the Hash algorithm authorized ex officio by MINCETUR for verification of the control program or other components, software, applications, database model.

1.5 Remote sports betting: Remote game, characterized by its randomness, which takes place on Technological Platforms in which bets are placed on the outcome of a sporting event or on any other fact or circumstance that may occur in such sporting event. Only those sporting events that are part of a national or international sporting association, federation or league duly accredited and authorized in the country where it takes place are subject to betting. Also qualifying as remote sports betting are those activities related to electronic sports (e-sports), such as fantasy sports and virtual sports.

1.6 Mystery Attraction: Attraction that may or may not appear during the development of a game and whose result is not associated to a specific paytable combination, and must comply with the approved Technical Standards I. It is also called "Mystery Prize". It is also called "Mystery Prize". When the mystery attraction awards a prize, it is redeemable in cash at the end of the game.

1.7 Authentication: Verification of the identity of a user, process, software package or device, as a requirement to allow access to the resources of the Technology Platform.

1.8 Education Center: Establishment in which regular basic education is provided, in accordance with the authorization granted by the Ministry of Education.

1.9 Service fee: Amount of money charged by the Holder for administering a tournament/competition or game where two or more players compete to win a prize.

1.10 Access Control: Process to grant or deny a specific request to obtain and use confidential information and associated system services; and, to physically enter the critical infrastructure of the data center and its communication network.

1.11 Bonus credits: These are credits granted by the Registrant to the player as part of a commercial promotion (promotional bonus), as referred to in paragraph 16.2 of Article 16 of the Law. These may welcome bonuses or similar (such as birthday bonus, anniversary bonus, bonus for the launch of a new game mode, among others). Bonus credits are restricted, since they are not allowed to be exchanged for cash until a condition set by the Cardholder is fulfilled.

1.12 Gaming Account: Account in which the player's information related to his financial transactions is recorded, such as deposits and withdrawals; bets, games, prizes and balance adjustments; bonuses and refunds; and other events or occurrences that are contemplated in the approved Technical Standards. This information is registered online in the Technological Platform.

1.13 User Account: Account in which the player's identification data is registered. This information is registered online in the Technological Platform.

1.14 Odds: Value that establishes the potential payout of a bet and its conditions for a bet to be a winner or loser.

1.15 Fantasy sport: An e-sports-like activity where players create their own virtual sports team, made up of real players from a specific sport (soccer, basketball, among others) in which teams compete based on their performance statistics in real matches.

1.16 Electronic sports: Also called e-sports, these are tournaments and competitions between video game players. Generally, e-sports are multiplayer video game competitions, particularly between professional gamers. Such as: League of Legends, Counter Strike, Overwatch, Dota, among others.

1.17 Virtual sport: An activity related to e-sports in which sporting events, competitions and horse races are simulated, the results of which are determined solely by a random number generator (RNG).

1.18 Overflow: A pool containing contributions that exceed the progressive jackpot or the incremental progressive jackpot limit.

1.19 DGJCMT: General Directorate of Casino Games and Slot Machines under the Vice Ministry of Tourism of MINCETUR is the administrative authority in charge, at national level, of regulating, authorizing, revoking, supervising and sanctioning the operation of remote gaming and remote sports betting.

1.20 Identity document: National Identity Card (DNI), in the case of Peruvian citizens, Foreigner's Identity Card, in the case of foreign citizens residing in Peru or Passport, in the case of foreign citizens not residing in Peru.

1.21 Live Gaming Environment: Physical location or studio that uses real-time video transmission technology to provide live casino gaming modalities to a gaming environment of the Technology Platform, which allows the player to participate in the game, interact with the game attendants and other players. The modalities of live casino games are those authorized and registered by MINCETUR. The casino gaming rooms authorized by MINCETUR, under Law No. 27153, can have live gaming environment environments, and must comply with the requirements set forth in these Regulations.

1.22 Guarantee: Bank Deposit, Bank Guarantee Letter or Surety Policy referred to in Article 22 of the Law.

1.23 Guarantee of the Certification Laboratories: Bank Deposit, Bank Guarantee Letter or Surety Policy referred to in article 23 of the Law.

1.24 Random Number Generator (RNG): A physical or computational device, algorithm, or system designed to produce numbers indistinguishably from a random selection.

1.25 Player Interface: Application or computer program through which the user visualizes or interacts with the player's software to communicate his actions to the Technology Platform.

1.26 Skill Play: A form of distance play that includes a skill component that allows the player to have a likely influence on the outcome of the game, within a continuous period of play.

1.27 Fantasy sports gambling: A form of remote sports betting in which participants form imaginary or virtual teams with respect to real players (athletes and/or sportsman) of a professional sport.

1.28 Persistence Game: A distance game modality associated with a single attribute and incorporates a feature that allows progress toward awarding game improvements and/or bonuses by achieving designated game outcome.

1.29 Live **Gaming:** Remote gaming modality that corresponds to a remote casino game conducted in a live gaming environment by a gaming assistant (dealer, croupier, etc.) and/or other gaming equipment (automatic roulette wheel, bowling alley, gaming media, etc.), in which players have the ability to review and communicate game decisions through the Technology Platform.

1.30 Law: Law No. 31557, Law that regulates the exploitation of remote gaming and remote sports betting, as amended by Law No. 31806.

1.31 General Corporations Law: Approved through Law No. 26887.

1.32 Radio and Television Law: Approved by Law No. 28278.

1.33 Law for the Prevention and Treatment of Gambling Addiction in Casino Gaming Rooms and Slot Machines: Approved by Law No. 29907.

1.34 LPAG: Law No. 27444, Law of General Administrative Procedure, whose Sole Ordered Text has been approved by Supreme Decree No. 004-2019-JUS.

1.35 Gaming media: Electronic device that allows the execution or formalization of bets placed directly by the player on the Technological Platform for remote gaming and/or remote sports betting. There are two types of gaming media: Those that do not require authorization and registration (homologation) such as personal computer, laptop, cell phone, tablet, and those that do require authorization and registration (homologation) such as sports betting terminals. The gaming media used in a remote sports betting gaming room must only allow remote sports betting.

1.36 Market: Different alternatives or options for betting on a given sporting event.

1.37 MINCETUR: Ministry of Foreign Trade and Tourism.

1.38 NIT: Tax Identification Number.

1.39 Occurrence: Any casual occurrence, fact, undesired or unexpected event, which appears during the development of the game, which will always be recorded in the game account, in accordance with the approved Technical Standards.

1.40 Jackpot: Accumulated progressive jackpot deposit or incremental progressive jackpot monetary contribution.

1.41 Bonus prize: These are credits obtained by the player(s) as a prize after participating in any of the attractions that are part of or associated with a gaming program, as referred to in Article 16.1, paragraph 16.1 of the Law. Bonus prizes include those obtained in the modalities of community bonus, double/risk bonus, among others.

1.42 Jackpot: Maximum prize awarded in a game modality or progressive jackpot or incremental progressive jackpot.

1.43 Progressive Jackpot: Progressive system prize that increases according to the credits wagered in the game.

1.44 Incremental Progressive Jackpot: A progressive system prize that increases in accordance with one or more specific conditions established by the game rules, as well as with the credits wagered in the game.

1.45 Integration Authorization Procedure: Administrative procedure through which MINCETUR authorizes the interconnection between the Technological Platform and the services offered by the related service providers. The Holder must previously accredit, by means of a Certificate of Compliance granted by an authorized Certification Laboratory, that such integration meets the conditions set forth in the approved Technical Standards.

1.46 Control program: Software that controls behaviors in relation to any applicable technical standard and/or regulatory requirement.

1.47 Game Program: Sequence of instructions, developed and written to perform a specific task (generation of games based on chance), which is executed on a Technological Platform and must guarantee the players, on the basis of chance and probabilities, a theoretical return percentage of no less than eighty-five percent (85%).

1.48 Regulations: Regulations of the Law.

1.49 National Traffic Regulation: Sole Ordered Text approved by Supreme Decree Nº 016-2009- MTC.

1.50 SBS: Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (Superintendency of Banking, Insurance and Private Pension Fund Administrators).

1.51 Remote Sports Betting Gaming Room: Physical establishment in which, exclusively or as an additional activity to the sale of other products or services, Technological Platforms for remote sports betting are operated. It may be installed in casino gaming rooms and/or slot machines authorized by MINCETUR.

1.52 Video system: Closed-circuit video system with the specifications detailed in these Regulations and mandatory Directives.

1.53 Multi-game progressive system: Modality of progressive system that links multiple games within the same Technological Platform. The progressive system must comply with the approved Technical Standards.

1.54 Multi-site progressive system: Modality of progressive system that interconnects multiple Technological Platforms. The progressive system must comply with the approved Technical Standards.

1.55 Stand-alone progressive system: Modality of stand alone progressive system, that is to say, it is not linked to any other game. The progressive system must comply with the approved Technical Standards.

1.56 Branch: Secondary establishment through which a company carries out, in a place other than its domicile, certain activities included in its corporate purpose, pursuant to Article 396 of the General Corporations Law.

1.57 SUNARP: National Superintendence of Public Registries.

1.58 SUNAT: National Superintendence of Customs and Tax Administration.

1.59 Temple: Physical space of worship specially conditioned where the free entrance of persons is allowed with the purpose of celebrating rites of religious character including the Catholic Church, and others, whose confession must be registered in the Registry of Religious Entities of the Ministry of Justice and Human Rights.

1.60 Holder: Legal entity authorized by MINCETUR to operate a Technological Platform for remote gaming or remote sports betting.

1.61 Technological Platform Holder: Legal entity recognized by MINCETUR as the manufacturer of the authorized and registered (approved) remote gaming and/or remote sports betting Technological Platform.

1.62 TUPA: Sole Text of Administrative Procedures of MINCETUR.

Article 2.- Functions of MINCETUR

2.1 MINCETUR exercises the administrative powers of regulation, authorization, revocation, supervision and sanction with respect to the operation of remote gaming and remote sports betting provided for in the Law, through the DGJCMT.

2.2 MINCETUR keeps updated in the institutional Web Portal the authorizations in force for the operation of Technological Platforms for remote gaming or remote sports betting, the authorizations of remote sports betting gaming rooms and the records related to the authorization and registration (homologation).

2.3 The Vice-Ministry of Tourism of MINCETUR, resolves in second and final administrative instance the procedures of authorization, sanction and complaints, related to the exploitation of remote gaming and remote sports betting.

Article 3.- Jurisdiction of the Municipalities

MINCETUR will publish the exploitation authorizations granted to the Holders in the institutional web portal.

Municipalities grant operating licenses to operate remote sports betting gaming rooms only to legal entities that have authorization issued by MINCETUR for the operation of a remote sports betting technology platform, under the responsibility of the competent officials.

Municipalities may extend the main line of business of the municipal operating license, in the case of establishments that operate remote sports betting gaming rooms as an additional activity to the sale of other products or services, as long as the authorization issued by MINCETUR to the Licensee is accredited.

Article 4.- Holders of the Authorizations for the Exploitation of Technological Platforms

In accordance with the provisions of the Law, the Holders are:

4.1 Legal entities incorporated in Peru.

4.2 Branches established in Peru of legal entities incorporated abroad.

4.3 Legal entities incorporated abroad.

Article 5.- Voluntary Exclusion of Persons Prohibited from Participating in Remote Games and/or Remote Sports Betting

5.1 In accordance with numeral 28.5 of article 28 of the Law, persons registered in the Registry of Persons Prohibited from Accessing Establishments for the Operation of Casino Games and Slot Machines, in charge of the DGJCMT created under Law No. 29907, cannot participate in the Technological Platforms of remote games and/or remote sports betting.

5.2 In order to comply with the obligation contained in the preceding paragraph, the Holders are responsible for accessing the information contained in the Register, as well as for guaranteeing the confidentiality of the identity of the person registered pursuant to the provisions of Law No. 29733, Personal Data Protection Law and its Regulations.

5.3 MINCETUR makes available to the Registrants the information of the Registry of Persons Prohibited from Accessing Establishments for the Operation of Casino Games and Slot Machines.

5.4 The Holders must include in the main page of the Technological Platforms of remote gaming and/or remote sports betting a link to the MINCETUR Web Portal for registration in the Register of Persons Prohibited from Accessing Establishments for the Operation of Casino Games and Slot Machines.

TITLE II

AUTHORIZATIONS FOR THE OPERATION OF REMOTE GAMBLING AND REMOTE SPORTS BETTING

CHAPTER I
AUTHORIZATION FOR THE OPERATION OF TECHNOLOGY PLATFORMS

Article 6.- Requirements for the Authorization to Operate Technological Platforms to branches established in Peru of legal entities incorporated abroad.

In order to grant the authorization to operate Technological Platforms for remote gaming or remote sports betting, the branches established in Peru of legal entities incorporated abroad submit an application to MINCETUR, attaching the following information and/or documentation:

a) Application Form

b) RUC number, registry entry number, registry entry and the registry zone in which the branch office is registered, issued by the Public Registries.

c) Document signed by the legal representative, indicating the registration number, registry entry, as well as the registry area where the representation is located, according to Public Records.

d) Affidavit signed by the legal representative, containing the list of service providers linked to the Technological Platform of remote gaming and/or remote sports betting, with their respective registration codes granted by MINCETUR and the description of the service(s) rendered.

e) Affidavit signed by the legal representative with powers registered in the Public Registry stating that the partners, directors, managers and representatives with registered powers, as applicable, are not subject, in Peru or in their country of origin, to the impediments established in Article 11 of these Regulations.

f) Identification of the registration code granted by MINCETUR to the Technological Platform to be exploited.

g) Detailed list, as applicable, of:

1. Game programs with the manufacturer's name, identification code and registration code issued by MINCETUR.

2. Progressive systems with the manufacturer's name, identification code and registration code issued by MINCETUR.

3. The modalities of live casino games with the commercial name and registration code granted by MINCETUR.

4. The game modalities with the commercial name and registration code granted by MINCETUR.

5. The models of sports betting terminals with the name of the manufacturer, identification code and registration code granted by MINCETUR that they intend to operate.

h) List of partners, managers, directors and representatives with powers registered in the Public Registry or equivalent document in the country of origin, as of the date of filing the application. In the case of partners, the information refers to shareholders holding shares whose participation in the capital of the legal entity is equal to or greater than 10% (ten percent), as recorded in the share registration book or equivalent instrument in the country of origin. Likewise, in the case of the aforementioned persons, they must submit the following:

1. Detailed and valued list of your assets.
2. Bank reference letter.
3. Report of compliance with its obligations issued by a credit bureau or equivalent instrument in its country of origin.

i) Description of the change management processes detailing the evaluation procedures to identify the criticality of updates to the Technology Platform, for which they must comply with the approved Technical Standards III.

j) Copy of Financial Statements prepared with closing date as of the month prior to the date of submission of the application and the Financial Statements of the last two (02) fiscal years, or the equivalent instrument in the country of origin. The Financial Statements must be signed by the permanent legal representative in Peru and by a certified public accountant or whoever takes his/her place, according to the regulations in force in the country of origin.

k) In case the legal entity is newly incorporated or has not had commercial operations in the last two (02) fiscal years, it must submit, in addition to the Financial Statements prepared with closing date as of the month prior to the date of submission of the application, a copy of a pre-feasibility study containing the projected financial statements for the three (03) fiscal years subsequent to the date of submission of the application, signed by the permanent legal representative in Peru and by a certified public accountant or whoever takes his place, in accordance with the regulations in force in the country of origin.

l) Copy of the share registration book or equivalent instrument in the country of origin.

m) Copy of the proof of payment of the processing fee, according to TUPA.

The documentation must be submitted duly translated into Spanish with the indication and signature of the translator, in accordance with the provisions of Article 49.1.2 of Article 49 of the LPAG, if applicable.

MINCETUR grants a unique registration to the Holder.

Article 7.- Requirements for the Authorization to Operate Technological Platforms for Legal Entities incorporated abroad that do not have a branch in Peru

In order to grant the authorization to operate Technological Platforms for remote gaming or remote sports betting of legal entities incorporated abroad that do not have a branch in Peru, they must submit an application to MINCETUR, attaching the following information and/or documentation:

a) Application form.

b) Document signed by the legal representative, indicating the NIT of the country of origin of the applicant legal entity.

c) Document signed by the legal representative, indicating the number of the registry entry and the registry entry where the representation is registered, as well as the registry area where the representation is registered, according to the Public Records.

d) Affidavit signed by the legal representative, containing the list of service providers linked to the Technological Platform for remote gaming and/or remote sports betting, their respective registration codes granted by MINCETUR and the description of the service(s) rendered.

e) Affidavit signed by the legal representative with powers registered in the Public Registry stating that the partners, directors, managers and representatives with registered powers are not subject, in Peru or in their country of origin, to the impediments established in Article 11 of these Regulations.

f) Identification of the registration code granted by MINCETUR to the Technological Platform to be exploited.

g) Detailed list, as applicable, of:

1. Game programs with the manufacturer's name, identification code and registration code issued by MINCETUR.

2. Progressive systems with the manufacturer's name, identification code and registration code issued by MINCETUR.

3. The modalities of live casino games with the commercial name and registration code granted by MINCETUR.

4. The game modalities with the commercial name and registration code granted by MINCETUR.

5. The models of sports betting terminals with the name of the manufacturer, identification code and registration code granted by MINCETUR that they intend to operate.

h) Description of the change management processes detailing the evaluation procedures to identify the criticality of updates to the Technology Platform, for which it must comply with the approved Technical Standards III.

i) List of partners, managers, directors and representatives with powers registered in the Public Registry or equivalent document in the country of origin, as of the date of filing the application. In the case of partners, the information refers to shareholders owning shares whose participation in the capital of the legal entity is equal to or greater than 10% (ten percent). Likewise, in the case of the aforementioned persons, the following must be submitted:

1. Detailed and valued list of your assets.
2. Bank reference letter.
3. Report of compliance with its obligations issued by a credit bureau or equivalent instrument in its country of origin.

j) Copy of Financial Statements prepared with closing date as of the month prior to the date of submission of the application and the Financial Statements of the last two (02) fiscal years, or the equivalent instrument in the country of origin. The Financial Statements must be signed by the permanent legal representative in Peru and by a certified public accountant or whoever takes his/her place, according to the regulations in force in the country of origin.

k) In case the legal entity is newly incorporated or has not had commercial operations in the last two (02) fiscal years, it must submit, in addition to the Financial Statements prepared with closing date as of the month prior to the date of submission of the application, a copy of a pre-feasibility study containing the projected financial statements for the three (03) fiscal years subsequent to the date of submission of the application, signed by the permanent legal representative in Peru and by a certified public accountant or whoever takes his place, in accordance with the regulations in force in the country of origin.

l) Copy of the share registration book or equivalent instrument in the country of origin.

m) Copy of the proof of payment of the processing fee, according to TUPA.

The documentation must be submitted duly translated into Spanish with the indication and signature of the translator, in accordance with the provisions of Article 49.1.2 of Article 49 of the LPAG, if applicable.

MINCETUR grants a unique registration to the Holder.

Article 8.- Requirements for the Authorization for the Operation of Technological Platforms to Legal Entities incorporated in Peru

In order to grant the authorization to operate Technological Platforms for remote gaming or remote sports betting, legal entities incorporated in Peru submit an application to MINCETUR, attaching the following information and/or documentation:

a) Application form.

b) Document signed by the legal representative, indicating the RUC number, registry number and registry entry, as well as the registry zone to which the applicant legal entity belongs.

c) Document signed by the legal representative, indicating the number of the registry entry and the registry entry where the representation is registered, as well as the registry zone to which it belongs according to the Public Records.

d) Identity Card Number of each of the partners, directors, managers and attorneys-in-fact with powers of attorney registered in the Registry of Legal Entities of SUNARP.

e) Affidavit signed by the legal representative, containing the list of service providers linked to the Technological Platform for remote gaming and/or remote sports betting, their respective registration codes granted by MINCETUR and the description of the service(s) rendered.

f) Identification of the registration code granted by MINCETUR to the Technological Platform to be exploited.

g) Detailed list, as applicable, of:

1. Game programs with the manufacturer's name, identification code and registration code issued by MINCETUR.
2. Progressive systems with the manufacturer's name, identification code and registration code issued by MINCETUR.
3. The modalities of live casino games with the commercial name and registration code granted by MINCETUR.
4. The game modalities with the commercial name and registration code granted by MINCETUR.
5. The models of sports betting terminals with the name of the manufacturer, identification code and registration code granted by MINCETUR that they intend to operate.

h) List of partners, managers, directors and representatives with powers registered in the Public Registry as of the date of filing the application. In the case of partners, the information refers to shareholders owning shares whose participation in the capital of the legal entity is equal to or greater than 10% (ten percent), and who are registered in the share registration book. Likewise, in the case of the aforementioned persons, they must submit the following:

1. Detailed and valued list of your assets.
2. Bank reference letter.
3. Report of compliance with its obligations issued by a credit bureau or equivalent instrument in its country of origin.

i) Description of the change management processes detailing the evaluation procedures to identify the criticality of updates to the Technology Platform, for which it must comply with the approved Technical Standards III.

j) Copy of Financial Statements prepared with closing date as of the month prior to the date of submission of the application and the Financial Statements of the last two (02) fiscal years. The financial statements must be signed by the legal representative and by a certified public accountant.

k) In case the legal entity is newly incorporated or has not had commercial operations in the last two (02) fiscal years, it must submit, in addition to the Financial Statements prepared with a closing date as of the month prior to the date of submission of the application, a copy of a pre-feasibility study containing the projected financial statements for the three (03) fiscal years following the date of submission of the application, signed by the legal representative and by a certified public accountant.

l) Copy of the share registration book.

m) Affidavit signed by the legal representative, stating that the legal entity incorporated in Peru has not been sanctioned for administrative liability according to Law No. 30424.

n) Affidavit signed by each of the partners, managers, directors and representatives with powers registered in the Public Registry stating that they are not affected by the impediments established in Article 11 of these Regulations.

o) Copy of the proof of payment of the processing fee, according to TUPA.

MINCETUR grants a unique registration to the Holder.

If the Holder has more than one authorization for the operation of remote sports betting gaming rooms, a correlative number is assigned for each remote sports betting gaming room.

Article 9.- Economic and Financial Evaluation for the Authorization to Operate Technology Platforms

For the purpose of the economic-financial evaluation, MINCETUR uses financial indicators of solvency, liquidity and profitability to determine the economic-financial solvency of the applicant legal entity and/or Holder. Said indicators are used in a comparative manner with respect to two (02) or more historical or projected fiscal years.

In the case of the financial solvency indicator, the equity of the legal entity of the applicant and/or Holder must not reflect a negative balance.

Likewise, MINCETUR verifies the economic and financial solvency of the partners, managers, directors and representatives with powers registered in Public Registries of the applicant legal entity and/or Holder, in accordance with the information presented in Articles 6, 7 and 8 of these Regulations, as applicable.

Article 10.- Scope of the Economic and Financial Evaluation

a) MINCETUR verifies the economic solvency of the company.
of the applicant legal entity and/or Holder.

b) MINCETUR verifies the economic and financial solvency of the partners, managers, directors and representatives with powers registered in Public Registries of the applicant legal entity and/or Holder.

c) The economic-financial evaluation is permanent and is carried out during the term of the authorization to operate Technological Platforms for remote gaming or remote sports betting granted by MINCETUR.

d) MINCETUR provides FIU-Peru with access to the reports containing the results of the economic and financial evaluations through a repository. This information is updated on a quarterly basis.

e) MINCETUR makes available to SUNAT, in the manner, term and conditions established by the latter through a superintendence resolution issued after coordination with MINCETUR, the authorizations granted for the operation of technological platforms and the results of the economic-financial evaluations referred to in numeral 7.5 of Article 7 of the Law. Such information made available to SUNAT must be updated.

Article 11.- Evaluation of Background

For the background evaluation referred to in numeral 27.3 of Article 27 of the Law, MINCETUR verifies that the partner, director, manager or legal representative with powers registered in the Registry of Legal Entities of SUNARP is not in the following situations:

a) Is a public official or public officer, in accordance with the provisions of Law No. 30057.

b) Is a public servant or employee of MINCETUR who directly or indirectly participates in the work of authorization, control and sanction of remote gaming or remote sports betting.

c) Is or has been a partner, director, manager or legal representative of a company sanctioned for the unauthorized operation of Technological Platforms for remote gaming or remote sports betting and/or remote gaming rooms and/or remote sports betting.

d) Have pending legal proceedings brought by the State for failure to comply with the Law and these Regulations.

e) Has a final and enforceable judgment against him/her in proceedings brought by the State for failure to comply with the Law and these Regulations.

f) Record protests not raised as of the filing date of the application, in Peru or in your country of origin.

g) It has been restructured or liquidated or declared bankrupt as a result of an Ordinary or Preventive Insolvency Proceeding in Peru or in its country of origin.

h) Has been disqualified for the operation of remote gaming or remote sports betting in Peru or in his country of origin.

i) Has been convicted of drug trafficking, terrorism, crimes against national security, money laundering, financing of terrorism, criminal organization, even if they have been rehabilitated in Peru or in their country of origin.

Responsibility of the Holder for the Exploitation of Technological Platforms

The Licensee is obliged as a precondition for the start of operations of the Platform Technological and/or opening of the remote sports betting room to:

a) To grant the guarantee provided for in Articles 22 and 24 of the Law and to deliver it to MINCETUR, under penalty of incurring in an administrative infraction.

b) Communicate the domain with the extension to be used for the exploitation of the Technological Platform for remote gaming and/or remote sports betting, as the case may be, under penalty of incurring in administrative infringement.

c) Provide MINCETUR with the users and/or passwords to access the servers and database of the Technological Platform for remote gaming and/or authorized remote sports betting.

CHAPTER II
AUTHORIZATION OF LABORATORIES CERTIFICATION

Article 13.- Certification Laboratory Authorization

The certification laboratory must submit an application with the following information and/or documentation:

a) Application form.

b) Document signed by the legal representative, indicating the RUC or NIT number of the country of origin of the applicant legal entity, registration number and registry entry, as well as the registry zone to which it belongs or the equivalent instrument in the country of origin.

c) Document signed by the legal representative, indicating the number of the registry entry and the registry entry where the representation is registered, as well as the registry zone to which it belongs.

d) Document that describes and supports:

1. Technological capacity for the certification, issuance of reports and audits of the Technological Platforms for remote gaming or remote sports betting;
2. The technical means and infrastructure used for the development of its activity; and,
3. Workshops, laboratories and offices.

e) Copy of the documentation accrediting five (05) years of experience in the technical evaluation required for the issuance of reports and/or certifications, such as qualifications or authorizations obtained in other jurisdictions.

f) Affidavit of not having any technical, commercial, financial or any other kind of relationship with the Technological Platform Holders and/or related service providers, except for the commercial relationship generated as a consequence of the service provided for the technical evaluation and certification tasks.

g) List of persons authorized by the Certification Laboratory to sign the Certificates of Compliance.

h) Copy of the proof of payment of the processing fee, according to TUPA.

MINCETUR grants a unique registration to the authorized Certification Laboratory, where the company name or corporate name and the person(s) responsible for signing the Certificates of Compliance are stated.

Changes in the data contained in the Register shall be processed in accordance with the provisions of this article, as applicable.

Article 14.- Obligations of the Authorized Certification Laboratory

The authorized certification laboratory has the following obligations:

a) The authorized Certification Laboratory is obliged to grant the guarantee referred to in articles 23 and 24 of the Law, and deliver to MINCETUR the following documents as a condition precedent to the issuance of a certificate of compliance.

b) It performs the technical evaluations of the Technological Platforms of remote gaming or remote sports betting, gaming programs, progressive systems, main components, related computer services, integration between Technological Platforms, remote gaming servers, betting servers and sports betting terminals, following the approved Technical Standards and the mandatory Directives.

c) It issues certificates of compliance of those Technological Platforms for remote gaming or remote sports betting, gaming programs, progressive systems, main components, related computer services, integration between Technological Platforms, remote gaming servers, betting servers and sports betting terminals, among other computer components that comply with the provisions of the Law, Regulations, Technical Standards of the Regulations and mandatory Directives.

d) Submit summaries of evidence of certifications, reports and audits carried out at the request of MINCETUR.

e) Informs within a term no longer than ten (10) working days about the defects or errors detected in the Technological Platforms of remote gaming or remote sports betting, gaming programs, progressive systems, main components, linked computer services, integration between Technological Platforms, remote gaming servers, betting servers and betting terminals, among other computer components, that were subject to certification and that affect or may affect the results of the technical evaluations or certifications performed.

f) Maintains during the term of the authorization the conditions under which it was granted.

g) Repay the guarantee granted in favor of MINCETUR in case of total or partial execution of the same, within a term not exceeding fifteen (15) working days from the date of its execution.

h) Performs the integration and certification tests of each server and other equipment with the Holder's Technology Platform.

i) Provides, at no cost, upon request of MINCETUR, a copy of the algorithm or adapter used to obtain digital fingerprints (electronic signatures), when it is its property, attaching the manual of operation, operation or use, as well as the information corresponding to any update of the algorithm.

j) Adopts appropriate measures to ensure, at all levels of its organization, the confidentiality of information obtained during the performance of its activities.

k) The Certificate of Compliance issued must contain, at least, the following information: the company name or corporate name of the Technological Platform Holder, the description of the architecture of the Technological Platform, with its different integration services and indication of the functions of its components, security and auditing conditions, as well as the description of the operation of the Technological Platform, indicating in detail the observance of the approved Technical Standards.

l) Performs audits of the Technological Platforms at the request of MINCETUR.

m) Inform MINCETUR of any changes in the data contained in the Register.

n) It complies with the obligations derived from the Law, these Regulations and the mandatory Directives.

CHAPTER III
AUTHORIZATION FOR THE OPERATION OF REMOTE SPORTS BETTING GAMING HALLS

Article 15.- Authorization for the Operation of a Remote Sports Betting Gaming Room

For the authorization of the remote sports betting gaming room, the Holder submits to MINCETUR the following documentation and/or information:

a) Application form.

b) Document signed by the legal representative, indicating the RUC number, registry number and registry entry, as well as the registry zone to which it belongs.

c) Document signed by the legal representative, indicating the number of the registry entry and the registry entry where the representation is registered, as well as the registry zone to which it belongs.

d) Copy of the location plan of the gaming room in a scale of 1/500 subscribed by a civil engineer or architect with current license, with the detail of the location of the property where the gaming room is located.

e) Affidavit of compliance with the minimum distance provided for in Article 29 of the Law.

f) List of the sports betting terminals to be operated in the remote sports betting gaming room, individualized by manufacturer, model, serial number and registration granted by MINCETUR.

g) List of gaming media to be operated in the remote sports betting gaming room indicating the type of device (such as personal computer, laptop, cell phone, tablet).

h) Registration code in the registry granted by MINCETUR to the Technological Platform it intends to exploit.

i) Description of the video system indicating the relationship of the equipment.

j) Copy of the proof of payment of the processing fee, according to TUPA.

In the event that the legal entity constituted in accordance with the General Law of Corporations, in whose commercial establishments the Holder requests the authorization for the operation of remote sports betting is different from the latter, it must submit the document evidencing the contractual relationship between the two.

Modification of the Authorization for the Operation of a Remote Sports Betting Games Room.

For the modification of the authorizations for the operation of remote sports betting gaming rooms, the Holder files an application with MINCETUR, attaching the following documentation and/or information:

a) Application form.

b) Document signed by the legal representative, indicating the number of the registry entry and the registry entry where the representation is registered, as well as the registry zone to which it belongs.

c) List of the betting terminals that are increased, withdrawn or replaced in the remote sports betting gaming room and individualized by manufacturer, model, serial number and registration granted by MINCETUR to the betting terminal model.

d) List of gaming media to be operated in the remote sports betting gaming room indicating the type of device (such as personal computer, laptop, cell phone, tablet).

e) Copy of the proof of payment of the processing fee, according to TUPA.

In the case of the modification of the Authorization for the Operation of a Remote Sports Betting Games Room, the licensee must only submit the requirements indicated in paragraphs c) and/or d) as requested.

Article 17.- Measurement of the Minimum Distance in the Remote Sports Betting Gaming Room

17.1 The measurement of the minimum distance referred to in Article 29 of the Law is made following the minimum possible pedestrian traffic, from the entrance or exit of persons from temples or study centers where regular basic education is provided to the entrance or exit of persons from sports betting gaming halls.

17.2 The determination of the minimum distance is made from corner to corner, prioritizing the signaling of crosswalks and the applicable rules set forth in the National Traffic Regulations.

17.3 The determination of the minimum distance following a minimum pedestrian traffic that is not identified with the pedestrian traffic that follows in natural conditions or situations is not allowed.

17.4 The determination of the minimum distance should not include the atrium of the temples.

17.5 The temples must belong to the Catholic Church or to denominations registered in the Registry of Religious Entities of the Ministry of Justice and Human Rights.

17.6 Education centers must have the authorization granted by the Ministry of Education, as well as the corresponding municipal operating license.

17.7 The temples or education centers installed after the authorization granted by MINCETUR are not opposable in the procedures for the renewal of the authorization to operate sports betting gaming rooms.

In the event of a discrepancy between the measurement declared by the holder of the requesting Technological Platform and the one determined by the Administration, MINCETUR initiates the actions leading to the initiation of the corresponding administrative sanctioning procedure.

Article 18.- Video System in the Remote Sports Betting Gaming Room

18.1 The remote sports betting gaming room must have a digital video system or similar technology that allows uninterrupted and real time recording with a minimum of thirty (30) frames per second and one (1) CIF of all the areas that make up the gaming room, as well as of the areas where people enter and exit, and the recordings must show the date, time and name of the gaming room.

18.2 In the areas where betting transactions and the payment of money balances available in the gaming account are made, the digital video system or similar in technology of the remote sports betting gaming rooms must allow uninterrupted and real time recording with a minimum of thirty (30) frames per second and one (01) CIF.

18.3 The recording and/or storage equipment that make up the video systems are installed in a secure place with restricted access to the public, inside or outside the establishment where the remote sports betting gaming room operates.

18.4 The recordings of the aforementioned systems are kept for a period of fifteen (15) calendar days and are presented upon request of MINCETUR.

18.5 The sports betting gaming room has an environment that complies with the corresponding security measures for the installation of the video system. The video recording and/or storage equipment may operate in a centralized manner, with respect to one or more gaming rooms of the same Holder; or, they may be installed in other properties or environments that are not part of the gaming room.

Article 19.- Hours of Operation of the Remote Sports Betting Gaming Room

The hours of operation of the remote sports betting gaming room may be from twenty-four hours a day to twenty-four hours a day.
(24) hours.

The Holder observes the zoning, safety, hygiene and parking regulations, among others, established by the Local Governments in their respective jurisdictions for the granting of the corresponding municipal operating license.

Article 20.- Control and Oversight of the Minimum Distance in the Remote Sports Betting Games Room

MINCETUR periodically verifies the compliance of the Holders established in article 29 of the Law, as part of the control and supervision of the operation of remote sports betting gaming halls.

CHAPTER IV
AUTHORIZATION AND REGISTRATION (HOMOLOGATION) OF TECHNOLOGY PLATFORMS

Authorization and Registration (homologation) of Technology Platforms.

For the authorization and registration of Technological Platforms for remote gaming and/or remote sports betting, the Technological Platform Holder submits an application to MINCETUR, attaching the following documentation and/or information:

a) Application form.

b) Document signed by the legal representative, indicating the RUC or NIT number of the country of origin of the applicant legal entity, registration number and registry entry, as well as the registry zone to which it belongs or the equivalent instrument in the country of origin.

c) Document signed by the legal representative, indicating the number of the registry entry and the registry entry where the representation is registered, as well as the registry zone to which it belongs.

d) Current registration code granted by MINCETUR to the applicant as a supplier of Technological Platforms.

e) List of service providers linked to the Technological Platform for remote gaming and/or remote sports betting, with their respective registration codes granted by MINCETUR and the description of the service(s) provided.

f) Identification of the Technology Platform, as well as the version and commercial name.

g) Copy of the certificate of compliance issued by a certification laboratory authorized by MINCETUR, indicating the company name or corporate name of the Technological Platform Holder, the description of the architecture of the Technological Platform, with its different services and indication of the functions of its components, security and auditing conditions, as well as the description of the operation of the Technological Platform, indicating in detail the observance of the approved Technical Standards.

h) Adaptor, device or special interface to be used for the reading of the digital fingerprint (electronic signature), at no cost to MINCETUR and upon request.

i) Copy of the proof of payment of the processing fee, according to TUPA.

MINCETUR grants a unique registry to authorized and registered (approved) Technology Platforms, where the approval code granted as a result of the authorization and registration process is recorded.

Variations in the data contained in the Register of Technology Platforms are processed in accordance with the provisions of Article 35 of these Regulations, as applicable.

Article 22.- Authorization of the Integration with the Technological Platforms.

For the authorization of the integration with the Technological Platforms, the Holder must submit a request to MINCETUR, attaching the following documentation and/or information:

a) Application form.

b) Document signed by the legal representative, indicating the RUC or NIT number of the country of origin of the applicant legal entity, registration number and registry entry, as well as the registry zone to which it belongs or the equivalent instrument in the country of origin.

c) Document signed by the legal representative, indicating the number of the registry entry and the registry entry.

where the representation is located, as well as the registry zone to which it belongs.

d) Registration code granted by MINCETUR to the Technological Platform.

e) Current registration code granted by MINCETUR to the provider of the related services to be integrated into the Technological Platform.

f) Copy of the certificate of compliance issued by a certification laboratory authorized by MINCETUR, detailing the integration between the platforms and their compatibility, among other technical considerations established in these Regulations and mandatory Directives.

g) Copy of the proof of payment of the processing fee, according to TUPA.

CHAPTER V
AUTHORIZATION AND REGISTRATION (HOMOLOGATION) OF GAMING PROGRAMS

Authorization and Registration (homologation) of gaming programs.

For the authorization and registration of gaming programs, the related service provider must submit an application to MINCETUR, attaching the following documentation and/or information:

a) Application form.

b) Document signed by the legal representative, indicating the RUC or NIT number of the country of origin of the applicant legal entity, registration number and registry entry, as well as the registry zone to which it belongs or the equivalent instrument in the country of origin.

c) Document signed by the legal representative, indicating the number of the registry entry and the registry entry where the representation is registered, as well as the registry zone to which it belongs.

d) Identification of gaming programs by identification code and trade name.

e) Indication of the minimum and maximum theoretical percentage of return to the public of each gaming program for each type or modality of gaming.

f) Current registration code granted by MINCETUR to the applicant as a supplier of related services subject to homologation.

g) Copy of the certificate of compliance issued by a certification laboratory authorized by MINCETUR, indicating in detail the observance of the approved Technical Standards.

h) Copy of the proof of payment of the processing fee, according to TUPA.

Processing fees are payable for every fifty (50) game programs.

MINCETUR grants a single registry of authorized and registered (homologated) gaming programs, where the homologation code granted as a result of the authorization and registration process is recorded.

Variations in the data contained in the Register of authorized and registered (approved) gaming programs are processed in accordance with Article 35 of these Regulations, as applicable.

CHAPTER VI
AUTHORIZATION AND REGISTRATION (HOMOLOGATION) OF PROGRESSIVE SYSTEMS

Article 24.- Authorization and Registration (homologation) of progressive systems

For the authorization and registration of progressive systems, the related service provider must submit an application to MINCETUR, attaching the following documentation and/or information:

a) Application form.

b) Document signed by the legal representative, indicating the RUC or NIT number of the applicant legal entity's country of origin, registration number and registry entry, as well as the registry area to which the applicant legal entity belongs or of the equivalent instrument in the country of origin.

c) Document signed by the legal representative, indicating the number of the registry entry and the registry entry where the representation is recorded, as well as the registry zone to which it belongs.

d) Identification of the progressive system and trade name.

e) Copy of the operating manual of the progressive system.

f) Copy of the certificate of compliance issued by a certification laboratory authorized by MINCETUR, indicating in detail the observance of the approved Technical Standards.

g) Current registration code granted by MINCETUR to the applicant as a supplier of related services subject to homologation.

h) Copy of the proof of payment of the processing fee, according to TUPA.

The processing fee is paid for each progressive system whose authorization and registration is requested.

MINCETUR grants a unique registry to authorized and registered (homologated) progressive systems, where the homologation code granted as a result of the authorization and registration process is recorded.

Variations in the data contained in the Register of authorized and registered (approved) progressive systems are processed in accordance with the provisions of Article 35 of this Regulation, as applicable.

CHAPTER VII
AUTHORIZATION AND REGISTRATION (HOMOLOGATION) OF GAMING MODALITIES

Authorization and Registration (homologation) of gaming modalities.

For the authorization and registration (homologation) of gaming modalities, except for live casino games, the related service provider must submit an application to MINCETUR, attaching the following documentation and/or information:

a) Application form.

b) Document signed by the legal representative, indicating the RUC or NIT number of the country of origin of the applicant legal entity, registration number and registry entry, as well as the registry zone to which it belongs or the equivalent instrument in the country of origin.

c) Document signed by the legal representative, indicating the number of the registry entry and the registry entry where the representation is registered, as well as the registry zone to which it belongs.

d) Identification of the game modality and commercial name.

e) Current registration code granted by MINCETUR to the applicant as a supplier of related services subject to homologation.

f) Details of the services provided for the Technology Platform by each related service provider.

g) Indication of the minimum and maximum theoretical percentage of return to the public of the type of game, if applicable.

h) Copy of the document including the electronic fingerprints of the game modality and the procedure to be followed to obtain them.

i) Description of the game modality, as well as description of the rules of the game modality.

j) Copy of the certificate of compliance issued by a certification laboratory authorized by MINCETUR, indicating in detail the observance of the approved Technical Standards.

k) Copy of the proof of payment of the processing fee, according to TUPA.

MINCETUR grants a single registry to authorized and registered (approved) gaming modalities, in which the approval code granted as a result of the authorization and registration process.

Variations in the data contained in the Register of authorized and registered (approved) gaming modalities are processed in accordance with Article 35 of these Regulations, as applicable.

CHAPTER VIII
AUTHORIZATION AND REGISTRATION (HOMOLOGATION) OF LIVE CASINO GAMES

Authorization and Registration (homologation) of the modalities of live casino games.

For the authorization and registration of live casino games conducted online that are part of remote gaming platforms, the linked service provider must attach the following documentation and/or information:

a) Application form.

b) Document signed by the legal representative, indicating the RUC or NIT number of the country of origin of the applicant legal entity, registration number and registry entry, as well as the registry zone to which it belongs or the equivalent instrument in the country of origin.

c) Document signed by the legal representative, indicating the number of the registry entry and the registry entry where the representation is registered, as well as the registry zone to which it belongs.

d) Description of the characteristics of the game, including the materials to be used.

e) Copy of the Study on the percentage of return to the public.

f) Current registration code granted by MINCETUR to the applicant as a supplier of related services subject to homologation.

g) Affidavit indicating the name of the game modality, the characteristics of the game materials to be used, as well as the game regulations and the permitted betting modalities.

h) Copy of the proof of payment of the processing fee, according to TUPA.

MINCETUR grants a unique registry to the modalities of live casino games (homologated), where the homologation code granted as a result of the authorization and registration process is stated.

The variations of the data contained in the Register of modalities of live casino games are processed in accordance with the provisions of Article 35 of these Regulations, as applicable.

CHAPTER IX
AUTHORIZATION AND REGISTRATION (HOMOLOGATION) OF SPORTS BETTING TERMINAL MODELS

Authorization and registration (homologation) of sports betting terminal models.

For the authorization and registration of sports betting terminal models, the related service provider must submit an application to MINCETUR, attaching the following documentation and/or information:

a) Application form.

b) Document signed by the legal representative, indicating the RUC or NIT number of the country of origin of the applicant legal entity, registration number and registry entry, as well as the registry zone to which it belongs or the equivalent instrument in the country of origin.

c) Document signed by the legal representative, indicating the number of the registry entry and the registry entry where the representation is registered, as well as the registry zone to which it belongs.

d) Current registration code granted by MINCETUR to the applicant as a supplier of related services subject to homologation.

e) Technical description of the hardware and software used, clear photographs of the front, profile, as well as the internal part of the sports betting terminal.

f) Technology Platform Identification (version and commercial name)

g) Copy of the technical operating manual of the sports betting terminal, including a complete and detailed description of all the functionalities of the sports betting terminal.

h) Copy of the certificate of compliance issued by a certification laboratory authorized by MINCETUR, indicating in detail the observance of the approved Technical Standards.

i) Copy of the proof of payment of the processing fee, according to TUPA.

MINCETUR grants a unique registry to authorized and registered (homologated) models of sports betting terminals, where the homologation code granted as a result of the authorization and registration process is recorded.

Changes to the data contained in the Register of authorized and registered (approved) sports betting terminal models are processed in accordance with Article 35 of these Regulations, as applicable.

CHAPTER X
OF THE REGISTRY OF AUTHORIZED SPORTS BETTING TERMINALS

Article 28.- Registration of Sports Betting Terminals

For the registration of sports betting terminals, the related service provider must submit an application to MINCETUR, attaching the following documentation and/or information:

a) Application form.

b) Document signed by the legal representative, indicating the RUC or NIT number of the country of origin of the applicant legal entity, registration number and registry entry, as well as the registry zone to which it belongs or the equivalent instrument in the country of origin.

c) Document signed by the legal representative, indicating the number of the registry entry and the registry entry where the representation is registered, as well as the registry zone to which it belongs.

d) Current registration code granted by MINCETUR to the related service provider.

e) Copy of proof of payment, commercial invoice or import policy evidencing the right of ownership of the sports betting terminals.

f) For each sports betting terminal, the terminal's model code, serial number, date of manufacture and manufacturer's name must be submitted.

g) Copy of the proof of payment of the processing fee, according to TUPA.

MINCETUR grants a unique registration to each sports betting terminal, where the terminal's model code, serial number, date of manufacture, manufacturer's name and owner's name, if applicable, are recorded.

Changes in the data contained in the Register shall be processed in accordance with the provisions of this article, as applicable.

CHAPTER XI
OF THE REGISTRY OF RELATED SERVICE PROVIDERS

Article 29.- Entry in the Registry

MINCETUR keeps a Registry of service providers linked to the Technological Platforms.

In order to access this registry, legal entities must submit the following documentation and/or information, as appropriate:

a) Application form.

b) Document signed by the legal representative, indicating the RUC or NIT number of the country of origin of the applicant legal entity, registration number and registry entry, as well as the registry zone to which it belongs or the equivalent instrument in the country of origin.

c) Document signed by the legal representative, indicating the number of the registry entry and the registry entry where the representation is registered, as well as the registry zone to which it belongs.

d) Description of the technological services provided, such as technological platform provider, quota provider, game provider, GNA provider, among others.

e) Copy of the proof of payment of the processing fee, according to TUPA.

Changes in the data contained in the Register shall be processed in accordance with the provisions of this article, as applicable.

Article 30.- Obligations of the Service Provider of Services Linked to the Technological Platforms

The related service provider is obligated to:

a) Register in the Registry of Service Providers linked to the Technological Platforms.

b) Request MINCETUR for the authorization and registration (homologation) of the services linked to the Technological Platforms provided for in these Regulations.

c) Only provide services to the Holder with authorization from MINCETUR.

Article 31.- Revocation of registration in the Registry of Related Service Providers

MINCETUR revokes the registration in the Registry of Related Service Providers to the supplier that provides services to Technological Platforms that do not have operating authorization.

CHAPTER XII ADMINISTRATIVE PROCEDURES

Article 32.- Granting of authorizations

The admission and evaluation of the applications referred to in the Regulations are subject to the following stages and procedural rules:

a) Receipt of application.

b) Verification of compliance with the economic-financial, technical and legal requirements, as applicable, established in the Law and in these Regulations.

c) The observations determined, after the evaluation of the requirements indicated in paragraph b), are notified by means of an Official Letter.

d) The following constitute prior evaluation procedures with application of the negative administrative silence:

1. Authorization and/or renewal of operation of Technological Platforms for remote gaming and remote sports betting.
2. Authorization and registration (homologation) and/or renewal and/or modification of the Technological Platforms for remote gaming and/or remote sports betting.
3. Authorization and registration (homologation) and/or modification of gaming programs.
4. Authorization and registration (homologation) and/or modification of progressive systems.
5. Authorization and registration (homologation) and/or modification of gaming modalities.
6. Authorization and registration (homologation) and/or modification of modalities of live casino games.
7. Authorization and registration (homologation) and/or modification of sports betting terminal models.

e) The following are automatic approval procedures:

1. Modification of the authorization for the operation of Technological Platforms for remote gaming and remote sports betting.
2. Authorization and/or modification of the authorization to the Certification Laboratories.
3. Authorization and/or modification of the authorization for the operation of remote sports betting gaming rooms.
4. Authorization of the integration with the Technological Platforms.
5. Registration and/or modification in the content of the Registry of sports betting terminals.
6. Registration and/or modification in the content of the Registry of related service providers.

f) The term to resolve the administrative procedures foreseen in paragraph d) of this article is thirty (30) working days.

The administrative acts of authorization granted under the Law and these regulations are published on the institutional website of MINCETUR.

Article 33.- Renewal of authorizations

The renewal of the applications referred to in article 7.3, paragraph 7.3 of the Law and article 8.3 of the Law, is subject to the following stages and procedural rules:

33.1. The renewal of authorizations must be requested two (02) months prior to the expiration date of the authorization to be renewed, attaching the documentation and information provided for in the Law and these Regulations.

33.2. The processing of the renewal application is subject to the operating authorization procedure provided for in the preceding article.

33.3. The term to resolve the renewal requests is thirty (30) working days, with application of the negative administrative silence.

Article 34.- Modification of the Authorization to Operate Technology Platforms

The Holder may request the modification of its exploitation authorization in the following cases:

a) Increase, withdrawal or replacement of gaming programs, submitting a detailed list, as appropriate, of the gaming programs to be increased and/or withdrawn, identified by name of the manufacturer, identification code, registration code granted by MINCETUR and copy of the proof of payment of the processing fee, according to TUPA.

b) Increase, withdrawal or replacement of live casino game modalities, submitting a detailed list, as appropriate, of the live casino game modalities to be increased and/or withdrawn, identified by commercial name, registration code granted by MINCETUR and copy of the proof of payment of the processing fee, according to the TUPA.

c) Increase, withdrawal or replacement of progressive systems, submitting a detailed list, as appropriate, of the progressive systems to be increased and/or withdrawn, identified by manufacturer's name, identification code, registration code granted by MINCETUR and copy of the proof of payment of the processing fee, according to TUPA.

d) Increase, withdrawal or replacement of gaming modalities, submitting a detailed list, as appropriate, of the gaming modalities to be increased and/or withdrawn, identified by commercial name, registration code granted by MINCETUR and a copy of the following documents proof of payment of the processing fee, according to TUPA.

To request a modification of the Authorization to Operate Technological Platforms, the holder must indicate the specific matter to be modified, attaching the documentation and information established in articles 6, 7 and 8 of these Regulations, according to TUPA.

Modification of Authorizations and Registrations (approvals) granted.

The modifications to the authorizations and registrations (approvals) referred to in numeral 8.5 of article 8 of the Law, must necessarily be submitted to a technical evaluation before an authorized Certification Laboratory and, therefore, follow the procedure indicated in articles 21, 23, 24, 25, 26 and 27 of these Regulations, as applicable.

TITLE III

OF THE RECORDS

Article 36.- Registries under the responsibility of MINCETUR

MINCETUR, through the competent body, keeps the following registries:

a) Registration of Holders for the exploitation of Technological Platforms.

b) Registry of authorized and registered (approved) Technology Platforms.

c) Registry of authorized and registered (approved) Gaming Programs.

d) Registry of authorized and registered (approved) live casino games.

e) Registry of authorized and registered (approved) gaming modalities.

f) Registration of authorized and registered (approved) sports betting terminals.

g) Registration of sports betting terminals authorized to be operated in sports betting gaming halls.

h) Register of authorized and registered (approved) progressive systems.

i) Registration of related service providers.

TITLE IV

OBLIGATIONS AND PROHIBITIONS OF THE HOLDERS OF THE AUTHORIZATION FOR THE OPERATION OF REMOTE GAMING OR REMOTE SPORTS BETTING

CHAPTER I OBLIGATIONS OF THE HOLDERS OF THE AUTHORIZATION FOR THE OPERATION OF REMOTE GAMING OR REMOTE SPORTS BETTING

Article 37.- Obligations of the Holder for the operation of Remote Games or Remote Sports Betting

The Holder, without prejudice to the provisions of the Law, must comply with the following:

a) Delivery to MINCETUR of the guarantee provided for in Articles 22 and 24 of the Law, as a condition prior to the start of operations of the operation of the Technological Platform for remote gaming or remote sports betting, as applicable.

b) It registers players in the Technological Platforms of remote games or remote sports betting, by means of an identity document.

c) Verifies the identity, age and nationality of the player as a precondition for placing a wager.

d) It records online, in the gaming account, the deposit of player's money, bets, prize payouts and returns of cancelled bets.

e) Immediately pays the money balances available in the gaming account (deposit of the player's money, prizes and returns of cancelled bets) when requested by the player, to the means of payment chosen by the player. When the payment is made to an account in a financial institution in the player's name, it must be taken into consideration that the time for the execution of the bank transactions cannot exceed three (03) business days after the transaction is made. The payment of refunds of cancelled bets cannot exceed three (03) business days after the bet has been cancelled.

f) It has in a visible place in the remote sports betting gaming room, the authorization registration code granted by MINCETUR, the RUC or NIT as appropriate, as well as the following warning: "Remote sports betting conducted in excess may cause compulsive gambling", according to the measures defined in Annex I of this Regulation.

g) Guarantees that any integration with the servers and other equipment of other related service providers complies with the specifications set forth in these Regulations, their respective approved Technical Standards and in the mandatory Directives.

h) Provides the necessary remote or *on-site* access to MINCETUR for auditing, inspection and control purposes of the Technological Platforms, applications, software, services, databases, critical components, critical control programs, among others.

i) Stores the information of the user account, gaming account and all transactions for a period of five (5) years counted from the granting of the authorization by MINCETUR to the Holder or during the statute of limitations period for the Remote Gaming and Remote Sports Betting Tax as provided in the Tax Code, whichever is greater.

j) It ensures that deposits made by players, as well as prize payments, are recorded online in the gaming account, including the transactions of circulating money made in remote sports betting gaming rooms.

k) Retains for a maximum period of thirty (30) working days the funds from prizes and money balances available in the gaming account that have been obtained with justified suspicions of fraud and/or swindle, so that the Holder can carry out the corresponding investigation. If the fact is formalized in criminal and/or judicial proceedings, the destination of the prize will be subject to the resolution of the respective instances.

l) Void bets when the following events occur:

1. Technical failures in the platform, including errors in the provisioning of linked service providers, databases, infrastructure.
2. Failures in the provision of communication services.
3. Failures in the provision of electric service.
4. Suspension or cancellation or withdrawal of sporting events.
5. Suspension or cancellation or withdrawal from the markets.
6. Agreement on the outcome of sporting events.
7. Quota error.
8. Error in the sporting events or markets offered.

m) Informs MINCETUR of the incorporation of new partners, directors, managers and attorneys-in-fact within a term not to exceed fifteen (15) business days from the date of registration in the share registration book, public registries or the one that serves as such in their country of origin; and submits a sworn statement of not being subject to the impediments established in Article 11 of these Regulations. In the case of partners, the information refers to shareholders owning shares whose participation in the capital of the legal entity is equal to or greater than 10% (ten percent).

n) Submit a sworn statement that the company name or corporate name has not changed. At

If such change has occurred, it must be communicated within ten (10) business days of registration with SUNARP or the equivalent entity in the country of origin.

o) It certifies before MINCETUR, that the Technological Platform of the remote games and/or remote sports betting it exploits, complies with the provisions of numeral 8.3 of article 8 of the Law. The deadline for submitting the information or documentation shall be no less than thirty (30) calendar days prior to the expiration date of the authorization and registration granted to the Technological Platform.

p) Submit to MINCETUR, every two (2) years as from the date of the Operating Authorization granted to the Licensee, a comprehensive audit report of the entire Technological Platform that certifies compliance with the approved Technical Standards and mandatory directives, including the services provided by the related service providers. Said report must be prepared by an authorized Certification Laboratory and submitted no less than two (2) months prior to the compliance date of the two (2) years mentioned above, in accordance with the provisions of numeral 34.2 of article 34 of the Law.

q) Submits to MINCETUR an audit report prepared by an authorized Certification Laboratory, or by an independent area of the Licensee not directly linked to the operation of remote gaming and/or remote sports betting, acting as external auditor. Said report must contain the description of the change management processes detailing the compliance with the approved Technical Standards III, and submitted no later than January twentieth (20) of each year.

r) Provides MINCETUR with the users and/or passwords to access the servers and database within ten (10) working days after the authorization to operate the Technological Platforms for remote gaming and/or remote sports betting has been granted.

s) It is liable to MINCETUR for non-compliance with the obligations arising from the services rendered by its related service providers.

t) Submit to MINCETUR, a report containing the integrity and security evaluation of the Technological Platform prepared by an authorized Certification Laboratory, no later than January twentieth (20) of each year. Said report must be submitted, for the first time, within ninety (90) days after the start of operations.

CHAPTER II PROHIBITIONS OF THE HOLDERS OF THE AUTHORIZATION FOR THE OPERATION OF REMOTE GAMING OR REMOTE SPORTS BETTING

Article 38.- Prohibitions of the Holder for the Operation of Remote Games or Remote Sports Betting

The Holder, without prejudice to the provisions of the Law, is prohibited from:

a) To transfer under any modality, in whole or in part, the authorizations granted by virtue of the provisions of the Law and these Regulations.

b) To allow the player who is not registered in the Technological Platform and whose gaming account is not active to carry out, free of charge, for commercial promotion purposes, remote gaming or remote sports betting, either in any type or modality of betting.

c) To contract the services of related service providers that are not registered or whose registration has expired, been cancelled or revoked by MINCETUR.

d) Perform transactions using cryptocurrencies.

e) Organizing, promoting and/or transmitting distance games involving animal fights and/or races not permitted by the Peruvian State.

f) Grant access to and allow participation in remote gaming and/or remote sports betting to the persons referred to in Article 28 of the Law.

g) To operate in the Technological Platforms, gaming programs, progressive systems, live casino gaming modalities, gaming modalities and betting terminals that are not authorized and registered (approved) by MINCETUR.

h) To operate remote games or remote sports betting expressly prohibited under the Fifth Final Complementary Provision of the Law; as well as those which:

1. Attempt against the right to dignity, honor, privacy, image and non-discrimination, against the right of children and adolescents, and against any right or freedom recognized in the Political Constitution of Peru;
2. Are based on the commission of crimes, misdemeanors or administrative infractions; and,
3. Recaigan on events prohibited by current legislation.

i) Accept advertising from legal entities not authorized and/or registered by MINCETUR in contravention of Article 30 of the Law.

CHAPTER III COMMUNICATIONS AT THE EXPENSE OF THE LICENSEE FOR THE OPERATION OF REMOTE OR REMOTE GAMES REMOTE SPORTS BETTING

Article 39.- Prior communications

The Holder brings to the attention of MINCETUR any of the following facts:

a) Permanent suspension of activities of the Technological Platform or the remote sports betting gaming room, as applicable.

b) Temporary suspension of the activities of the Technological Platform or the remote sports betting gaming room, as applicable, indicating the reasons and the exact duration of the suspension, which, in no case, exceeds ninety (90) calendar days.

c) The implementation of the integration service between the platform of the linked service provider and the Technological Platform of the Holder.

d) The implementation or operation of any update or improvement of the Technological Platform, carried out by the Technological Platform Holder.

e) Change of provider of linked services, indicating the provider's registration code in the Registry of Service Providers Linked to Technological Platforms, granted by MINCETUR (in force) and attaching a copy of the contract signed with the provider.

f) Any other communication in charge of the Holder as established by the Law, these Regulations and mandatory Directives.

Article 40.- Deadline for prior communications The Holder has a term of up to three (03) business days prior to the occurrence of the event in order to make the communication provided for in the preceding article.

TITLE V PROVISIONS RELATED TO THE TECHNOLOGICAL PLATFORMS, AUTHORIZATION OF OPERATION, DEVELOPMENT OF REMOTE GAMING AND REMOTE SPORTS BETTING

CHAPTER I TECHNICAL REQUIREMENTS

Technical requirements of the Technological Platforms for remote gaming and remote sports betting.

The Technology Platforms must comply with the technical requirements described in the approved Technical Standards, as applicable.

Modification of technical requirements of the Technological Platforms of remote gaming and remote sports betting.

MINCETUR may develop and specify the technical requirements described in the approved Technical Standards through mandatory Directives.

Delivery of bonuses in the Technological Platforms of remote gaming or remote sports betting.

The bonuses may be delivered to the player registered in the Technological Platform of remote games or remote sports betting, in accordance with article 16 of the Law, its Regulations and the approved Technical Standards.

Article 44.- Fantasy sports games and other games of skill

Fantasy games, as well as games of skill that may be subject to wagering, are regulated in these Regulations, which may be developed and specified by means of mandatory Directives.

Transmission of technical and economic data.

45.1. Terminal or workstations

The Technology Platform may have more than one terminal or workstation to provide authorized users with access to servers, applications, services, among other components of the Technology Platform.

45.2. Information on the economic data to be transmitted to MINCETUR's Data Center

The Technological Platform must have an automatic mechanism to generate and transmit the information of the consolidated economic data to the MINCETUR Data Center, with a periodicity of at least once (01) a day, with operations closing at 23:59:59 hours of each day, seven (07) days a week, three hundred and sixty-five (365) days a year. For the transmission of such information, the structure established in the approved Technical Standards IV is taken into account.

a) The economic data information is automatically collected by the Remote Gaming and/or Remote Sports Betting Technology Platform maintaining the integrity of the data:

i. Total bets (Soles);
ii. Total prize payments (Soles);
iii. Total bonuses paid (Soles);
iv. Total returns made (Soles);
v. Any other counter necessary for the correct calculation of the daily production obtained by each Technology Platform.
vi. The meters stored in the Technology Platform must be properly labeled, so that they can be clearly identified according to their function.

b) The information of the economic data to be transmitted to MINCETUR's Data Center is in national currency (Soles).

In case the Technology Platform uses a currency other than the national currency (US dollars or other currency), it must use the exchange rate published by the SBS as the average sale rate used for the day of the transaction (consider the exchange rate of the day at the close of operations of the previous day).

For purposes of the foregoing, the publication made by the SBS on its website or in the official newspaper El Peruano is considered.

If the SBS does not publish the weighted average exchange rate for the day of the transaction, the rate corresponding to the last previous day for which the transaction was made must be used. The aforementioned superintendency shall have made the respective publication.

If the SBS does not publish an exchange rate for such foreign currency, it must be converted into U.S. dollars and then expressed in local currency. For the conversion of foreign currency into dollars, the exchange rate used is the buying rate of the country to which the currency used for the transactions corresponds, while for the conversion of dollars into local currency, the provisions of the preceding paragraphs must be applied.

45.3. Information on the technical data to be transmitted to MINCETUR's Data Center

The Technological Platform must have an automatic mechanism to generate and transmit consolidated technical information to the MINCETUR Data Center, with a periodicity of at least once a year.
(01) once a day, with operations closing at 23:59:59 hours of each day, seven (07) days a week, three hundred and sixty-five (365) days a year. For the transmission of such information, the structure established in the approved Technical Standards IV must be taken into account.

The following technical events are transmitted to MINCETUR's Data Center, and data integrity must be maintained:

a) The Technological Platform has critical failures that temporarily stop its operation.
b) Loss of communication between the Technological Platform and the remote sports betting gaming room.

For the recording of economic and technical data and the generation of reports, the Technology Platform must be synchronized with the Peruvian official time GMT-5.

The Holder is obliged to transmit the information on economic and technical data at least once (01) a day, with operations closing at 23:59:59 hours of each day, seven (07) days a week, three hundred and sixty-five (365) days a year, once the authorization to operate Technological Platforms has been obtained from MINCETUR.

On the other hand, in case the Technological Platform does not establish connection with the MINCETUR Data Center, it shall make new connection attempts every five days.
(05) minutes, until the connection is successful.

In case of failure to transmit the economic and/or technical data, the Technology Platform must be reconnected for transmission purposes until a positive acknowledgement of receipt is obtained.

Similarly, data transmission must be performed daily without any possibility of not performing it within the following twenty-four (24) hours. In case such connection is not established, new connection attempts must be made every five (05) minutes, until the connection is successful. The economic and technical data stored in the server of the Technological Platform may not fail to be transmitted to the MINCETUR Data Center three hundred and sixty-five (365) days a year.

TITLE VI

CONTROL, SUPERVISION, PROSECUTION OF ILLEGAL GAMING AND REGIME OF INFRACTIONS AND PENALTIES

CHAPTER I
CONTROL, CONTROL AND PROSECUTION OF ILLEGAL GAMBLING

Article 46.- Scope of the activity of control and prosecution of illegal gambling

MINCETUR exercises its powers to control the exploitation of remote gaming and remote sports betting, as well as to prosecute illegal gaming, in accordance with the provisions of the LPAG. For such purposes:

a) It issues mandatory directives in matters within its competence for the control of remote gaming and remote sports betting;

b) Requires documentation and information to the Holder;

c) Determines the documentation and information that the Holder must keep at its disposal;

d) Requires the recording files of the remote sports betting gaming rooms or live casino games, which must be submitted on magnetic media or other means established by MINCETUR;

e) Conducts inspection visits to remote sports betting gaming halls;

f) Performs remote audits of the Technological Platforms;

g) It forwards information to other agencies or entities in case infringing facts are determined so that they may in turn exercise their corresponding faculties,

h) It carries out any other activity that allows it to supervise the operation of remote gaming and remote sports betting; and to prosecute illegal gaming.

Article 47.- Use of technological means

MINCETUR incorporates in its auditing work the available technological and information technology means or those it has developed and, as the case may be, arranges for their implementation by the Holder.

Article 48.- Audits

MINCETUR carries out planned or unannounced inspections remotely or in person, through the Gaming Supervisors or Inspectors it designates, who record the facts found in an Act or report. Likewise, it can count on the support of the authorized Certification Laboratories, the Peruvian National Police and the Public Prosecutor's Office, as appropriate.

For such purposes, the Registrant must provide MINCETUR with the users and/or passwords to access the servers and database within the required term, as well as grant all the facilities required by the Gaming Supervisors or Inspectors for the exercise of their inspection work.

Article 49.- Destruction of goods

MINCETUR destroys the assets related to the direct exploitation of remote gaming and remote sports betting that it has commissioned or that have been placed at its disposal by various State entities in the following cases:

a) When they do not have an operating authorization

b) When they do not have authorization and registration (homologation).

c) When they do not present the technical characteristics authorized by their manufacturers according to their authorization and registration (homologation).

CHAPTER II
REGIME OF INFRACTIONS AND PENALTIES

Article 50.- Administrative sanctions

The administrative violations provided for in the Law are classified in accordance with Annex II, Table of Violations and Penalties of the Regulations, as follows:

a) Minor infractions: With a warning or a fine of up to fifty (50) UIT.

b) Serious infractions: With a fine greater than fifty (50) UIT and up to one hundred and fifty (150) UIT.

c) Very serious infractions: With a fine greater than one hundred and fifty (150) UIT up to two hundred (200) UIT, cancellation or disqualification, either for up to ten (10) years or permanent.

Article 51.- Mitigating factors and reduction of fines

Once the administrative sanctioning procedure is initiated with the communication of the facts, conducts or omissions that constitute administrative infringement, if the infringer expressly acknowledges his responsibility in writing, until before the issuance of the administrative act. The penalty determined by the sanction, corresponds to a reduction of thirty-five percent (35%) of the applicable fine.

The maximum term to cancel the fine with the applicable reduction is fifteen (15) working days counted from the date of notification of the sanction resolution, otherwise pay one hundred percent (100%) of the fine imposed.

Once the sanction resolution has been notified without the offender having expressly acknowledged his responsibility in writing during the administrative sanctioning procedure in any of its two phases, he is entitled to a reduction of twenty-five percent (25%) of the fine imposed, provided that he does not file the administrative appeals provided for in the LPAG and cancels the fine within the term for filing the appeal.

The reductions of the fine sanction provided for in this article are not cumulative and are not applicable in case of recidivism in the commission of the imputed infraction.

Article 52.- Recidivism

Recidivism is considered to be the aggravating circumstance of liability consisting in the commission of the same infraction by the Holder, within one (01) calendar year after the resolution that sanctioned the first infraction became final.

In the event of repeated commission of violations punishable by fine, double the original sanction imposed is applied, which is increased proportionally to the number of times the violation is committed within one (01) calendar year from the date the resolution that sanctioned the first violation became final.

Recidivism in the commission of the same infraction sanctioned with a reprimand is sanctioned with a fine equivalent to one (01) UIT, which is increased proportionally to the number of times the infraction is committed within one (01) calendar year from the date the resolution sanctioning the first infraction became final.

The DGJCMT determines in the Directorial Resolution imposing the sanction, whether the corrective measures referred to in numeral 36.2 of Article 36 of the Law are applicable.

Article 53.- Phases of the Administrative Sanctioning Proceeding

The sanctioning procedure is always initiated ex officio, either on the Control and Sanction Directorate's own initiative, as a result of a superior order, a reasoned request from other bodies or entities, or a complaint. The procedure for the determination of infractions and application of sanctions is as follows:

53.1 Instructing phase. - The Directorate of Control and Sanction of the DGJCMT constitutes the instructing body of the administrative sanctioning procedure referred to in the Law and these Regulations, for such purposes:

a) Exercises the acts, proceedings, powers and attributions aimed at charging the alleged commission of an administrative infraction.

b) The administrative sanctioning procedure is initiated in accordance with the provisions of the LPAG with the respective charge to the person in charge, who has ten (10) working days from the day following the date of notification of the act that initiates the sanctioning procedure, to present his or her written defense.

c) Evaluates the arguments presented by the person in charge.

d) It carries out the necessary actions for the examination of the facts and collects the data and information that are relevant to determine, if applicable, the existence of liability susceptible to sanction.

e) It formulates the final investigation report in which it determines, in a reasoned manner, the conducts that are considered to constitute an infringement, the rule that provides for the imposition of a sanction; and the proposed sanction or the declaration of non-existence of an infringement, as the case may be.

53.2 Penalty phase. - The DGJCMT is in charge of the sanctioning phase of the administrative sanctioning procedure referred to in the Law and the Regulations, for such purposes:

a) Notifies the final report of the investigation to the person in charge, so that he/she may present his/her arguments within ten (10) working days after the notification.

b) It provides for complementary actions to be carried out, if deemed indispensable to resolve the administrative sanctioning procedure.

c) It issues the resolution imposing the sanction or ordering the procedure to be closed,

d) Notifies to the person administered the resolution that imposes the sanction or pronounces the non-existence of liability.

e) Informs the person who denounced the infraction of the decision, if applicable.

CHAPTER III MEANS OF APPEAL

Article 54.- Administrative Appeals

The administrative appeals established in the LPAG may be filed against the resolutions issued by virtue of this Law.

Article 55.- Appeals

Appeals filed against DGJCMT Resolutions will be resolved by the Vice Ministry of Tourism, as the second and final administrative instance.

TITLE VII

ADVERTISING

CHAPTER I
ADVERTISING AND SPONSORSHIP BROADCASTING

Article 56.- Warnings in the advertising of remote gaming and remote sports betting.

Both in the advertising of remote gaming and remote sports betting and in remote sports betting gaming rooms, the Registrant conspicuously places the phrase "Excessive remote gaming and remote sports betting may cause compulsive gambling".

In remote sports betting gaming halls, such phrase is placed in a visible place in the remote sports betting gaming hall, taking into account the dimensions established in Annex I of this Regulation.

In addition, the sentence "Excessive remote gambling and sports betting may cause compulsive gambling" is placed on the home page of the Holder's website in legible and easily visible characters, in proportion to the rest of the information.

With respect to advertising, the phrase "Excessive remote gambling and sports betting may cause compulsive gambling" is written in legible and easily visible characters, in proportion to the rest of the information advertised in the case of visual and audiovisual media, and in the case of radio advertising, said phrase is disseminated and pronounced in clear and understandable terms.

Article 57.- Prohibitions on advertising and sponsorship

57.1 The advertising of remote gambling or remote sports betting is prohibited:

a) Directed to minors;

b) That includes minors; and,

c) On legal entities that do not have authorization granted by MINCETUR for the operation of remote gaming or remote sports betting.

57.2 It is prohibited for companies that do not have an authorization for the operation of games of chance to operate in the following areas The advertisers of remote gaming and remote sports betting sponsor companies, natural persons, events or activities of any nature related to the remote gaming and remote sports betting activity. To this effect, those who receive such sponsorship verify the advertiser's authorized status.

SUPPLEMENTARY PROVISIONS

TRANSITIONAL SUPPLEMENTARY PROVISIONS

FIRST: Procedure for the authorization to operate Technological Platforms for remote gaming and/or remote sports betting.

The legal entities covered by article 4 of the present regulation that have been operating Technological Platforms for remote gaming and/or remote sports betting in the country before the entry into force of the Law, may continue operating them as long as they submit their request for authorization within thirty (30) calendar days as from the date of entry into force of the Law. Said request must be accompanied by the respective documentation evidencing the operation of the Technological Platform prior to the entry into force of the Law.

The legal entities included in the Second Transitory Complementary Provision of these Regulations may continue to operate their remote sports betting gaming rooms, provided that they attach to their request for authorization referred to in the preceding paragraph, the list and location of each of the remote sports betting gaming rooms they were operating before the entry into force of the Law.

MINCETUR authorizes the operation of the Technological Platforms for remote gaming and/or remote sports betting, to the legal entities that have submitted their application within the aforementioned term, after verifying compliance with the requirements set forth in articles 6, 7 and 8 of these Regulations, with the exception of paragraphs f) and g) of the aforementioned articles, as applicable.

The Holders of the authorization to operate Technological Platforms granted in accordance with the preceding paragraph have a term of no more than ninety (90) calendar days from the date of the operating authorization to comply with the requirement set forth in paragraphs f) and g) of articles 6, 7 and 8 of this Regulation. Otherwise, the authorization granted for the operation of remote gaming and/or remote sports betting is revoked.

SECOND.- Adequacy of remote sports betting rooms.

For the authorization to operate remote sports betting rooms, the legal entities included in numeral 9.1 of article 9 of the Law, in accordance with numeral 4.1 of article 4 of these Regulations must submit an application for each of the remote sports betting rooms within a term not to exceed thirty (30) calendar days from the day after obtaining their authorization, following the procedure set forth in article 15 of these Regulations.

MINCETUR authorizes the operation of remote sports betting gaming rooms, provided that the Holder has submitted its application within the aforementioned term, after verifying compliance with the requirements set forth in article 15 of this Regulation, being exempted from the prohibition set forth in numeral 29.1 of article 29 of the Law, as established in the Tenth Final Complementary Provision of the Law, for which they must submit the respective documentation evidencing the operation of each of the remote sports betting gaming rooms, prior to the entry into force of the Law.

For the adaptation of the remote sports betting rooms, the Licensees have a term of no more than sixty (60) calendar days as from the authorization of the remote sports betting rooms to comply with the requirement set forth in paragraph h) of article 15 of this Regulation. Otherwise, the authorization granted is revoked.

THIRD.- Control and sanctioning actions

At the end of the term of thirty (30) calendar days referred to in the Second Complementary Transitory Provision of these Regulations, MINCETUR proceeds to close the establishments where remote gaming and remote sports betting activities are carried out that have not complied with obtaining the respective authorization for their operation. The closing of such establishments, if applicable, is carried out together with the confiscation of the betting terminals, gaming means, gaming programs and other goods related to the direct exploitation of remote gaming and remote sports betting. Additionally, MINCETUR proceeds to the blocking of IP addresses, URLs, web pages and/or computer applications in the case of unauthorized exploitation of remote gaming and remote sports betting.

The aforementioned inspection actions are carried out without prejudice to the corresponding administrative sanctions.

FINAL SUPPLEMENTARY PROVISIONS

FIRST - VALIDITY

These Regulations shall enter into force the day after Law No. 31557 becomes effective.

SECOND - Issuance of mandatory directives and modification of technical requirements

MINCETUR, through the General Directorate of Casino Games and Slot Machines, may develop and specify the technical requirements contained in the approved Technical Standards, or dictate complementary provisions for compliance with the Law and the Regulations, by means of mandatory Directives.

THIRD.- Authorization for the operation of Technological Platforms for remote gaming and remote sports betting to the same Holder.

In the case of the same Licensee who has an authorization to operate remote gaming and remote sports betting, and operates them in the same Technological Platform, they may use the same user account and gaming account, and must necessarily differentiate the financial transactions for each of the authorizations. The Licensee transmits to the MINCETUR Data Center the economic and technical data for each Technology Platform operating authorization independently.

ANNEX I
NOTICE REGARDING THE WARNING AGAINST GAMBLING ADDICTION

IĞĞĞ--ĞĞĞĞĞĞĞĞĞĞĞĞĞĞĞĞĞĞĞĞĞĞĞĞ--------ĞĞĞĞĞĞĞĞĞĞ-----ĞĞ50 cmĞ-------ĞĞĞ-ĞĞI

IĞĞĞĞĞĞ---------ĞĞ30 cm- - - - - - - - -ĞĞI

"REMOTE GAMBLING AND
SPORTS BETTING CARRIED OUT
IN EXCESS OF
CAN CAUSE PATHOLOGICAL
GAMBLING".

ANNEX II
TABLE OF INFRACTIONS AND PENALTIES

NO.	Infringement	Legal Basis	Sanction			
			Caution	Fine	Cancellation	Ineligibility
1	Exploiting Technological Platforms of remote gaming or remote sports betting without the need to The corresponding administrative authorization must have been previously obtained.	Art. 38, literal a) of Law No. 31557		Very Serious: Fine from 150 UIT to 200 UIT		
2	To operate gaming programs for the Technological Platforms of remote gaming that do not previously have the corresponding authorization and registration (homologation).	Art. 38, paragraph b) of Law No. 31557		Minor: From 1 UIT up to 50 UIT per program		
3	Operating remote sports betting gaming rooms without having the operating authorization granted by MINCETUR.	Art. 38, paragraph d) of Law Nº 31557		Very Serious: Fine from 150 UIT to 200 UIT		
4	To operate progressive systems for the Technological Platforms of remote gaming or remote sports betting without the corresponding operating authorization or authorization and registration.	Art. 38, paragraph e) of Law No. 31557		Minor: Fine from 1 UIT up to 50 UIT		
5	Exploiting a quantity or type of gaming programs other than those authorized for the Technological Platforms of remote gaming.	Art. 38, paragraph f) of Law Nº 31557		Minor: Fine of 1 UIT up to 50 UIT per program.		

NO.	Infringement	Legal Basis	Sanction			
			Caution	Fine	Cancellation	Debarment
6	Impeding, hindering or not providing the facilities established in the Law or in the Regulations for the exercise of control and inspection actions by the competent authority.	Art. 38, paragraph g) of Law Nº 31557		Minor: Fine from 1 UIT up to 50 UIT		
7	Modify the modalities, types or conditions of the wager once it has been placed by the player and accepted by the Holder.	Art. 38, paragraph h) of Law No. 31557 Art. 12 paragraphs 12.1, 12.2 and 12.3 of Law No. 31557		Serious: Fine 50 UIT up to 150 UIT		
8	Failure to comply with the delivery of bonuses or payment of prizes obtained by the players, under the established conditions and deadlines.	Art. 38, paragraph i) of Law No. 31557		Minor: Fine from 1 UIT up to 50 UIT		
9	It does not comply with providing players with welcome bonuses or similar bonuses that are not redeemable for cash.	Art. 38, paragraph i) of Law No. 31557 Art. 16, numeral 16.2 of the Law No. 31557		Serious: Fine 50 UIT up to 150 UIT		
10	It does not pay the prizes obtained in the means of payment in which the player placed the bet or in an account in his name opened in a company of the financial system supervised by the SBS.	Art. 38, paragraph i) of Law No. 31557 Art. 15, numeral 15.5 of the Law No. 31557		Serious: Fine 50 UIT up to 150 UIT		
11	Failure to submit the information required by the competent authority within the established deadlines.	Art. 38, paragraph j) of Law Nº 31557		Minor: Fine of 1 UIT up to 50 UIT		
12	Allowing the placing of bets by persons not previously registered in the Technological Platforms of remote gaming and remote sports betting.	Art. 38, paragraph k) of Law Nº 31557 Art. 27, paragraph 27.9 of the Law No. 31557		Serious: Fine 50 UIT up to 150 UIT		
13	Not to register online the bets placed on the players' accounts on remote gaming or remote sports betting platforms.	Art. 38, literal l) of Law Nº 31557 Art. 26, numeral 26.10 of the Law No. 31557		Serious: Fine 50 UIT up to 150 UIT		
14	Employing or consenting to the use of fraudulent or irregular procedures or illicit operations in the operation of remote gaming or remote sports betting.	Art. 38, paragraph m) of Law Nº 31557			X	
15	Consenting to or allowing the performance on remote gaming or remote sports betting platforms, as well as in remote sports betting gaming halls, of acts that threaten public health and safety.	Art. 38, literal n) of Law Nº 31557		Very Serious: Fine from 150 UIT to 200 UIT		
16	Allowing access to remote gaming or remote sports betting platforms to persons prohibited from accessing them.	Art. 38, paragraph o) of Law Nº 31557 Art. 28 of Law No. 31557		Serious: Fine 50 UIT up to 150 UIT		
17	Contravene the rules established in the Law or in the Regulations related to the database, servers, data transmission and information security.	Art. 38, paragraph p) of Law Nº 31557		Serious: Fine 50 UIT up to 150 UIT		
18	The Technological Platform of remote gaming or remote sports betting does not have the necessary physical and logical access controls, network security and risk management in accordance with the regulations in force regarding information security and/or comply with the international standards and/or good practices that may be required.	Art. 38, paragraph p) of Law Nº 31557 Art. 17 of Law No. 31557		Serious: Fine 50 UIT up to 150 UIT		
19	The Technological Platform for remote gaming or remote sports betting does not include the measures and controls that protect the security of the data contained in the Technological Platforms, in accordance with the regulations in force and the best practices regarding information security and protection of personal data.	Art. 38, paragraph p) of Law Nº 31557 Art. 18 of Law Nº 31557		Serious: Fine 50 UIT up to 150 UIT		
20	The Technological Platform does not allow real-time transmission of technical and economic data to MINCETUR and SUNAT, in accordance with the provisions of the Regulations and Directives of mandatory compliance.	Art. 38, paragraph p) of Law Nº 31557 Art. 19 of Law Nº 31557		Serious: Fine 50 UIT up to 150 UIT		

NO .	Infringement	Legal Basis	Sanction			
			Caution	Fine	Cancellation	Debarment
21	The servers of the Technological Platforms of the remote gaming or sports betting at The distance are not installed in exclusive use environments with air conditioning, fire protection and grounding systems, server redundancy, high availability systems, uninterruptible power supply systems, as well as systems to protect against unauthorized physical and logical access, in order to guarantee uninterrupted operation and availability of the service, according to the conditions and specifications established in the Regulations.	Art. 38, paragraph p) of Law Nº 31557 Art. 20, numeral 20.2 of the Law No. 31557		Serious: Fine 50 UIT up to 150 UIT		
22	The Holder does not provide MINCETUR directly or through the service providers linked to the operation and exploitation of Technological Platforms of remote gaming and/or remote sports betting, the necessary accesses that allow obtaining information on the operations carried out by the players registered in the Technological Platforms.	Art. 38, literal p) of Law No. 31557 Art. 21, numeral 21.1 of the Law No. 31557		Minor: Fine of 1UIT up to 50 UIT		
23	Failure to comply with the obligations or prohibitions incumbent upon the holders of administrative registries derived from the application of the Law that are not related to the authorization to operate remote gaming or remote sports betting.	Art. 38, literal q) of Law No. 31557		Minor: Fine of 1UIT up to 50 UIT		
24	Failure to maintain in the remote sports betting gaming rooms the requirements or conditions set forth in the Law or in the Regulations.	Art. 38, paragraph r) of Law Nº 31557			X	
25	The Proprietary does not maintain the minimum distance established in numeral 29.1 of Article 29 of the Law.	Art. 38, paragraph r) of Law Nº 31557 Art. 29, paragraph 29.1 of the Law No. 31557			X	
26	The Registrant has not implemented a video system in accordance with the provisions of paragraph 1 of Article 18 of the Regulations of the Law.	Art. 38, paragraph r) of Law Nº 31557 Art. 18, numeral 1 Regulation Law Nº 31557		Minor: Fine of 1 UIT up to 50 UIT		
27	The Registrant does not maintain a video system that allows uninterrupted and real-time recording with a minimum of thirty (30) frames per second and one (01) CIF.	Art. 38, paragraph r) of Law Nº 31557 Art. 18, numeral 2 Regulation Law Nº 31557		Minor: Fine from 1 UIT up to 50 UIT		
28	The Contractor does not keep the recording and/or storage equipment that make up the video systems in a safe place with restricted access to the public.	Art. 38, paragraph r) of Law Nº 31557 Art. 18, numeral 3 Regulation Law Nº 31557		Minor: Fine from 1 UIT up to 50 UIT		
29	The Registrant does not maintain a video system that retains the recordings for a period of fifteen (15) months. (15) calendar days	Art. 38, paragraph r) of Law Nº 31557 Art. 18, numeral 4 Regulation Law No. 31557		Minor: Fine from 1 UIT up to 50 UIT		
30	Failure to maintain the conditions under which registration was granted administrative proceedings arising from the application of the Law or the Regulations.	Art. 38, paragraph s) of Law Nº 31557		Minor: Fine from 1 UIT up to 50 UIT		
31	Failure to maintain the conditions under which the authorization to operate remote gaming or remote sports betting was granted.	Art. 38, paragraph s) of Law Nº 31557			X	
32	The holder does not grant the guarantee provided for in Article 22 of Law No. 31557.	Art. 38, literal s) of Law No. 31557 Art. 22, numeral 22.1 of the Law No. 31557			X	
33	The holder does not maintain in force the guarantee referred to in numeral 22.1 of Article 22 of Law No. 31557.	Art. 38, literal s) of Law No. 31557 Art. 22 and 24, numeral 24.3 of Law No. 31557			X	
34	The Holder does not replace the guarantee within the established term after its execution.	Art. 38, literal s) of Law No. 31557 Art. 25, numeral 25.2 of the Law No. 31557			X	

NO.	Infringement	Legal Basis	Sanction			
			Caution	Fine	Cancellation	Ineligibility
35	The holder maintains as partner, director, manager or legal representative with powers registered in Public Records, persons who do not comply with the legal, economic-financial and/or background requirements and conditions set forth in the Law, its Regulations and/or mandatory Directives.	Art. 38, paragraph s) of Law Nº 31557 Art. 27, paragraph 27.3 of the Law No. 31557			X	
36	To entrust, delegate or subcontract with third parties, under any modality or circumstance, the total or partial performance of the tests, trials, consultations and/or reports in charge of the authorized certification laboratories, on the compliance of the technical standards required to the Technological Platforms of the remote games and remote sports betting.	Art. 38, paragraph t) of Law Nº 31557		Minor: Fine of 1UIT up to 50 UIT		
37	To grant certifications regarding Technological Platforms, gaming programs, progressive systems and components in charge of the authorized certification laboratories, which do not comply with the technical requirements established in the Law or in the Regulations.	Art. 38, literal u) of Law Nº 31557		Serious: Fine of 50 UIT up to 150 UIT		
38	Failure of authorized certification laboratories to provide facilities to MINCETUR's accredited personnel for the exercise of inspection functions.	Art. 38, paragraph v) of Law No. 31557		Minor: Fine from 1UIT up to 50 UIT		
39	Failure to comply with the conditions of The operating rules established for remote sports betting gaming halls.	Art. 38, literal w) of Law Nº 31557		Minor: Fine from 1UIT up to 50 UIT		
40	Contravene the other obligations and prohibitions established in the Law and the Regulations.	Art. 38, paragraph x) of Law Nº 31557		Minor: Fine of 1UIT up to 50 UIT		
41	The holder of the Technological Platform of remote games uses modalities or types of bets that violate the Law or the Regulations, affect the randomness of the game and/or the minimum percentage of return to the public.	Art. 38, paragraph x) of Law Nº 31557 Art. 12, paragraph 12.2.1 of the Law No. 31557		Minor: Fine of 1UIT up to 50 UIT		
42	The holder of the technological platform for remote sports betting games uses modalities or types of bets that violate the Law or the Regulations.	Art. 38, paragraph x) of Law Nº 31557 Art. 12, numeral 12.2.2.2 of the Law No. 31557		Minor: Fine of 1UIT up to 50 UIT		
43	The holder of the Technological Platform for remote sports betting games allows bets on sporting events that are not part of a national or international sporting association, federation or league.	Art. 38, paragraph x) of Law Nº 31557 Art. 12, numeral 12.3.2 of Law No. 31557, as amended by Law No. 31806.		Minor: Fine of 1UIT up to 50 UIT		
44	The holder of the Technological Platform for remote gaming uses progressive systems that do not have prior authorization from MINCETUR.	Art. 38, paragraph x) of Law Nº 31557 Art. 13, numeral 13.1 of the Law No. 31557		Serious: Fine of 50 UIT up to 150 UIT		
45	The holder of the Remote Gaming Technology Platform uses progressive systems that are not authorized and registered.	Art. 38, paragraph x) of Law Nº 31557 Art. 13, numeral 13.1 of the Law No. 31557 Art. 38, paragraph g) of the Regulations		Serious: Fine of 50 UIT up to 150 UIT		

46	The Holder carries out transactions with cryptocurrencies.	Art. 38, paragraph x) of Law Nº 31557 Art. 15, numeral 15.1 of the Law No. 31557 Art. 38, paragraph d) of the Regulations to Law No. 31557		Serious: Fine of 50 UIT up to 150 UIT		

NO.	Infringement	Legal Basis	Sanction			
			Caution	Fine	Cancellation	Ineligibility
47	It does not guarantee compliance with the characteristics, functionalities, integration of components and services, high availability connections, access controls and information security that must be met by the gaming technology platforms. and remote sports betting, in accordance with the provisions of the Law, its Regulations, mandatory Directives, and the regulations in force on the matter.	Art. 38, paragraph x) of Law Nº 31557 Art. 26, numeral 26.3 of the Law No. 31557		Serious: Fine of 50 UIT up to 150 UIT		
48	The Registrant does not maintain backup copies and backup and continuity controls that allow immediate recovery of the database. and transactions generated in the Technological Platforms subject to authorization, in accordance with the regulations in force regarding personal data and information security.	Art. 38, paragraph x) of Law Nº 31557 Art. 26, numeral 26.5 of the Law No. 31557		Serious: Fine of 50 UIT up to 150 UIT		
49	The Holder does not promote responsible gaming guidelines and establishes opt-out procedures in the Technological Platforms, in accordance with the provisions of the Regulations and/or mandatory Directives.	Art. 38, paragraph x) of Law Nº 31557 Art. 26, numeral 26.9 of the Law No. 31557		Serious: Fine from 50 UIT to 150 UIT		
50	It does not guarantee that, in the Technological Platforms of remote games or remote sports betting, the prizes and bonuses will be registered online in the corresponding account of the player.	Art. 38, paragraph x) of Law Nº 31557 Art. 26, numeral 26.10 of the Law No. 31557		Serious: Fine of 50 UIT up to 150 UIT		
51	The Holder does not comply with redirecting the entry made by the player of a Technological Platform not authorized in the country, to a Technological Platform that has such authorization, in cases where both Technological Platforms belong to the same holder.	Art. 38, paragraph x) of Law Nº 31557 Art. 26, numeral 26.11 of the Law No. 31557		Severe: Fine of 50 UIT up to 150 UIT		
52	The Holder does not comply with maintaining an open account in a financial or banking institution under the supervision of the SBS, in which the deposits for bets made by the players are kept exclusively and the intangibility of the deposits made for the referred concept is guaranteed.	Art. 38, paragraph x) of Law Nº 31557 Art. 26, numeral 26.12 of the Law No. 31557		Severe: Fine of 50 UIT up to 150 UIT		
53	The Holder does not verify the use of only one means of payment per user registered in the Technological Platform, and that the ownership of such means of payment corresponds to the identity of the player placing the bet.	Art. 38, paragraph x) of Law Nº 31557 Art. 26, paragraph 26.13 of the Law No. 31557		Severe: Fine of 50 UIT up to 150 UIT		
54	The Holder does not incorporate in the Technological Platforms, in a visible and easily accessible manner, the authorization registration code granted by MINCETUR.	Art. 38, paragraph x) of Law Nº 31557 Art. 26, numeral 26.14 of the Law No. 31557		Minor: Fine of 1UIT up to 50 UIT		
55	The Holder does not incorporate in the Technological Platforms, in a visible and easily accessible manner, the Single Taxpayer Registry.	Art. 38, paragraph x) of Law Nº 31557 Art. 26, paragraph 26.14 of the Law No. 31557		Minor: Fine from 1UIT up to 50 UIT		
56	The Holder does not incorporate in the Technological Platforms, in a visible and easily accessible manner, the following warning: "Games and bets". excessive distance sporting activities can cause compulsive gambling.	Art. 38, paragraph x) of Law Nº 31557 Art. 26, paragraph 26.14 of the Law No. 31557		Minor: Fine from 1UIT up to 50 UIT		
57	The Holder, in remote sports betting game rooms, does not guarantee that the players are duly registered.	Art. 38, paragraph x) of Law Nº 31557 Art. 26, numeral 26.16 of the Law No. 31557		Serious: Fine of 50 UIT up to 150 UIT		

58	The Proprietor does not verify the identity, age and nationality of the players when registering on the Technological Platform.	Art. 38, paragraph x) of Law Nº 31557 Art. 26, numeral 26.18 of Law No. 31557, as amended by Law No. 31806.		Serious: Fine of 50 UIT up to 150 UIT		

NO.	Infringement	Legal Basis	Sanction			
			Caution	Fine	Cancellation	Ineligibility
59	It does not guarantee that the service providers of the authorized and registered Technological Platforms will provide MINCETUR and/or SUNAT with the information and accesses required, in the procedures of control of remote gaming platforms or remote sports betting.	Art. 38, paragraph x) of Law Nº 31557 Art. 26, numeral 26.19 of the Law No. 31557		Serious: Fine of 50 UIT up to 150 UIT		
	The Contractor does not guarantee that any integration with the servers and other equipment of other related service providers complies with the specifications set forth in these Regulations, their respective Technical Standards and in the mandatory Directives.	Art. 38, paragraph x) of Law Nº 31557 Art. 26, numeral 26.20 of the Law No. 31557 Art. 37, paragraph g) of the Regulations to Law No. 31557		Minor: Fine from 1 UIT up to 50 UIT		
60	Exploiting unauthorized games of chance on the Technological Platforms.	Art. 38, paragraph x) of Law Nº 31557 Art. 27, numeral 27.1 of the Law No. 31557		Minor: Fine of 1UIT up to 50 UIT		
61	To exploit on the Technological Platforms, games of chance expressly prohibited.	Art. 38, paragraph x) of Law Nº 31557 Art. 27, numeral 27.1 of the Law No. 31557 Art. 38, paragraph h) of the Regulations to Law No. 31557		Minor: Fine of 1 UIT up to 50 UIT		
62	Incorporate in the Technological Platforms betting games on events or happenings of any nature that are not related to the games or bets authorized for their operation.	Art. 38, paragraph x) of Law Nº 31557 Art. 27, paragraph 27.4 of the Law No. 31557		Minor: Fine of 1UIT up to 50 UIT		
63	It establishes conditions for the placing of bets in remote games or remote sports bets that allow the money obtained as prize or bonus to be used to place new bets that do not form part of the taxable base of the Gaming Tax.	Art. 38, paragraph x) of Law Nº 31557 Art. 27, numeral 27.6 of the Law No. 31557		Serious: Fine from 50 UIT to 150 UIT		
64	Performs extortions, cancellations or any other operation regardless of the name assigned to it, aimed at rendering the wager ineffective, except in the cases provided for in the Regulations.	Art. 38, paragraph x) of Law Nº 31557 Art. 27, numeral 27.7 of the Law No. 31557		Minor: Fine from 1 UIT up to 50 UIT		
65	Transfer under any modality, in whole or in part, the authorization to operate Technological Platforms for remote gaming and remote sports betting.	Art. 38, paragraph x) of Law Nº 31557 Art. 27, numeral 27.8 of the Law No. 31557		Serious: Fine of 50 UIT up to 150 UIT		
66	Accept bets placed by players who are not previously registered in the Technological Platforms of remote gaming or remote sports betting.	Art. 38, paragraph x) of Law Nº 31557 Art. 27, paragraph 27.9 of the Law No. 31557		Serious: Fine of 50 UIT up to 150 UIT		
67	Contravene the other prohibitions set forth in the Regulations.	Art. 38, paragraph x) of Law Nº 31557 Art. 27, numeral 27.10 of the Law No. 31557		Minor: Fine of 1 UIT up to 50 UIT		
68	The Holder allows the player who is not registered in the Technological Platform and whose gaming account is not active to place, free of charge, for commercial promotion purposes, remote games or remote sports bets, either in any type or modality of betting.	Art. 38, paragraph x) of Law Nº 31557 Art. 27, numeral 27.10 of the Law No. 31557 Art. 38, paragraph b) of the Regulations to Law No. 31557		Minor: Fine from 1 UIT up to 50 UIT		

69	The holder contracts the services of related service providers that are not registered or whose registration has expired, been cancelled or revoked by MINCETUR.	Art. 38, paragraph x) of Law Nº 31557 Art. 27, numeral 27.10 of the Law No. 31557 Art. 38, paragraph c) of the Regulations to Law No. 31557		Very Serious: Fine from 150 UIT to 200 UIT		

NO.	Infringement	Legal Basis	Sanction			
			Caution	Fine	Cancellation	Ineligibility
70	The holder organizes, promotes and/or broadcasts remote games involving animal fights and/or races not permitted by the Peruvian State.	Art. 38, paragraph x) of Law Nº 31557 Art. 27, numeral 27.10 of the Law No. 31557 Art. 38, paragraph e) of the Regulations to Law No. 31557		Minor: Fine from 1 UIT up to 50 UIT		
71	The authorized certification laboratory does not deliver the guarantee foreseen in Article 23 of Law No. 31557 within the term foreseen in the Regulations.	Art. 38, paragraph x) of Law Nº 31557 Art. 23 Law No. 31557			X	
72	Operating betting terminals not authorized and registered by MINCETUR.	Art. 38, paragraph y) of Law No. 31557		Minor: Fine from 1 to 50 ITU per terminal		
73	Accept advertising from legal entities not authorized by MINCETUR in contravention of Article 31 of the Law.	Art. 38, paragraph z) of Law No. 31557, as amended by Law No. 31806.		Minor: Fine from 1 UIT up to 50 UIT		
74	The holder does not submit a comprehensive audit report of the entire Technology Platform that certifies compliance with the approved Technical Standards and mandatory directives, including the services provided by the related service providers, in accordance with the provisions of the following in Article 34.2, paragraph 34.2 of the Law and its Regulation	Art. 38, paragraph x) of Law No. 31557, Art. 34, paragraph 34.2 of the Law No. 31557, Art. 37, paragraph p) Regulation Law No. 31557		Minor: Fine from 1 UIT up to 50 UIT		
75	The licensee does not submit the report containing the integrity and safety assessment of the Technology Platform prepared by an authorized Certification Laboratory in accordance with the provisions of the Regulations.	Art. 38, paragraph p) of Law No. 31557, Art. 37, paragraph t) Regulation Law Nº 31557		Minor: Fine from 1 UIT up to 50 UIT		

TECHNICAL STANDARDS I
FOR REMOTE GAMING TECHNOLOGY PLATFORMS

Section 1. Evaluation and Technical Testing of Technology Platforms

The Technological Platform for remote gaming, gaming programs, progressive systems, integration between platforms, gaming modalities, among other components and services, prior to its authorization and registration (homologation) must be submitted to a technical evaluation by a Certification Laboratory authorized by MINCETUR.

The Remote Gaming Technology Platform Holder, as well as the linked service providers are responsible for all costs associated with testing and obtaining the certificate of compliance. For such purpose:

a) The authorized Certification Laboratory must have access to the source code of the Technology Platform software, game programs, progressive systems, integration between platforms, game modes, among other components and services, as well as the means to verify the compilation of the source code. The result of the compiled source code must be identical to that of the software submitted for evaluation;

b) In order for the authorized Certification Laboratory to issue the respective certificate of compliance, the remote gaming Technological Platform, the gaming programs, progressive systems, integration between Technological Platforms, gaming modalities, among other components and services, must comply at least with the technical specifications established in these Regulations and their respective approved Technical Standards, as well as those established in mandatory Directives;

c) For the approval of an authorization for the operation of Remote Gaming Technological Platforms, the Licensee must submit to MINCETUR, the description of the change management processes detailing the evaluation procedures to identify the criticality of the updates and determine which updates should be submitted to the authorized Certification Laboratory for review and certification. These change management processes should be:

i. Communicated to MINCETUR prior to implementation; and

ii. Audited at least once (01) a year by an authorized Certification Laboratory or by an independent area, not directly linked to the operation of remote gaming and/or remote sports betting of the Holder, acting as external auditor.

Section 2. Integration with the Technology Platforms

a) The Holder is responsible for the remote games carried out through its related service providers.

b) The servers and other equipment of the service providers are considered for the purposes of these Regulations as part of the Technological Platform, and the Contractor shall be responsible for ensuring compliance with the technical specifications set forth in these Regulations and their respective approved Technical Standards, as well as with the mandatory Directives.

c) The Contractor must ensure that any integration with the servers and other equipment of a Technology Platform is carried out in a manner that complies with the specifications set forth in these Regulations and their respective approved Technical Standards, as well as those established in mandatory Directives.

d) An authorized Certification Laboratory must perform integration and certification tests of each server and other equipment with the Licensee's Technology Platform, prior to its implementation and authorization by MINCETUR. For example, integration and certification tests must be performed between the remote gaming servers and the Technological Platform, as well as between the payment processing and the Technological Platform. Remote Gaming Servers should be understood as follows to the hardware and software that drives the features common to the game offerings, game configurations, the Random Number Generator (RNG), reporting, etc.

Section 3. Technology Platform Requirements

The Technological Platform may be made up of multiple Technological Platforms installed in one or several data centers. The Technological Platform, as well as the communication between its components must guarantee the adequate operation and integration of its components and services, and have high availability connections and access and information security controls. Likewise, they must comply with all the technical requirements contained in the approved Technical Standards I and III.

1.1. Technology Platform Clock Requirements

1.1.1 Technology Platform Clock

The Technology Platform including its components, services, applications and computer media must be synchronized with a single clock that reflects the current date (dd/mm/yyyy) and time (hh/mm/ss), which is used for:

a) The record of all transactions, games and events;
b) Recording of significant data and events;
c) Report generation; and
d) Transmission of economic and technical data to MINCETUR's Data Center.

1.1.2 Time synchronization

The Technology Platform must have a mechanism to ensure that the date and time is the same (synchronized and configured) in all its components, applications and computer media. The Technology Platform must be synchronized with the official Peruvian time GMT-5, for the registration of all transactions and occurrences, as well as for the generation of reports.

3.2 Control program requirements

In addition to the requirements contained in this section, the requirements contained in the "Verification Procedures" section of the approved Technical Standards III must also be complied with.

3.2.1 Automatic verification of the control program

The Technology Platform must have a self-diagnostic method that, at least every 30 days, verifies and authenticates that all components of the critical control programs or critical files that may affect gaming operations (executables, libraries, Technology Platform or game configuration, operating system files, components that control the required Technology Platform reports, and database elements that may affect Technology Platform operations) are identical to those evaluated and approved by the authorized certification laboratory that performed the corresponding technical evaluation.

Likewise, by means of user and password, the Holder, MINCETUR or the entity authorized by MINCETUR, may audit by means of remote or on-site access the Technological Platform, applications, software, services, databases, critical components and critical control programs.

The authentication method for control programs or files rated as critical must:

a) Employ a hashing algorithm that generates a 160-bit (40-digit) message digest as follows minimum. If other algorithms or methodologies are used, the authorized Certification Laboratory shall evaluate them and authorize their use, if applicable; and

b) Generate and display an authentication error message when any critical component of the control program is determined to be invalid.

3.2.2 Independent verification of the control program

a) The hashing algorithm used for the verification of each component of the critical control program or critical file must meet the following requirements:

i. Minimum of 160 bits (40 digits); and
ii. Allow its use from a personal computer. You can also use installation media such as: USB, DVD or CD or other similar media.

b) If the hash algorithm used is owned by the authorized Certification Laboratory, a copy must be provided at MINCETUR's request, free of charge, attaching its operation manual, operation or use, as well as the information corresponding to any update of the algorithm;

c) For the purposes of this Regulation, the SHA-1 Algorithm is considered approved ex officio by MINCETUR as a means of verification of the control program or other components, software, applications, database model. Any other algorithm to be used for such purpose must comply with the provisions of paragraph a) of 3.2.2. of this Technical Standard;

d) The impossibility of determining the electronic fingerprint (digital signature) does not lead to deny the authorization and registration of a Technology Platform. When, due to the nature of the storage medium, an electronic fingerprint cannot be determined, the authorized Certification Laboratory must state this fact in the respective Certificate of Compliance and indicate the reasons why such electronic fingerprint could not be generated; it shall also indicate the appropriate control mechanism to be used to ensure the integrity of each component of the critical control program of the Technology Platform or other components, software, applications, database model; and

e) Together with the submission of the request for authorization and registration (homologation) of the Technology Platform, the Technology Platform Holder provides any adapter, device or special interface used for reading the electronic fingerprint. Likewise, in case of updates of the authorized and registered (homologated) Technological Platforms, the authorized Certification Laboratories and the Technological Platform Holder must comply with submitting to MINCETUR the adapter, device or special interface, if applicable. Such delivery must be free of charge for MINCETUR.

3.3 Game Management

3.3.1 Game Management

The Technology Platform must have a secure mechanism that allows the Registrant to interrupt through the use of username and password or other secure method the following:

a) All gaming activities;
b) Game themes/pay tables or individual versions (desktop, mobile, tablet, etc.); and
c) Access to each player's session;

The Technology Platform must keep a record that identifies the time (hh/mm/ss), date (dd/mm/yyyy), and description of the interruption.

3.4 Player account management

The Technological Platform must have a method that allows each player to register his data, creating a user account and a game account, which are associated and must comply with the requirements contained in the "Game Account Controls" section of the approved Technical Standards III.

3.4.1 Registration and verification

For the creation of the game account on the Technology Platform, the player must first register his personal data. The process of registration of personal data and user account verification, as well as the game account must be supported directly by the Technology Platform or through the software of a related service provider, and must comply with the following requirements:

a) To create a game account on the Technological Platform, the player must register at least the following data:

i. Full name(s) and last name(s);
ii. Type of identity document
iii. Identity card number;
iv. Date of birth;
v. Nationality;
vi. Address (address, district, province and department); and
vii. Sworn statement regarding their status as Politically Exposed Person (PEP), in accordance with the regulations in force, if applicable.

b) Only persons of legal age (18 years or older) may register and access a user account and game account. During the registration process the player must be informed of the following:

i. You cannot access a gaming account if you are validated as a minor according to your date of birth.
ii. You cannot access a user account and a game account without completing the required fields of the electronic registration form.
iii. You must accept the terms and conditions, as well as the privacy policy.
iv. That it is forbidden for any person to access or use the game account without authorization and/or in violation of the permitted accesses.
v. That the Registrant and/or MINCETUR may monitor the user account and the gaming account;
vi. That your registered data is validated for the opening of the gaming account; and
vii. A gaming account may not be created if the player is registered in the Registry of Persons Prohibited from Accessing Establishments Intended for the Operation of Casino Games and Slot Machines, under the responsibility of the General Directorate of Casino Games and Slot Machines, or those acting in its stead, under MINCETUR.

c) Holders must restrict wagering by individuals in remote games until the validation process of the information and data registered is concluded:

i. Verification of the person's identity must include at a minimum, first name(s), last name(s), type of identity document, identity document number, age and nationality;
ii. The verification of the identity of the person must also verify that the player is not registered in any exclusion list of the Technological Platform and registered in the Registry of Persons Prohibited from Accessing Establishments Intended for the Operation of Casino Games and Slot Machines, in charge of the General Directorate of Casino Games and Slot Machines, or those in its stead, under the MINCETUR;
iii. The individual's identity verification data must be recorded and stored in a secure manner, in compliance with the Personal Data Protection Act; and
iv. The user account data must be kept during the period of validity of the user account, this period is calculated from the authorization granted by MINCETUR to the Holder and during the five years of validity of the user account.
(5) years following its cancellation or annulment, or during the statute of limitations period for the Remote Gaming and Remote Sports Betting Tax as provided in the Tax Code, whichever is greater.

d) The gaming account is blocked when the verification of the identity of the person is not successful or it is determined that the player is registered in any exclusion list, or registered in the Registry of Persons Prohibited to Access Establishments Intended for the Exploitation of Casino Games and Slot Machines, in charge of the General Directorate of Casino Games and Slot Machines, or those in its stead, under the MINCETUR, and the player has accepted the terms, conditions and privacy policies;
e) A player can have only one active user account and game account per Cardholder;
f) The Technology Platform must have the capability to update per player authentication credentials, person identity record information, and the player account used for financial transactions. Multi-factor authentication may be used for this purpose; and
g) The user account and the game account created in the Technological Platform are considered personal and non-transferable, as well as the funds associated with them.

3.4.2 Player access

The player must access his game account through username and password (authentication credentials) or through another secure authentication method approved by the authorized Certification Laboratory. The Technology Platform may present more than one authentication method for the player to access his/her gaming account.

a) If the Technology Platform does not recognize the authentication credentials entered, an informative message is displayed to the player requiring the credentials to be re-entered. The message is always the same as long as incorrect authentication credentials are entered.
b) When the player forgets his authentication credentials, a multi-factor validation process is used to recover or restore his credentials.
c) Current game account balance information, including any bonus credits, and transaction options must be available to the player upon authentication. All restricted bonus credits and bonus credits that have a stated expiration are detailed separately.
d) The Technology Platform must have a mechanism that allows a gaming account to be blocked when suspicious activity is detected, such as three
(3) consecutive failed login attempts within a thirty (30) minute period. A multi-factor authentication process must be used to unlock the game account.
e) Authentication credentials must be at least eight (8) characters long according to the security measures determined by the Holder.

3.4.3 Player inactivity

After thirty (30) minutes of inactivity in the game environment, the player must re-authenticate to access his/her game account.

a) No gaming or financial transactions are allowed in the Gaming Environment until the player re-authenticates.
b) The player can be offered a simpler method to re-authenticate in the Game Environment, such as,

authentication at the operating system level (biometrics) or a personal identification number (PIN). Each re-authentication method must be evaluated and approved by the authorized Certification Laboratory:

i. This functionality can be disabled according to the player's preference.
ii. Once every thirty (30) days the player is required to complete authentication of the Game Media.

3.4.4 Limitations and exclusions

The Technological Platform must have the capacity to correctly implement any limitation and/or exclusion established by the player and/or Holder, and in accordance with the Registers established by MINCETUR:

a) The Technology Platform must comply with allowing and managing limitations and/or exclusions, complying with the requirements established in the "Limitations" and "Exclusions" section contained in the approved Technical Standards III.
b) Limitations established by the player do not override more restrictive limitations imposed by the Holder. The more restrictive limitations must take precedence; and
c) Limitations should not be compromised by the status of internal events, as well as self-imposed exclusion orders and revocations.

3.4.5 Financial Transactions

When financial transactions can be performed automatically by the Technology Platform, the following requirements apply:

a) The Technology Platform must support the confirmation or rejection of each financial transaction initiated, including:

i. The type of transaction (deposit/withdrawal);
ii. The value of the transaction; and

b) The deposit made by the player to his gaming account is made by means of a transaction of circulating money, debit card, credit card or other means of payment accepted by the Holder, with the exception of cryptocurrency, which produce a proper audit trail.
c) Player funds are not available for play until a confirmation of authorization for their use is received. The authorization number generated as a result of the transaction confirmation is stored in the audit trail.
d) Payments from a gaming account must be sent directly to an account at a financial institution in the player's name, payment method of the player's choice or such other place as the Holder and the player may agree.
e) If a player initiates a transaction in the gaming account that exceeds the limits established by the Holder and/or MINCETUR in these Regulations or in a mandatory Directive, this transaction is processed only up to the maximum limit established, and the player is notified of this situation.
f) Transferring funds between two gaming accounts is not allowed.

3.4.6. Transaction register or gaming account summary

The Technological Platform must have the capacity to generate a record of the transactions or history of the gaming account summary, when required by the player. The information must be available to the player for at least two (02) years, and must include at least the following types of transactions:

a) Financial transactions (unique identification of the transaction with date and time):

i. Deposits to the gaming account;
ii. Withdrawals from the gaming account;
iii. Bonus credits added to/withdrawn from the gaming account;
iv. Adjustment of balances in the gaming account;
v. Any deposit of money to the gaming account without wagering;
vi. Total amount won for entire games, including, any bonus credits and/or prizes, and any progressive jackpot and/or incremental progressive jackpot (if applicable).
vii. Total number of cancellations.

b) Game history (by game theme);

i. The name of the game theme and the type of game (reel, blackjack, poker, table, etc.);
ii. Total amount wagered, including any bonus credits (if applicable); and
iii. Total amount won for entire games, including, any bonus credits and/or prizes, and any progressive jackpot and/or incremental progressive jackpot (if applicable).
iv. Total number of cancellations.

3.4.7. Player loyalty programs

Player loyalty programs are those that allow the delivery of bonuses to players based on the volume of play or revenue received from a player. If the Technology Platform features player loyalty programs, it must comply with the following:

a) All prizes, on an equitable basis, are available to those players who reach the qualifying level defined for player loyalty points;
b) The redemption of player loyalty points earned must be a secure transaction that automatically adds the value of the redeemed award to the points balance; and
c) All player loyalty point transactions must be recorded by the Technology Platform in the gaming account.

3.5. Player Software

The player software allows the Gaming Media to interact with the Technology Platform, so that the player can participate in the games and perform financial transactions. The player software is downloaded and installed on the Gaming Environment, run from the Technology Platform, accessed from the Gaming Environment or a combination of the two.

3.5.1 Software identification

The player software must have the necessary information to identify the software and its versions.

3.5.2 Software validation

The software for the player installed in the Gaming Media, each time it is loaded for use, and when the Technology Platform supports it, must authenticate that all its critical components are correct. Critical software components may include, but are not limited to, game rules, paytable information, elements that control communications between the Gaming Media and the Technology Platform or other software components that are necessary to ensure the proper functioning of the software. In the event of a failed authentication (program incompatibility or authentication failure), the software prevents gaming operations and displays a clear, simple and unambiguous error message.
Program verification mechanisms are evaluated by the authorized Certification Laboratory.

on a case-by-case basis, according to standard security practices in the remote gaming industry.

3.5.3. Communications

The player software must be designed in such a way that it can only communicate with authorized components via secure communication. If communication between the Technology Platform and the Gaming Medium is lost, the software must prevent further gaming operations and must display a clear, simple and unambiguous error message. It is acceptable for the software to detect this error when the Gaming Medium attempts to communicate with the Technology Platform.

3.5.4 Client-server interactions

The player can participate in games and financial transactions with the Technology Platform by downloading an application or software package containing the software for the player on the Gaming Environment or accessing the software through a browser.

a) The software must not allow players to transfer data between each other, except for chat functions (text, voice, video, etc.) and approved files (user profile pictures, photos, etc.);
b) The software does not automatically disable any virus scanners, detection programs or alter the firewall rules specified by the Gaming Environment to open ports that are blocked by a hardware or software firewall;
c) The software must only access the port (TCP/UDP) that is necessary for communication between the Gaming Media and the Technology Platform server;
d) If the software includes additional non-gaming functionality, this additional functionality does not alter the integrity of the software in any way;
e) The software must not have the ability to override the volume setting of the Play Medium;
f) The software is not used to store confidential information. Autofill, password storage or other methods that populate the password field must be disabled by default in the software; and
g) The Software does not have any logic used to generate the outcome of any type of game or event. All critical functions, including the generation of any game outcome, are generated by the Technology Platform and are independent of the Gaming Media.

3.5.5 Compatibility check

In the installation or initialization process and before starting the first game or event operation, the player software to be used in conjunction with the Technology Platform must have the ability to detect any incompatibilities or resource limitations of the Gaming Environment that prevent the correct operation of the software. If incompatibilities or resource limitations are detected, the software must prevent game operations and display a clear, simple and unambiguous error message.

3.5.6 Software content

Player software must not contain malicious code or functionality. This includes, and is not limited to, unauthorized file extraction/transfer, unauthorized device modifications, unauthorized access to any locally stored personal information (contacts, calendar, etc.) and malware (malicious program).

3.5.7 Cookies

Where the use of cookies is mandatory for gambling, bets may not be accepted until the player agrees to their use in the game environment. Players must be informed about the use of cookies after installation of the game software or during player registration. All cookies used must not contain malicious code.

3.5.8 Access to information

The player software must have the capability to display directly from the user interface or through a page accessible to the player, the sections detailed below:

a) Game rules and content;
b) Information for the protection of the player;
c) Terms and Conditions; and
d) Privacy policy.

3.5.9 Information in Several Languages

The information provided through the player software must be offered in the English language. When the information available to the player is provided in different languages, the following principles should be applied:

a) Each language option of the same activity must offer the same payout percentages or odds/payouts and prices, as the case may be.
b) When a player chooses to participate in different languages of an activity, he/she should have the same probability of winning, regardless of the language option he/she chooses.
c) Each language variant must be consistent with the information in that variant.
d) All information must be provided in the language specified for that variant.
e) Information should have the same meaning in all languages, so that no variant is favored or disfavored.
f) It is not mandatory to translate common game terms used internationally. In case of including commercial words in a language other than English, they must be introduced in a glossary available to the player.

3.5.10 The home page of the Holder's website

The Holders must include on the home page of the Remote Gaming Technology Platforms:

a) A link to the MINCETUR Web Portal for registration in the Registry of Persons Prohibited from Accessing Establishments for the Operation of Casino Games and Slot Machines.
b) The phrase "Excessive remote gambling and sports betting may cause compulsive gambling" must be displayed in legible and easily visible characters, in proportion to the rest of the information.

3.6 Information to be maintained

The Holder or the technological platforms of its related service providers must register, store and have a backup of the data and information in this section. In case the information is stored by the related service providers, the Holder is responsible that such information is available to MINCETUR and/or SUNAT.

3.6.1 Data storage and date and time stamping

The Technological Platform must have the capacity to store and have a backup of the data and information registered for a minimum period of five (05) years, counted from the granting of the authorization by MINCETUR to the Holder, or during the period of prescription of the Tax on Remote Gaming and Gambling.

Remote Sports Betting as provided in the Tax Code, whichever is greater:

a) The clock must be used to record all data and events;
b) It must have a mechanism that allows exporting data to be analyzed, audited and verified, using CSV, XLS or compatible formats.

3.6.2 Game information

In the Technological Platform of the Holder or its related service providers, a backup must be registered, stored and maintained independently for each player and for each game played individually or with multiple players. In case the information is stored by the related service providers, the Holder is responsible for making such information available to MINCETUR. At least the following information must be available:

a) The date and time the game was played;
b) If it is a multi-denomination game type, indicate the denomination used in the game;
c) The display associated with the final result of each game, either graphically or in a clear and unambiguous text description;
d) The funds available for wagering at the beginning of the game and/or at the end of the game;
e) Total amount wagered, including bonus credits;
f) Total amount earned, including:

i. Any bonus credits and/or awards; and
ii. Any progressive jackpot or incremental progressive jackpot;

g) Any non-wagered game account deposits that occurred between the beginning and the end of the game;
h) The results of any player election involved in the outcome of the game;
i) The results of any phase, such as doubling/betting or bonus/game features;
j) If a progressive jackpot and/or incremental progressive jackpot was won, an indication that the jackpot was awarded;
k) Any "player tips" offered to the player for games of skill;
l) Progressive jackpot or incremental progressive jackpot contributions;
m) The current state of the game;
n) Unique game cycle ID; and/or game session ID (if different from the cycle);
o) Identification of the theme of the game/pay table; and
p) Unique player identification.

3.6.3 Game Theme/Pay Table Information

For each individual game theme and paytable available for play, the information that the Technology Platform stores and supports, as applicable must include:

a) Identification of the theme of the game/pay table;
b) Game configuration data (denominations, betting categories, etc.);
c) The date and time when the game theme/payment table was available for play;
d) Theoretical percentage of return to the player;
e) The number of games played;
f) Total value of all bets, not included:

i. Any bonus credits wagered; and
ii. Subsequent bets on intermediate prizes accumulated during the game, such as those acquired from the doubling/betting features;

g) Total value paid as a result of winning bets, not included:

i. Any bonus credits and/or awards earned;
y
ii. Any progressive jackpot and/or incremental progressive jackpot won;

h) Total value paid as a result of progressive jackpot and/or incremental progressive jackpot win;
i) Total amount of bonus credits wagered;
j) Total amount of bonus credits and/or awards earned;
k) Total amount of cancelled bets, including bonus credits;
l) The number of times each jackpot is awarded;
m) For games that support doubling/betting functions:

i. Total bet amount to double/bet;
ii. Total amount of doubling/betting earned;
iii. Number of doubling/betting games played;
iv. Number of doubling/betting games won;

n) The current status of the gaming/pay table issue; and
o) The date and time that the game topic/pay table was or is scheduled to be decommissioned (blank until known).

3.6.4 Competition/Tournament Information

The Technology Platform that supports the competition/tournament must record, store and maintain a separate backup for each competition(s)/tournament(s) and at a minimum must have the following information:

a) Name or identification of the competition/tournament;
b) The date and time the competition/tournament occurred or takes place (if known);
c) Identification(s) of the subject(s) of the participating game(s)/payment table(s);
d) For each registered player:

i. Unique player identifier;
ii. Total amount of the competition/tournament entry fee, including all bonus credits, and the date of collection;
iii. Player ratings/rankings;
iv. Amount of awards paid, including all bonus credits, and the date of payment;

e) Total amount for competition/tournament entry fee, including all bonus credits;
f) Total amount of prizes paid to players, including all bonus credits;
g) Total amount of commissions per service, if applicable; and
h) The current state of the competition/tournament.

3.6.5 Game account information

The Technology Platform must record, store and maintain an independent backup for each gaming account and at least the following information must be available:

a) Unique player ID and player name (if different);
b) Personally identifiable information of the player, such as:

i. The information collected by the Registrant in the registration of the player and that creates the user account, which includes the first name(s), last name(s), type of identity document, identity document number, age, nationality, telephone number and address;
ii. The player's personal identity must be encrypted, including the type of identity document and identity document number, authentication credential, and the player's identity card.

(password, PIN, etc.) and personal financial information (debit card numbers, credit card numbers, bank account numbers, etc.);

c) The date and method of identity verification, including, where applicable, a description of the identity document provided by a player to confirm his identity;
d) The date the player accepted the Holder's terms and conditions and privacy policy;
e) Account details and current balance, including deposits, awards, bonus credits, balance adjustment and returns. All restricted bonus credits and bonus credits that have an expiration date are recorded separately;
f) The date and time of the cancellation of the bets, as well as the reason for the cancellation.
g) Previous accounts, if any, and reason for deactivation;
h) The date and method from which the account was registered (Gaming Media or Remote Sports Betting Gaming Room);
i) The date and time of entry to the account (player, Holder or MINCETUR), including the IP address;
j) Exclusions/limitations information:

i. The date and time of the request;
ii. Description and reason for exclusion/limitation;
iii. Type of exclusion/limitation (exclusion imposed by the Registrant, self-imposed deposit limitation, among others);
iv. The exclusion/limitation start date
v. The date of exclusion/limitation completed;

k) Financial transaction information:

i. Type of transaction;
ii. The date and time of the transaction;
iii. Unique transaction identifier;
iv. Transaction amount;
v. Total account balance before/after the transaction;
vi. Total amount of cost per transaction (use of credit card, debit card, etc.), if applicable;
vii. Identification of the user who processed the transaction, if applicable;
viii. Transaction status (pending, complete, etc.);
ix. Deposit/withdrawal method (cash, personal check, cashier's check, wire transfer, debit card, credit card, electronic funds transfer, etc.);
x. Deposit authorization number;

l) Persistence game information, if supported by the Technology Platform:

i. Unique game theme/paytable identification, if linked to a particular game theme or paytable;
ii. Game contributions, earned capabilities or similar;
iii. Last saved point, if the game is supported from a saved location;

m) Identification information, if supported by the Technology Platform:

i. Unique game theme/paytable identification, if related to a particular game theme or paytable;
ii. The date and time of the transaction;
iii. Unique transaction identification;
iv. Criteria for the use of the identifier (player skill level, subscriptions, account memberships, player tracking information, game skill requirements, etc.);
v. The type of action taken, or alteration made to the game (game rule change, paytable change, or other configuration change related to the outcome of the game); and

n) The current status of the game account (active, inactive, closed, excluded, etc.).

3.6.6 Bonus information

The Technology Platform that supports bonus awards that may be redeemable in cash or wagering credits, must record, store and support the following information for each bonus award offered, as applicable:

a) Unique identifier of the bonus offer;
b) The date and time the bonus was made available;
c) Current balance for bonuses;
d) Total number of bonuses granted;
e) Total number of bonus awards redeemed;
f) Total number of expired bonuses granted;
g) Total number of bonus adjustments granted;
h) The current status of the bonus(s); and
i) The date and time the bonus was or is scheduled to be terminated (blank until known).

3.6.7 Progressive jackpot and incremental progressive jackpot information

The Technology Platform that supports the progressive jackpot or incremental progressive jackpot must record, store and support the following information for each jackpot offered (progressive or incremental progressive), as applicable:

a) Unique identification of the jackpot (if the jackpot is not linked to a particular game theme, paytable or player);
b) The date and time the jackpot became available;
c) Identification(s) of the subject(s) of the participating game(s)/payment table(s);
d) Unique identifier(s) of player(s), if the jackpot is linked to a player(s);
e) Current value of the progressive jackpot;
f) Any other pot containing contributions to the jackpot, as applicable

i. Current value of the amount exceeding the limit, as established by MINCETUR in this Regulation or Directive of mandatory compliance;
ii. Current value of the jackpot diversion scheme;

g) Reset value of the current jackpot if different from the initial value (reset value);
h) Where these parameters are configurable after the initial configuration:

i. Initial value of the jackpot (initial value);
ii. Percentage rate of increase, (increase);
iii. Value limit of the jackpot (maximum);
iv. Percentage rate of increase after reaching the maximum (secondary increase);
v. Percentage rate of increase for the diversion fund;
vi. Limit value of the diversion fund;
vii. The odds of triggering the jackpot (odds);
viii. Any parameter that indicates the time periods in which the progressive jackpot is available for a trigger (time limit);
ix. Any additional information to reconcile the jackpot properly;

i) The current status of the jackpot (active, disabled, paid, etc.); and
j) The date and time the jackpot was or is scheduled to be paid (blank until known).

3.6.8 Significant event information

The Holder or the technological platforms of its related service providers must record, store and permanently have a backup of the information of significant events. In case, the information is stored by the related service providers, the Holder is responsible that such information is available to MINCETUR and/or SUNAT, as appropriate:

a) Unsuccessful attempts to access the game account or the account of the Holder, including the IP address;
b) Authentication error or discrepancy;
c) Significant periods of unavailability of any critical component of the platform (any period of time that the game is stopped for all players, and/or transactions cannot be successfully completed for any user);
d) Cancellations and adjustments of balances of the Technology Platform;
e) Changes in live data files occurring outside the normal execution of the program and Technology Platform;
f) Changes made to the data download library, including the addition, change or deletion of software, if applicable;
g) Changes in policies and parameters for Technology Platforms, databases, networks and applications (audit settings, password complexity settings, Technology Platform security levels, manual database updates, etc.);
h) Date/time changes on the main server;
i) Changes in the parameters of the game theme (e.g. game rules, payout schedules, payout tables, etc.);
j) Changes in the parameters of progressive jackpots or incremental progressive jackpots;
k) Changes in the bonus parameters (startup/ purpose, value, eligibility, restrictions, etc.);
l) Gaming account management:

i. Gaming account balance adjustments;
ii. Changes made to the player's personal identity information and other confidential information recorded from a game account/user account;
iii. Deactivation of a game account;
iv. Major financial transactions (unique and aggregated in a defined period of time) that exceed the values that may be established by these Regulations and Directives of mandatory compliance, including the information of the transaction;
v. Negative balance of the gaming account (due to balance adjustments);

m) Loss without recovery of the player's personal identity information and other confidential information;
n) Any other activity that requires the user's intervention and that occurs outside the normal scope of the Registrant; and
o) Other significant or unusual events that may be specified in mandatory Directives.

3.6.9 Holder Access Information

The Technological Platform must register, store and maintain a backup independently for each account of the Holder that allows access to the Technological Platform and at least the following information must be registered:

a) Name of the employee of the Holder who accessed, as well as his or her position;
b) Identification of the Holder's employee;
c) Complete list and description of the roles and permissions that each Holder account or group can execute;
d) The date and time when the Holder's worker account was created;
e) The date and time of the last access, including the IP address;
f) The date and time of the last password change;
g) The date and time when the Holder's worker account was disabled/deactivated;
h) Members of the Registrant's group or account, if applicable; and
i) The current status of the worker's account (active, inactive, closed, suspended, etc.).

3.7 Reporting requirements

3.7.1 General reporting requirements

The Technological Platform must have the capacity to generate online reports, as required by MINCETUR through a WEB Application or other secure access method using a user name and password, which are provided by the Holder at the request of MINCETUR and SUNAT.

In addition to complying with the provisions of the section "Data storage and date and time stamping", the following reporting requirements apply:

a) The Technology Platform must have the capacity to allow filters to be made on the content of the reports, on a daily, monthly (start and end date) and annual (start and end date) basis, as a minimum;
b) Each required report must contain:

i. Report title;
ii. The company name or corporate name of the Holder and identification code;
iii. Date and time of generation;
iv. The selected period;
v. Identification of the MINCETUR user who requested the report;
vi. An indication of "No activity" or a similar message if no data appear for the specified period;
vii. Labeled fields that must be clearly understood according to their function; and
viii. Ability to be exported to PDF or Excel files.

3.7.2 Game performance reports

The Technological Platform must have the capacity to generate online reports, as required by MINCETUR, on the performance of the game for each game theme or pay table, as appropriate. Access is through a WEB Application or other secure access method using a username and password, which are provided by the Holder at the request of MINCETUR and SUNAT:

a) The name of the theme and type of game (roller, blackjack, poker, table, etc.);
b) The date and time when the game theme/payment table was available for play;
c) For games against the house:

i. Theoretical percentage of return;
ii. Theoretical percentage of current return;

d) The number of games played;
e) Total amount of wagers collected, including separately the amounts set aside for bonus credits;
f) Total amount of prizes paid to players, including amounts separated by bonus credits and/or prizes;
g) Total amount of cancelled bets, including separately the amounts set aside for bonus credits;
h) Total amount of credits remaining in interrupted games, including separate amounts for bonus credits;

i) Identification of the theme of the game/pay table; y

j) The current status of the game/payment table topic (active, disabled, terminated, etc.).

3.7.3 Report of the Holder's consolidated income:

The Technological Platform must have the capacity to generate online reports, as required by MINCETUR, on the Holder's consolidated income, as appropriate. Access is through a WEB Application or other secure access method using a username and password, which are provided by the Holder at the request of MINCETUR and SUNAT.

The required report must at least allow daily, monthly (start and end date) and annual (start and end date) filters of:

a) Consolidated income generated daily (total bets received, total prize payments, total bonuses, total prizes associated with the progressive system, total cancellations, total refunds, total service fees, registration fees; among others, date and time, identifying the Holder, as well as any other counter necessary for the correct calculation of the daily production) by the Technological Platform, taking into consideration the operations of the day occurring between 00:00:00 hours of a day (start) and 23:59:59 hours of the same day.

b) The search is performed by the registration code granted by MINCETUR to the Holder.

3.7.4 Jackpot Payment Reports (Progressive Systems)

The Technological Platform must have the capacity to generate online reports, according to MINCETUR's needs, on one or more progressive jackpots or incremental progressive jackpots that exceed the value established by MINCETUR. Access to the report is made through a WEB Application or other secure access method using a user name and password, which are provided by the Holder at the request of MINCETUR and SUNAT:

a) Unique identification of the jackpot (if the jackpot is not linked to a particular game theme, paytable or player);
b) Identification of the winning player;
c) Identification of the theme of the game/pay table;
d) Identification of the winning game cycle and/or game session identification (if different);
e) The date and time of the jackpot activation;
f) Winning jackpot and payment amount; and

3.7.5 Reporting of significant events and disturbances

The Technological Platform must have the capacity to generate online reports, according to MINCETUR's needs, on each significant event or alteration. Access to the report is done through a WEB Application or other secure access method using username and password, which are provided by the Holder at the request of MINCETUR and SUNAT:

a) The date and time of each significant event or disturbance;
b) Event/component identification;
c) Identification of the user(s) who performed and/or authorized the significant event or alteration;
d) Reason/description of the significant event or alteration, including the data or parameter altered;
e) Value of the data or parameter before the alteration; y
f) Value of the data or parameter after the alteration.

3.7.6 Report of transactions made by each player

The Holders directly or through the service providers linked to the operation, provide MINCETUR and SUNAT with the necessary access through a WEB Application or other secure access method using username and password, which are provided by the Holder at the request of MINCETUR and SUNAT, to obtain the information contained in the section "Transaction record or gaming account summary" made by the players in their gaming accounts according to the following search filters:

a) Player identification:

i. Full name;
ii. ID card number/foreigner's card number/passport number; and
iii. Unique player identifier.

b) Identifier of the place where the transaction took place (Technological Platform or physical establishment);
c) Transactions performed (such as deposit history, withdrawals, bets, prizes, etc.) by each player, allowing filtering by date and time; and
d) Other filters that may be established by mandatory Directives.

3.7.7 Player account report

The Holders of an authorization to operate Technological Platforms for remote sports betting, directly or through the service providers linked to the operation, provide MINCETUR with the necessary access through a WEB Application or other secure access method using a username and password, which are provided by the Holder at the request of MINCETUR and SUNAT, to obtain information contained in the section "Gaming Account Information" made by the players in their gaming accounts according to the following search filters:

a) Player identification:

i. Full name;
ii. ID card number/foreigner's card number/passport number; and
iii. Unique player identifier.

b) Identifier of the place where the transaction took place (Technological Platform or physical establishment);
c) Transactions performed (such as deposit history, withdrawals, bets, prizes, etc.) by each player, allowing filtering by date and time; and
d) Other filters that may be established by mandatory Directives.

3.7.8 Platform Specific Report

The Technological Platform must have the capacity to generate online reports, as required by MINCETUR, which are delivered by the Holder at the request of MINCETUR and SUNAT, showing the following information:

a) Commercial name of the Technology Platform;
b) Version of the Technological Platform;
c) Detailed information on available gaming programs by service provider;
d) Detailed information on the different types of remote games in operation; and
e) Any other information that MINCETUR may require by means of a mandatory Directive.

3.7.9 Construction of new reports

Notwithstanding the reports described above, MINCETUR may request the Registrant, upon prior notice, to prepare new supplementary reports.

3.8 Physical and logical accesses to the Technology Platform

3.8.1 Audit

Holders of an operating authorization must provide MINCETUR and/or an entity authorized by MINCETUR with physical or logical access to the Technological Platform to perform a comprehensive audit of critical control components or programs, critical files, services, integration services between Technological Platforms, databases, applications, among other software or hardware components that MINCETUR deems necessary.

In the case of logical access, the Registrant must provide a secure access method by means of user and password or other mechanism that allows for a comprehensive audit of the Technology Platform, taking into consideration the following:

a) The Holder must establish a secure communication mechanism to its Technological Platform and that of its related service providers, as well as allow and facilitate at all times the remote audit to MINCETUR and/or entity authorized by MINCETUR, regardless of the physical location of its data centers;

b) MINCETUR may inform the Registrant of the date scheduled for the audit of the Technological Platform, as well as provide information on the activities to be performed and, if necessary, require the specialized support of the Registrant's personnel.

c) The personnel designated by the Contractor must provide the necessary facilities, access, permits and privileges to MINCETUR in order to comply with the scheduled audit. MINCETUR may carry out the corresponding auditing activities and collect the necessary evidence in accordance with the provisions of the LPAG.

d) If not otherwise required, it should be understood that the access provided to MINCETUR is read-only and has the necessary permissions and privileges to access the entire Technology Platform, services, applications, databases, among other software or hardware components deemed necessary without any filter. Once the access is finished, the Holder must close the secure access.

3.8.2 Real-time supervision and control of remote games

The Licensees must deliver to MINCETUR the remote accesses to the Technological Platform where the remote games are exploited, in order to allow the control and supervision of the different modalities of remote games being exploited. The accesses have secure communication channels by means of user and password or another secure access method that does not allow vulnerability of the Technological Platform security. Likewise, the necessary privileges must be granted to carry out the control.

MINCETUR may require the specialized support of the Holder's personnel to carry out the inspection and control of the Technological Platform. MINCETUR may carry out the corresponding inspection activities and collect the necessary evidence in accordance with the provisions of the LPAG.

Section 4. Random Number Generator (RNG) Requirements

This section sets out the technical requirements for a random number generator (RNG). Types of RNGs include the following:

a) A software-based GNA does not use hardware devices and derives its randomness primarily from a computer- or software-based algorithm. They do not incorporate hardware randomness in any significant way.

b) A hardware-based GNA derives its randomness from small-scale physical events (feedback from electrical circuit, thermal noise, radioactive decay, photon spin, etc.).

c) Mechanical GNAs generate game results mechanically, using the laws of physics (wheels, drums, blowers, shufflers, etc.).

4.1. GNA General Requirements

4.1.1 Source Code Review

The authorized Certification Laboratory reviews all source code for each of the basic randomization algorithms, scaling algorithms, shuffling algorithms, and other algorithms or functions that play a critical role in the final randomized outcome selected for use in a game. This review should include comparisons with previous studies where appropriate, and an examination for sources of bias, implementation errors, malicious code, code with potential to corrupt behavior, or undisclosed switches or parameters that may influence randomness and fair play.

4.1.2 Statistical Analysis

The authorized Certification Laboratory uses statistical tests to evaluate the results obtained by the GNA, after scaling, shuffling or other type of mapping (final result). The authorized Certification Laboratory chooses the appropriate tests on a case-by-case basis, depending on the GNA under test and its use in the game. The tests are selected to ensure conformity with the intended distribution of values, statistical independence between draws and, where appropriate, statistical independence between multiple values within a single draw. The tests applied are evaluated collectively at a 99% confidence level. The amount of data tested is such that significant deviations from the applicable GNA test criteria can be detected with high frequency.

In the case of a GNA intended for variable uses, it is the responsibility of the independent testing laboratory to select and test a representative set of uses as test cases. Statistical tests may include one or more of the following:

a) Total distribution or Chi-square test;
b) Overlap test;
c) Coupon collector test;
d) Test runs;
e) Interaction correlation test;
f) Serial correlation power test; and
g) Duplicate testing.

4.1.3 Distribution

Each possible GNA selection has the same probability of being chosen. When the game design specifies a non-uniform distribution, the final result conforms to the expected distribution.

a) All scaling, assignment and shuffling algorithms used must be unbiased, which is verified by review of the source code. Discarding GNA values is allowed in this context and may be necessary to eliminate bias.

b) The final result is tested against the intended distribution using appropriate statistical tests (Total Distribution Test).

4.1.4 Independence

Knowledge of the numbers chosen in one draw does not provide information about the numbers that may be chosen in a future draw. If the GNA selects multiple values in the context of a single draw, knowledge of one or more values does not provide information about the other values within the draw, unless provided by the game design.

a) As verified through source code review, the GNA does not discard or modify selections based on previous selections, except as provided by the game design (non-substitution functionality).

b) The final result is tested for independence between draws and, as applicable, independence within a draw, using appropriate statistical tests (Serial Correlation Test or Interaction Correlation Test and Runs Test).

4.1.5 Available Results

As verified by the source code review, the set of possible outcomes generated by the GNA solution (i.e., the GNA period), considered as a whole, must be sufficiently large to ensure that all outcomes are available at each draw with adequate probability, regardless of previously obtained outcomes, except where specified in the game design.

4.2 GNA Scaling and Monitoring

4.2.1 Scaling the GNA for Outcome Determination

The GNA used in determining game outcomes on a Gaming Technology Platform is cryptographically strong. "Cryptographically strong", means that the GNA is resistant to attack or compromise by an intelligent attacker with modern computational resources, and who may have knowledge of the source code of the GNA.

4.2.2 GNA Cryptographic Attacks

A cryptographic GNA cannot be compromised by the ability of an attacker who knows the source code. At a minimum, cryptographic GNAs are resistant to the following types of attacks:

a) Cryptanalytic Direct Attack: Given a sequence of past values produced by the GNA, it is not computationally feasible to predict or estimate future values of the GNA. This must be ensured by the appropriate use of a recognized cryptographic algorithm (GNA algorithm, hash, cipher, etc.). Note that a hardware-based GNA or mechanical GNA can potentially qualify as a cryptographic algorithm, provided it passes statistical tests;

b) Known Input Attack: It is not computationally feasible to determine or reasonably estimate the state of the GNA after the initial seed. In particular, the GNA should not be initialized with a seed from a specific time value. The manufacturer should ensure that sets do not have the same initial seed. Seeding methods must not compromise the cryptographic strength of the GNA; and

c) Compromised State Attack Extension: The GNA must periodically modify its state, through the use of external entropy, limiting the effective duration of any potential attack exploited by an attacker.

4.2.3 Dynamic Output Monitoring for Hardware Based Random Number Generator

Due to their physical nature, the performance of hardware-based random number generators may deteriorate over time or may malfunction, regardless of the platform. Failure of a hardware-based GNA can have serious consequences for the intended use of the GNA. For this reason, if a hardware-based GNA is used, there should be dynamic monitoring of the result by statistical testing. This monitoring process should disable the game when malfunction or degradation is detected.

4.3. Mechanical GNA (Physical Randomness Devices)

The requirements defined in this section apply to mechanical random number generators or "physical randomness devices". While software may be part of the device, the software is primarily limited to operating machinery and/or reading and recording game outcome data (the software does not play a deterministic role in determining the outcome of the game).

Approved components of a physical randomness device cannot be interchanged or replaced with non-approved components, as they are integral parts of the behavior and performance of a physical randomness device. "Approved components" in this context include the physical products that produce the random behavior - e.g., balls in a shuffler, cards in a shuffler, etc. As an example, a shuffler certified by the authorized Certification Laboratory to use plastic cards cannot be considered an approved equivalent for the same mechanical shuffler using paper cards.

4.3.1 Data Collection

To provide the best guarantee of random behavior, the Authorized Certification Laboratory collects at least 10,000 game results data. The data collection is performed in a similar way as when a player participates in the development of a game. Devices and components (cards, balls, etc.) should be started with the recommended configuration and calibration, and replaced or maintained during the data collection period as recommended by the manufacturer.

Exceptionally, upon justification by the authorized Certification Laboratory, the collection of less than 10,000 game result data may be accepted.

4.3.2 Durability

All mechanical parts are manufactured with materials that prevent degradation of any component during their service life.

4.3.3 Manipulation

Players and/or game assistants (dealers, card dealers, dealers, dealers, etc.) used in live games may not physically manipulate or influence the game results randomly generated by the physical devices, except as provided for in the game design.

Section 5. Game Requirements

This section establishes the technical requirements of the player interface, game rules, fair play requirements, game selection, game outcome, player related artwork and displays, payout percentages and odds, bonuses, progressive jackpot, incremental progressive jackpot game history, game modes, skill games, tournaments and other game requirements.

5.1 Gaming Testing and Authorization

The Holder may not operate a game unless it has been evaluated and certified by a Certification Laboratory authorized by MINCETUR.

The playground equipment supplier is responsible for the total costs associated with testing and obtaining such certificate of compliance. Each game supplier must submit all games proposed for use to an authorized Certification Laboratory for evaluation and certification prior to operation, as well as all changes to the games.

a) If it is an addition of a new game running on a certified remote game server, the game provider must provide certification of the game.

b) If it is an addition of a new game running on a new remote game server, the game provider must provide certification of the game, while the Registrant must provide certification of the integration between the Technology Platform and the remote game server.

5.2 Player Interface

Player interface is defined as an application or interface program through which the user views and/or interacts with the player software, including touch screen(s), keyboard, mouse or other forms of player interaction devices.

5.2.1 Player Interface Requirements

The player interface must meet the following requirements:

a) Any resizing or overlaying of the player interface screen is accurately identified to reflect the revised display and touch/click points;

b) All touch points/clicks or buttons selected by the player or buttons represented on the player interface that impact the course of the game and/or the integrity or outcome of the game must be clearly labeled according to their function and must operate in accordance with the rules applicable to the game;

c) There shall be no hidden or undocumented touch points or buttons anywhere on the player interface that affect game play and/or affect the integrity or outcome of the game, except as indicated by the rules of the game.

d) The display of instructions and information is adapted to the player interface. For example, when a device uses smaller touch screen technologies, it is permissible to present a summarized version of the game information accessible directly from the game screen and make available the full/complete version of the game information through another method, such as a secondary screen, help screen or other interface that is easily identified on the visual game screen.

e) When multiple items of instructions and information are displayed on the player interface, it is acceptable for this information to be displayed alternately provided that the speed at which the information is alternated allows the player a reasonable opportunity to read each item.

5.2.2 Simultaneous Entries

Simultaneous or sequential activation of multiple player interaction devices that include a player interface does not cause game failure or result in outcomes contrary to the game's design intent.

5.3. Game Session Requirements

A gaming session is defined as the period of time that begins, at the moment the player initiates a game(s) on a Technology Platform for a given gaming theme, placing one or more bets and ends at the moment of the final outcome of the game(s) which may coincide with the opportunity for the participant to exit the game.

5.3.1 Simultaneous Games

This section is not intended to exclude or prohibit designs that allow simultaneous play of multiple game themes on a Technology Platform. When multiple game themes can be accessed simultaneously, players may play more than one game at a time on separate game sessions. However, in such a case, the applicable metrics and limits apply to each available game, as played, and all other requirements contained in the approved Technical Standards continue to apply to these multiple-play designs in the games.

5.3.2 Game selection

The following requirements apply to the selection of a specific game in the player interface:

a) The Technology Platform informs the player of all games available for play.

b) The player must know what game theme he has selected to play and what is being played.

c) The selection of a game theme does not imply that the player is obliged to play it, and the player may return to the main menu or game selection screen before placing a bet unless the game screen indicates that the selection cannot be changed.

d) When entering the game from the main menu or from the game selection screen, the game screen displayed by default must not correspond to the highest prize (unless it is the result of the player's last play). The above is only related to the main game and not to secondary bonuses or features.

5.3.3 Game Requirements

The following requirements apply to play within a game session:

a) A game cycle consists of all player actions and game activity that occur between bets. The start of the game cycle must occur after the player:

i. Places a bet or evidence of intent to bet;
and/or
ii. Press a "Play" button or perform a similar action to start a game according to the game rules.

b) Amounts wagered, or those where the player evidences intent to wager, at any time at the beginning or during the course of a game cycle are subtracted from the player's credit meter or game account balance. A wager that may cause the player to have a negative balance is not accepted.

c) The following game elements are considered part of a single game cycle:

i. Games that initiate a free play bonus and any subsequent free games;
ii. "Second screen" bonus(s);
iii. Games with choices by the player (draw poker or blackjack);
iv. Games where the rules allow for additional credit bets (insurance for blackjack, or the second part of a two-part Keno game);
v. Fold/Risk.

d) A game cycle is considered complete when all wagered funds are lost, or when the final transfer to the player's credit meter or game account balance occurs. The value of each prize at the end of a game cycle is added to the player's credit meter or game account balance.

e) It is not possible to place a new bet within the same game session until any previous bets placed in the same game have been settled and the available betting funds and game history have been updated.

5.3.4 Information to be displayed

The player interface must display the following information within the game session, except that the player is in an informative screen such as a menu or help screen:

a) Current funds available for wagering;
b) Designation of active play, if applicable;
c) The amount of the current bet and the placement of all active bets, or display enough information to otherwise derive these parameters;
d) Any player's wager option that occurred prior to the initiation of the game or during the course of the game;
e) For the last completed game, the following information should be displayed until the next game starts, betting options are modified or the player exits the game;

i. An accurate representation of the outcome of the game;
ii. The prizes awarded;
iii. Any betting option of the player.

5.3.5 Credit Meter

Depending on the Technology Platform, funds may be transferred from the game account balance to a credit meter for the start of the game session. This may be automatic when the game account balance is automatically transferred to the credit meter or the Technology Platform presents transfer options to the player, which requires confirmation before it occurs. Once the game is completed, the player has the option to transfer part or all of their funds to their game account balance. Upon exiting a game session, all funds are automatically transferred to the player's game account balance. In addition, the credit meter must meet the following requirements when in use:

a) The credit meter is always visible to the player when; a wager can be placed, a transfer to or from the game account balance is allowed, or the meter is incremented or decremented.
b) The credit meter can display the information in credits or in circulating currency format (Soles, US Dollars or other currency). If the game's credit meter allows toggling between credits and currency, this functionality must be player friendly and easy to understand. The credit meter must show unambiguously whether the information displayed is in credits or in circulating currency.
c) If the current circulating currency amount (Soles, US Dollars or other currency) is not an even multiple of the denomination of a game, or the credit amount has a fractional value, the credits displayed for that game may be displayed and played as a truncated amount (the fractional portion is removed). However, the fractional credit amount is made available to the player when the truncated credit balance is zero.
d) If restricted bonus credits and unrestricted player funds are combined in a credit meter, restricted credits are wagered first, as permitted by the game rules, before unrestricted player funds are wagered.

5.4. Game Information and Game Rules

5.4.1 Game Information and Game Rules

The following requirements apply to game information, artwork, payout tables and help screens including any written, graphic and audio information provided to the player either directly from the player interface or from a page accessible to the player:

a) Player interface and instructions for the use of the interaction device, paytable information and game rules must be complete and unambiguous and not misleading or unfair to the player.
b) The information on the help screens is accessible by the player without the need for deposited funds or intent to wager.
c) Minimum, maximum and other available bets are indicated, or can be inferred from the artwork, with appropriate instruction for any available bets.
d) Paytable information which should include all possible winning outcomes and combinations along with their corresponding payouts for any available betting options.
e) Artwork should clearly indicate whether prizes are designated in credits and/or cash.
f) In the case of artwork containing game instructions that explicitly advertise a prize credit, it must be possible to win the referred prize, whether through a single game or a series of games which were enabled by an initial game, including bonuses or other game options, the artwork must clearly specify the criteria necessary to win the referred prizes.
g) The game reflects any changes in the prize value, which may occur during the course of the game. This can be accomplished with a digital display in a visible location on the player interface. The game clearly indicates the criteria for any prize value to be modified.
h) Game instructions that are presented aurally are also presented in written form within the art illustrations.
i) Game instructions are depicted in a color that contrasts with the background color to ensure that all instructions are clearly visible and legible.
j) The artwork clearly indicates the rules for prize payouts. If a specific winning combination is paid where multiple prizes are possible, then the means of payment must be described.

i. Artwork should clearly indicate the procedure for matching game results. For example, a straight flush may be interpreted as either a flush or a straight flush. Where a payline may be interpreted as having more than one such winning combination, it is noted if only the highest winning combination is paid per line.
ii. Where the same symbol may qualify for a line payout and scatter payout simultaneously or where line and scatter payouts occur simultaneously on the same line, the artwork indicates whether the player receives payouts for both prizes, or the higher of the two.
iii. The artwork should clearly inform the treatment of scattered winning combinations with respect to each other. For example, the artwork indicates whether the scatter symbol combinations give all possible prizes or only the highest prize.

k) When multiplier symbols are displayed on the player's screen, the functions of the multiplier and when the multiplier does not apply must be clearly shown.
l) All symbols/objects in the game must be clearly visualized by the player and must not confuse them.

i. Game instructions that specifically correspond to one or more symbols/awards must be clearly associated with those symbols/awards. For example, this can be accomplished with an appropriate framing or picture. Additional text such as "these symbols" may also be used.
ii. If the game instructions refer to a particular symbol and the name of the written symbol may be confused with another symbol, or may imply other characteristics then the visual presentation of the instructions should clearly indicate which symbol is referred to in the game instruction.
iii. Game symbols and objects retain their shape throughout all artwork, except while an animation is in progress. Any symbol that changes its shape or color during a process

animation, it cannot appear in a way that can be misinterpreted as some other symbol defined in the paytable.

iv. If the function of a symbol changes (for example, a non-substitute symbol becomes a substitute symbol during a bonus), or the appearance of the symbol changes, the artwork must clearly describe this change in function or appearance and any special conditions that apply to it.

v. If there are limitations regarding the location and/or appearance of any symbol, the limitation should be indicated in the artwork. For example, if a symbol is only available in a bonus game, or on a specific reel strip, then the artwork should indicate this.

m) The artwork clearly indicates which symbols/objects can act as a substitute or wild symbol and in which winning combinations the substitute or wild symbol can be applied; this description should clarify all phases of the game where a wild or substitute symbol operates.

n) The artwork clearly indicates which symbols/objects can act as a scatter symbol and in which winning combinations the scatter symbol can be applied.

o) The artwork must contain textual and/or graphic information explaining the order in which the symbols appear for a prize to be awarded or for when a bonus is initiated, including numbers to indicate how many correct symbols/objects correspond to each pattern.

p) The game should not announce that the prize is about to be awarded.

q) The artwork should explain any form of game restriction, as well as any game duration limits, maximum prize values, etc. that are implemented as a design element of the game.

r) There will be sufficient information on any award payment adjustments, as appropriate.

5.4.2 Multiple Betting Games

The following requirements apply to games where multiple independent wagers may be applied simultaneously towards the prizes offered, as conditions relevant to the specific game design:

a) Each individual bet placed must be clearly indicated so that the player has no doubt about the bets placed and the credits wagered for each bet;

b) The prize amount for each separate wager and the total amount of the prizes must be displayed on the game screen; and

c) Each winning prize must be clearly displayed to the player so that the prize is associated with the wager placed. Where there are prizes associated with multiple wagers, each winning wager must be indicated. In cases where there is a large volume of wager information to be communicated, an on-screen summary is sufficient. Any exceptions are reviewed by the authorized Certification Laboratory on a case-by-case basis.

5.4.3 Line Games

The following requirements are specific to the design of online games:

a) For multi-line games, the game provides a summary display of the paylines that are available to form winning combinations;

b) Each individual line to be played must be clearly indicated by the game so that the player has no doubt as to which lines are being wagered. Showing the number of lines wagered is sufficient to meet this requirement;

c) For games that allow multiple credits to be wagered on selected lines, the illustration must:

i. For linear payouts, clearly indicate that the prizes for each selected line are multiplied by the bet multiplier; or

ii. For non-linear payouts, transmit all possible bets and their prizes;

d) Bet multipliers must be displayed. It is acceptable if this can be easily derived from other displayed information;

e) The illustration should indicate the rules and/or limitations related to how payments are assessed, including an indication of:

i. How earned lines are evaluated (left to right, right to left or both directions);

ii. How individual symbols are evaluated (whether payouts are awarded only on adjacent reels or as scattered payouts); and

f) Winning paylines must be understandable to the player. Where there are multiple line prizes, each winning payline is indicated in turn. This requirement should not preclude other intuitive methods of displaying line prizes such as grouping common prize types, nor should it prohibit a player the option to override the detailed display of line prize results, where supported.

5.4.4 Playing Cards

For games represented by cards drawn from one or more decks, the following requirements apply, depending on their importance in the specific game design:

a) At the start of each game and/or hand, cards must be drawn from one or more randomly shuffled decks; it is acceptable to draw random numbers for replacement cards at the time the random number for the first hand is drawn, provided that the replacement cards are used sequentially when needed and provided that the stored GNA values are encrypted;

b) Once cards have been drawn from the deck(s), they are not returned to the deck(s), except as provided in the rules of the game;

c) The deck or decks may not be reshuffled, except as provided in the rules of the game;

d) The game should alert the player to the number of cards in a deck and the number of decks being played;

e) The face of the cards must clearly show the value of the card and its suit; and

f) Joker cards and jokers must be distinguishable from other cards.

5.4.5 Poker Games

The following requirements apply to the design of games containing poker game simulations:

a) The artwork provides a clear indication of which poker variant is being played and the rules that apply;

b) Joker card rules should be clearly explained in the help screens; and

c) The cards held and not held, including cards recommended to be held, must be clearly detailed on the screen, and the method of changing the status of a selected card is clearly shown to the player.

5.4.6 Blackjack games (blackjack)

The following requirements apply to the design of games containing simulations of blackjack games:

a) Insurance rules should be clearly explained if insurance is available;

b) The rules for separating a Pair should be explained to include:

i. Separate aces have only one card dealt to each ace, if this is the rule,

ii. Separate more times, if available;

iii. Fold after separating, if available;

c) The bending rules should be clearly explained, including limitations on which totals may allow a selection of bending;

d) Any limits on the number of cards that may be dealt by the player and/or dealer must be explained, including declared winners (if any) when the limit is reached;

e) Surrender rules are explained, if any;

f) If a separate Pair has occurred, the results of each hand are displayed (total points, resulting prize category or loss, prizes awarded, amount wagered);

g) Special rules, if any, should be clearly explained; and

h) All player options that are available at any time are shown in the artwork.

5.4.7 Roulette Games

The following requirements apply to the design of games containing roulette game simulations:

a) The method of selection of individual bets must be explained by the rules of the game;

b) The bet or bets already selected by the player must be displayed on the screen; and

c) The result of each spin of the wheel is clearly indicated to the player.

5.4.8 Dice Games

The following requirements apply to the design of games containing dice game simulations:

a) Each face of the die must clearly show its face value;

b) After the dice are rolled, it should be obvious which is the top face on each die, and

c) The result of each die must be clearly visible or displayed.

5.4.9 Sports/Racing Games

The following requirements apply to the design of games containing sports or racing game simulations:

a) Each participant in a game is unique in appearance, where it applies to the bet;

b) The result of a race must be clear and not left to misinterpretation by the player;

c) If prizes are paid for combinations with participants other than exclusively the first place finisher, the order of the participants involved with these prizes is clearly indicated on the screen (result of 8-4-7); and

d) The rules of any other type of unusual bet (perfect, trifecta, quiniela, etc.) and the expected payouts should be clearly explained in the artwork.

5.4.10 Ball/Number Extraction Games

The following requirements apply to the design of games that depict the removal of balls or numbers from a container:

a) Simulated balls are drawn from a randomly mixed container consisting of the complete set of balls/numbers applicable to the rules of the game;

b) At the start of each game, only the balls/numbers applicable to the game are represented. For games with bonus and additional balls/numbers that are drawn, these are drawn from the original selection unless allowed by the rules of the game;

c) The container is not stirred again unless permitted by the rules of the game; and

d) All balls/numbers drawn are clearly displayed to the player.

5.4.11 Keno or Bingo Games

The following requirements apply to the design of games containing simulations of keno or bingo games, where balls or numbers are drawn from a simulated box (or equivalent) and a player attempts to choose in advance which of the balls are selected:

a) All player selections are clearly identified on the game screen. Where the game uses multiple player cards, it is acceptable for player selections to be accessible by flipping or switching cards;

b) The numbers selected in the drawing must be clearly identified on the screen;

c) The game highlights numbers that match the player's selections;

d) Special awards, if any, are clearly identified;

e) The display should provide a clear indication of how many positions were selected and how many prizes were won; and

f) The rules for obtaining additional game bonuses, if any, should be explained.

5.4.12 Immediate Prize Games

The following requirements apply to the design of games containing simulations of instant win games:

a) Instant win games are based on randomness rather than player skill;

b) A precise definition of which player options are required to complete the immediate prize game must be shown in the artwork;

c) For instant win games that take advantage of popular real-life themes (cards, dice, etc.), but do not reflect the actual game and probabilities, a disclaimer is added to the artwork stating that the results are not distributed with the probabilities normally expected from this game; and

d) After the player acquires an instant win game, the game outcome and prize are revealed to the player. The player may or may not have to interact with the game to reveal the prize/loss results.

5.4.13 Multiplayer Games

The following requirements apply to the design of multiplayer games:

a) The multiplayer game is designed so that the actions or results obtained by any player do not affect the results of any other player, unless the rules of the game indicate otherwise; and

b) There will be a method provided by a multiplayer game for each player to know when the next game starts.

5.5 Game Result Using a Random Number Generator (RNG)

5.5.1 The GNA and the Game Outcome Assessment

When using the GNA in the outcome of the game, the following rules must be complied with:

a) If more than one GNA is used to obtain the result of the games, each of the GNAs is evaluated separately; and

b) Where each instance of a GNA is identical, but includes a different implementation in the set, each implementation is evaluated separately.

5.5.2 Game Selection Process

The determination of opportunity events that result in a monetary award must not be influenced, affected or controlled by anything other than the values selected by a GNA, in accordance with the following requirements:

a) In the course of the game when the GNA is invoked all combinations, symbols and elements are available for your choice, except those foreseen in the game design;
b) The game does not modify or discard the results selected by the GNA due to modeling, being the results used as established in the rules of the game;
c) After selecting the outcome of the game, the game must not show a "near miss" that affects the result displayed to the player.
d) Except as provided by the rules of the game, opportunity events are independent and do not correlate with any other event within the same game, or events within previous games;
e) A game must not allow the probability of a bonus occurring based on the history of prizes won in previous games;
f) The percentage of return to the public should not be based on previous awards;
g) Any associated equipment that is used in conjunction with a platform must not influence or modify the behaviors of the game's GNA and random selection process, except as provided in the design; and
h) Chance events are not affected by the effective bandwidth, link utilization, bit error rate or other characteristics of the communications channel between the Technology Platform and the Gaming Media.

5.6 Fair Play Requirements

5.6.1 Fair Play

The following requirements apply to the fairness of the game:

a) Games that are designed to give a player the perception of control over the outcome of the game, due to skill or dexterity, when in fact they do not (the outcome of the game is random and the illusion of skill is for entertainment only), should inform the player of this fact within the game's help screens;
b) Games must not include any hidden source code that may provide an advantage to a player to circumvent game rules and/or intentional game design behavior; and
c) The final result of each game is displayed to the player for a reasonable period of time to verify the outcome of the game.

5.6.2 Simulation of Physical Objects

When a game incorporates a graphical representation or simulation of a physical object that is used to determine the outcome of the game, the behavior represented by the simulation must be consistent with the real-world object, unless otherwise stated in the game rules. The following requirements apply to simulation:

a) The probability of any event occurring in the simulation that affects the outcome of the game is analogous to the properties of the physical object, unless otherwise indicated to the player;
b) Where the game simulates multiple physical objects that are expected to be independent of one another in accordance with the rules of the game, each simulation must be independent of the others; and
c) Where the game simulates physical objects with no history of previous events, the behavior of the simulated objects must be independent of their previous behavior, so as not to be predictable, unless otherwise instructed to the player.

5.6.3 Physical Engine

Games can use a "physics engine" which is specialized software that approximates or simulates a physical environment, including behaviors such as motion, gravity, velocity, acceleration, inertia, trajectory, etc. A physics engine is designed to maintain behaviors of the game and its environment, unless the rules of the game instruct the player otherwise. A physics engine can use the random properties of a GNA to impact the game outcome, in this case, the "Random Number Generator (RNG) Requirements" requirements apply.

5.6.4 Correlation of Live Games

Unless otherwise indicated in the artwork, when the Technology Platform offers a simulation game of a live casino game, such as Poker, Blackjack, Roulette, etc., the same odds associated with the live game are identical in the simulated game.

5.6.5 Probability of Random Events

For games that incorporate a random event or an element of chance that affects the outcome, the mathematical probability of any chance event occurring in a paid game is constant, unless otherwise indicated in the artwork.

5.7 Payout Percentages, Odds and Non-Cash Prizes

5.7.1 Requirements for the Percentage of Payments software

Each game must have a theoretical return of not less than eighty-five percent (85%) over the expected life of the game. Progressive jackpots, incremental jackpots, bonus prizes, etc., are not included in the payout percentage if they are external to the game, unless required for the operation.

a) The minimum percentage requirement is met for all wager configurations. If a game is played continuously at any individual bet level, line configuration, etc. for the life of the game, the minimum percentage requirement is met.
b) Games that may be affected by player skill must meet the minimum percentage requirement when using an optimal method of play that provides the greatest return for the player over a continuous period of play.
c) For the progressive jackpot and incremental progressive jackpot used in the calculations of the theoretical percentage return to player (TRP) for the game, the minimum percentage requirement is met using the lowest available parameters for the jackpot over the expected life of the game.

5.7.2 Theoretical Player Return Percentage (TRP) Display

If the gaming software displays the return to the player it must meet the following requirements:

a) The artwork clearly explains how the displayed TRP was determined (minimum, maximum, average, etc.) and, therefore, how the player can realize it (wagering requirements).

b) For games that may be affected by player skill, the displayed TRP is based on a strategy specifically announced in the rules of the game or on an optimal strategy that can be derived from the rules of the game.
c) For games that offer progressive jackpots or incremental jackpots, limited time prizes or other bonuses/features, the variable contribution of such prizes to the displayed TRP is clearly shown.
d) For games that offer bonus games that require additional credits to be wagered, the displayed TRP considers that an additional wager was placed unless otherwise announced.
e) If the TRP displayed represents the actual TRP, the number of games associated with that calculation is announced along with the period with which the games took place.

5.7.3 Odds

The odds of achieving the highest explicitly advertised prize that is based solely on chance must occur at least once in every 100 million games, unless the game artwork prominently displays the actual odds of that prize to the player. This does not apply to multiple prizes won together in the same game where the aggregate prize is not announced. This odds rule does not apply to games that make it possible for a player to win the highest advertised prize multiple times through the use of a bonus. This rule applies to all betting categories that can win the highest advertised prize. If the highest advertised prize can occur within a bonus, the odds calculation includes the odds of winning the bonus, including the odds of winning the prize. This rule does not apply to promotional bonuses.

5.8 Bonus Requirements

5.8.1 In-game bonus

Games offering bonus(s) must meet the following requirements:

a) A game that offers one or more bonus(s), other than those that occur randomly, must display sufficient information to the player to indicate the current status towards the activation of the next bonus game;
b) If a game requires multiple achievements towards the activation of one or more bonus(s) or the awarding of a prize, the number of achievements required to activate the bonus, or earn the prize, is indicated, along with the number collected at any point;
c) The game should make it clear to the player that he is in a bonus mode;
d) If a game offers a bonus that allows the player to hold one or more reels/cards/symbols for the purpose of an additional spin or draw, then the reels/cards/symbols held must be clearly indicated and the method of changing the hold must be clearly explained to the player;
e) If a bonus(s) is triggered after the accumulation of a certain number of events/symbols or combination of events/symbols of a different type in multiple games, the probability of obtaining matching symbols/events shall not deteriorate as the game progresses, unless otherwise disclosed to the player; and
f) If a bonus(s) consists of multiple events or spins, then a counter is maintained and displayed to the player to indicate the number of spins initially awarded and the number of spins remaining during the bonus game or alternatively, the number of spins that have been played.

5.8.2 Player Selection or Bonus Interaction

Games that offer a bonus(s) that require player selection or interaction, are prohibited from making selections or initiating the bonus automatically, unless the game meets one of the requirements listed below and explains the automatic initiation or selection mechanism in the artwork:

a) The player is presented with a choice and expressly acknowledges his or her intent that the Gaming Terminal will automatically initiate a bonus game by means of a button press or other interaction by the player;
b) The bonus provides only one option for the player, i.e. pressing a button to spin the wheel. In this case, the bonus may automatically start after a period of time of at least two (2) minutes; or
c) The bonus is offered as part of a community game involving two or more players and where the delay of an offered selection or the initiation of the game directly impacts the ability for other players to follow their bonus. Prior to making selections or initiating a bonus, the player should be prompted so that they are aware of the time remaining in which they must make their selection or initiate the game.

5.8.3 Bonus credit wagering during a bonus

If a bonus in progress requires additional funds to be wagered to continue, the player has the opportunity to opt out. If all prizes in the current game are accumulated in a temporary counter called "win", instead of directly to the credit counter or in the game account balance, the game must:

a) Provide a means whereby prizes in the temporary meter called "win" can be wagered to allow for instances where the player does not have sufficient funds available to complete the bonus, or allow the player to add funds to the credit meter or game account balance; and
b) Transfer all credits from the temporary counter named "winnings" to the credit counter or to the game account balance when the bonus is completed.

5.8.4 Community Bonus

Community bonuses, where players collaborate and/or compete for a shared prize, must:

a) Have a proper description of the rules governing each community bonus, each payout and any conditions regarding the player's choice of community bonus prizes;
b) Continuously and conspicuously displays the player's selection for a community bonus, regardless of the amount of credits in the game. For example, if the player has thirty seconds of eligibility time remaining, but has run out of credits, the game continues to display and count the remaining seconds; and
c) For bonuses that are not dependent on the amount of credits available, it alerts the player of their continued eligibility regardless of whether the player has credits remaining in the game.

5.8.5 Doubling/risk bonuses

A double up or risk bonus consists of the player as part of the game taking a risk by deciding to accept the bonus offered and playing it, which can end up with winning double/triple the wagered amount or losing it. These types of games may use alternative terminology such as "Triple Up" or "Take or Risk". The following requirements apply to games that offer some form of the double up or risk bonus:

a) All instructions for the bend/risk bonus are fully indicated in the game artwork and should be accessible without committing to play the bonus;

b) Access to the double up/risk bonus can only occur at the end of a winning primary base game;

c) The player has the option to participate or not in the doubling/risk bonus;

d) The doubling/risk bonuses have a theoretical return to the player of one hundred percent (100%);

e) The maximum number of doubling/risking games available must be clearly specified, or as an alternative, the doubling/risking prize limit must be indicated to the player;

f) Only credits earned in the primary game are available for wagering on a double/take a risk bonus, (it is not possible to wager funds from the credit meter or game account balance to double/take a risk);

g) When the doubling/risk bonus is automatically discontinued before the maximum available number of the doubling/risk bonus is reached, the reason must be clearly indicated;

h) Any game conditions during which the doubling/risk bonus is not available must be specified;

i) If the doubling/risk bonus offers a choice of multipliers, it should be clear to the player the range of options and what the payouts are; and

j) If the player selects a doubling/risk multiplier, it must be clearly indicated on the screen which multiplier has been selected.

5.8.6 Mystery Awards

A mystery prize is a prize paid for a game that is not associated with a specific paytable combination. It is acceptable for games to offer a mystery prize, however, the game artwork must indicate the minimum and maximum amounts that the player can potentially win. If the minimum amount that can potentially be awarded is zero, then it need not be explicitly shown. If the value of the mystery prize depends on credits wagered, or any other factor, the conditions should be clearly stated.

5.9 Alternative Game Modes

5.9.1 Free Game Mode

The free play mode allows the player to participate in a game without having to place a wager. If the game has a free play mode operation, the following requirements apply:

a) Free games must accurately represent the normal operation of a paid game. Games played in the free games mode must not mislead the player about the probability of winning any prize available in the wagered version of the game;

b) The free play mode should be prominently displayed so that the player is informed at all times if/when this mode is active;

c) Free play mode does not increase any credit meter or game account balance. Specific meters are allowed for this mode, provided that the meters are clearly indicated as such;

d) The free play mode is concluded when the player wishes to exit this mode, or when the free play game is concluded; and

e) When you exit the free play mode, the game must return to its previous state.

Paid games that can be played with credits received from a bonus prize are not considered free games.

5.9.2 Automatic Game Mode

The auto play mode allows a game to place wagers automatically without player interaction, once a denomination, wager, and other game attributes have been selected by the player. If the game has an autoplay mode, the following rules apply:

a) The automatic play mode must be safely controlled using a function that allows enabling or disabling this function.

b) The autoplay mode can allow the player to choose the individual game bet, the number of autoplay bets and/or the total amount to be wagered;

i. All limits defined by the player remain in effect for the duration of the auto games;

ii. The game must show the number of remaining autoplay bets or the number used, reflecting the limit defined by the player;

iii. The autoplay mode should automatically terminate and return to manual play when the limits defined by the player are reached;

c) The autoplay must offer the player an option to terminate the autoplay mode upon completion of the current game, regardless of how many autoplay bets were initially chosen or how many remain; and

d) If the autoplay mode supports player options, these options should default to the manual mode of the game.

5.9.3 Tournament Mode

Tournament mode allows a player to engage in competitive play against other players in an organized and measured event. Play during tournament mode may be either revenue or non-revenue. If the game supports a specific tournament mode, which is independent of normal play, the following requirements apply:

a) All rules within the "Competitions/Tournaments" section of the approved Technical Standards III are displayed to the player;

b) The player has the option to enter or not. If when opting in, the player may complete his non-tournament play before entering tournament play mode, unless the Technology Platform supports simultaneous tournament and non-tournament play modes;

c) A visible message is displayed in the game informing the player that he is operating in tournament mode;

d) For non-revenue tournaments, the game does not accept real money from any source, nor does it pay real money in any way. Tournament mode uses tournament-specific credits, points or tokens that have no cash value;

e) For time-based tournaments, a timer is displayed to players to indicate the remaining period of play. If a tournament is based on an extended duration of play or is initiated or concluded based on the occurrence of a specific event, this information is disclosed to the players;

f) At the end of the tournament, player rankings are displayed and winners are notified;

g) When exiting tournament mode, the game returns to the original state it was in before entering tournament mode; and

h) Any tournament-specific game meters displayed to the player in the game are automatically cleared when the player exits tournament mode.

5.10 Games with Ability/Skill

A game with skill/skill contains one or more elements in its design that can be leveraged by a player to make an impact on the return percentage. Skill/Skill means the player's human attributes such as knowledge, skill/skill, visual recognition, logic, memory, reaction, strength, agility, athleticism, hand-eye coordination, lexical and/or numerical ability, or any other skill or specialty relevant to the game.

5.10.1 Deployments for Games with skill/skill

A game of skill must comply with the applicable display requirements found in the "Game Information and Game Rules", "Information to be Displayed", and "Fair Play Requirements" sections of this Technical Standard. In addition, any skill/skill game, other than traditional casino games (poker, blackjack, etc.), must clearly indicate that the outcome is affected by the skill/skill of the player. This information is visibly displayed in the game before the player chooses his or her intention to wager.

5.10.2 Virtual Opponent

A game with skill/skill can offer a player the opportunity to compete against a virtual opponent as long as the Technology Platform:

a) Communicate in a timely manner that a virtual opponent is participating; and
b) Prevents the virtual opponent from using privileged information of the live player in making a decision, unless the player is instructed otherwise.

5.10.3 Ability/Skill Games Results

Unless otherwise indicated to the player, once a game of skill/skill is initiated, no game function related to the outcome of the game shall be altered during play. In addition, in the event of paytables becoming available, or changes to the game rules between games, notice of the change shall be displayed to the player via the game artwork and adequate information shall be provided so that a player can make an informed decision. An example of the latter case may be the use of an identifier to change the paytables available to the player during the course of the game.

5.10.4 Odds for Ability/Skill Based Awards

If the highest advertised prize is a skill-based prize, it is available to be achieved by a player. If this skill-based prize incorporates an element of chance, the chance of achieving the prize must comply with the "Odds" section specified in this Technical Standard.

5.10.5 Player Advisor Modality

A game with skill may have a mode that offers advice, hints, or suggestions to the player. A game with skill/skill may have a mode that offers advice to the player as long as it conforms to the following requirements:

a) It must be clearly shown to the player that the advisory mode is available, as well as the options available for selection;
b) Any guidance offered to the player to wager must show the cost and benefit of the wager;
c) The guidance to the player should be clear and simple, unambiguous, and should reflect the rules of the game. While the rules of the game may change as a function of the guidance offered, any such changes must be notified to the player prior to accepting the guidance;
d) The game design should prevent access to any source of information, so that data related to the skill element is not readily available through manipulation of the software;
e) The player orientation mode should allow the player the option to accept it, and should not force the player to accept the orientation unless it reflects the only possible option for the player to choose at that time;
f) The availability and content of player guidance should remain unchanged, unless otherwise notified, and should not disadvantage the player.

5.10.6 Player Interaction Devices Used with Ability/Skill Containing Games

If the player interaction devices (joystick, game controllers, camera platforms, sound platforms, motion sensors, image sensors, accelerators, etc.) used by the game in order to implement the skill/skill, then the game with skill must provide adequate and clear instructions for their purpose, use and effect. If there are several player interaction devices capable of affecting the same player action involving skill, then all such options are clearly explained to the player.

5.11 Peer to Peer Games (P2P)

5.11.1 P2P Gaming Sessions

Peer-to-peer (P2P) gaming sessions are environments that offer players the opportunity to play with each other. In these environments, the Holder generally does not participate in the P2P gaming session as a group (home games, etc.), but typically provides the environment for use by its players and may charge a service fee. The following requirements apply:

a) Players should be prevented from occupying more than one position in any P2P gaming session unless authorized by the rules of the game;
b) Players have the option to enter a P2P game session where all players have been randomly selected;
c) Any player playing with house money (shills) or who is a proposition player must be clearly indicated to all other players in that P2P gaming session; and
d) Players receive warnings where the use of bots or other unauthorized player software may affect the game so that they can make an informed decision about whether to participate.

5.11.2 P2P Advantage Function

A P2P game session may contain a feature that allows a player or players to gain an advantage over other players as long as the game is played:

a) Clearly describe to all players that the feature is available and the advantage it offers;
b) Communicates the method for obtaining the function, including any required wager; and
c) It provides players with sufficient information to make an informed decision, prior to the game, as to whether or not to compete against other players who may possess such a feature.

5.11.3 Out-of-Game Status

The Technology Platform may support an "Out of Game" status that may be activated at the player's request or at a period of inactivity, which is disclosed to the player and is less than or equal to the period of inactivity specified in the "Player Inactivity" of this Technical Standard. This status is fully described in the help screens or in the applicable game rules.

a) The player is informed when the "Out of Game" status is activated.
b) The "Out of Game" status does not allow any moves and causes the player's turn to be skipped.

automatically during any game round that takes place while in this state.

c) If the "Out of Game" status is activated in the middle of a game, that game is treated as an interrupted game and meets the requirements of the "Termination of Suspended Games" section.

d) If a player performs any confidential game actions while in an "Out of Game" state (selecting an amount to wager, etc.), the state is removed and the player is enrolled in the next game. Non-confidential game actions, such as accessing the help menu, do not require this status to be removed.

e) If a player has been in "Out of Game" status for more than the period of time disclosed to the player, the player is automatically removed from the P2P game session in which he/she is currently enrolled.

5.12 Persistence Games

A persistency game is associated with a unique attribute (player ID, paytable or game ID, etc.) and incorporates features that enable progression to a prize with game enhancements and/or bonuses through the achievement of some designated game outcome. These additional offerings are available to the player when specific limits associated with the game have been achieved. Achievement of a design outcome allows for advancement in the persistence levels of the game. Multiple playthroughs of a game are usually necessary to activate the persistence award.

5.12.1 Persistence Game Limits

A persistence game should recognize a particular identifier for the purpose of restoring previously acquired limits associated with that identifier on each subsequent visit to a game. A persistence game should contain in its help screens, a clear description of each related persistence modality and/or function, and the requirements of reaching the game's persistence limits, as well as related information on how the player restores previously acquired limits. In addition, players should be notified each time a game persistence limit has been reached.

5.12.2 Playing from a Saved Point

Playing from a save point is a modality used in some persistence game designs where complexity is increased, or additional elements are added to the game as the game continues. In addition, playing from a save point allows the player to save a persistence game at critical points (i.e., save points), typically after completing some achievement or goal. The player can resume play from that point at a later date and continue on to the next goal. The following requirements apply to playing from a save point:

a) Prizes awarded or made available for reaching a save point must be clearly defined and displayed to the player before any wager is placed. If a random type prize can be won, the details and all possible payouts must be shown to the player;

b) The game shall provide an appropriate notification to the player whenever a designed save point is reached during the game;

c) If game rules or rewards change as different levels are reached during game activity from a save point, these changes must be clearly displayed to the player, and

d) If a game from a save position is not maintained indefinitely, then the game must provide an indication to the player of any limitations and/or expiration of the save data that is stored for use in a game at a later time period.

5.13 Progressive systems (Incremental Progressive Jackpot)

This section applies to progressive systems that increase, depending on the game, as follows:

a) Progressive jackpots increase according to the credits wagered in the game.

b) Incremental progressive jackpots behave identically as the progressive jackpot, except that they increase based on the occurrence of one or more specific conditions (defined events) established by the game rules instead of, or in addition to, increases based on credits wagered.

This section does not apply to restricted bonus credit prizes, bonus, which offer prizes that may increase in a single game cycle or, static prizes whose odds of triggering change as the game unfolds. This section also does not apply to persistence game features that increase as the game is played (number of free games, multipliers, multiple achievements towards triggering a bonus, or issuing a prize, etc.) or static prize "tiers" available to be won based on player experience and/or achievements.

5.13.1 Progressive Systems Screen

The progressive system display is used to indicate the current progressive jackpot amount or the "payout" of each prize in credits or local currency format to all players who are participating in a game that can potentially trigger the progressive jackpot. If the progressive system offers a "mystery attraction", i.e., the actual reward is not shown to the player, the "Mystery Prizes" detailed in 5.8.6 of this Technical Standard apply.

a) As the games progress, the current amount for each progressive jackpot is updated on the progressive system screen at least every thirty minutes.
(30) seconds from the incremental play event to reasonably reflect the actual payout amount. The use of the odometer and other "step" update screens is permitted.

b) When the progressive system screen has a maximum display limitation, that is, it can only display a certain number of digits, it is required that the maximum payout limit or "upper limit" must meet the requirements for "as a consequence of the verification of a winning play, to be exchanged for money, in whole or in part, at the sole will of the player".

5.13.2 Maximum Payment Limits

If a maximum payout limit or "upper limit" is supported by the progressive jackpot, once the payout reaches its upper limit, it remains at that value until a winning play or combination is verified and the player is paid out.

a) The Holder must inform MINCETUR of any additional contribution that constitutes an excess or a deviation scheme of the progressive jackpot, in which case it must indicate where they were diverted, in accordance with the provisions of section 5.13.4 of this technical standard.

b) When the player is shown the artwork, the amount of the upper limit indicated must be accurate.

5.13.3 Linked Probabilities

In the event the player is notified of progressive jackpots linked to multiple game themes, the probability of winning such jackpot will be proportional to the player's monetary stake.

For this requirement, a variation of no more than five percent (5%) probability and no more than one percent (1%) tolerance in the calculation of theoretical expected return percentage is accepted.

5.13.4 Progressive Jackpot Deviation

A progressive jackpot diversion scheme may be used, where a portion of the progressive jackpot contributions are diverted to another pool for the resetting of the next progressive jackpot or to be used as set forth in the progressive system design, such as the simultaneous payment of such jackpots.

a) A progressive jackpot diversion scheme can be implemented so that it does not have a mathematical expectation of infinity.
b) Diversion funds are not truncated. Diverted contributions will be counted once the progressive jackpot pool has reached its upper limit.
c) When a diversion fund is used to fund the reset value of a progressive jackpot, the reset value assumes an empty diversion fund for purposes of the theoretical return percentage calculations.

5.13.5 Progressive Jackpot

The progressive jackpot can be awarded based on winning symbols, or by other criteria. When a progressive jackpot is triggered:

a) The player is informed at the end of the game of the amount of the prize and its payment.
b) Contributions to the progressive jackpot are not forfeited. Progressive jackpot payments, when awarded, are not rounded or truncated, unless transferred to the reset amount.
c) When in use, the progressive jackpot payout can be added to the player's credit meter if:

i. The credit counter is maintained in the format of the amount in currency (Soles, US Dollars or other currency);
ii. The progressive jackpot payment is increased by full credit amounts; or
iii. The progressive jackpot payout in the format of the local currency amount is properly converted into credits upon transfer to the credit meter in a manner that does not mislead the player.

d) The progressive jackpot payout is updated to the reset value and continues with normal operations.

5.13.6 Progressive Jackpot Level Swapping

In progressive jackpots that offer multiple prize levels, when the player obtains a winning combination, out of more winning combinations available in the paytable, the highest possible value should always be paid to the player, unless explicitly defined in the game rules.

5.13.7 Progressive Jackpot Triggered by Mystery Prize

To determine when the progressive jackpot triggered by a mystery prize that has a hidden trigger amount is awarded, it must be considered:

a) The hidden active amount is set randomly at each progressive jackpot reset and remains hidden at all times; and
b) It is not possible to obtain access to or knowledge of the hidden asset amount.

5.13.8 Multi-Player Progressive Jackpot Triggers

The Technology Platform is designed to accurately identify and record the order of the triggers when several players activate it at almost the same time, so that the total amount of the payout shown can be awarded to the winning player who activated it first. When this is not possible, or if several players activate it at the same time, it shall:

a) To deliver to each winning player the full amount of the payment shown; or
b) Communicate to the player the precise information on how the Progressive Jackpot is distributed.

5.13.9 Changes to the progressive jackpot parameters

When a progressive system is in use and received contributions based on player wagers, the modification of the progressive jackpot or the increase of the progressive jackpot parameter values must comply with the following requirements:

a) When the rate or factor of increase of the progressive jackpot is configurable and affects the percentage of theoretical return to the public or to the gaming programs, the changes made shall not come into operation until the progressive jackpot is awarded.
b) When the progressive jackpot presents a configurable maximum limit independent of the percentage of return to the public and of the game programs, the changes to the maximum limit may only be of a higher value than the current prize. In the event that a lower value is configured than the current progressive jackpot, the excess resulting from this reduction must be part of a new progressive jackpot. This new configuration of a lower value must be communicated to MINCETUR as established in article 39 of the Regulation.
c) Changes in the parameters should not affect the odds of being awarded the current progressive jackpot;
d) For an active mystery prize, whose winning progressive jackpot is based on a hidden active amount, the following must be taken into account:

i. The awarding of the prize must maintain its randomness, even if any parameter that may influence the result of the awarding of the prize is modified;
ii. The selected hidden active amount must be in the range of the current award up to the maximum limit and the award must not be surrendered as a result of the modification.

5.13.10 Modifications to the progressive jackpot

The Technology Platform must have a secure mechanism that allows:

a) The total or partial transfer of inactive progressive jackpot contributions (and any overflow or diversion of specific progressive jackpot funds);
b) Correct progressive jackpot errors; and
c) Any other modification requested by MINCETUR.

5.14. Game Memory

5.14.1 Game Memory Retrieval

A 'game memory' function is provided to the player, either as a reenactment or by description. The 'game memory' function clearly indicates that it is a replay of the previous game.

5.14.2 Information Required from the Latest Games

Game memory must consist of graphics, text, video content, or some combination of these options, or other media, as long as a complete and accurate reconstruction of the game outcome and/or player actions is possible. It is permissible to display currency values in lieu of credits. The game history must display the following information, as appropriate:

a) Date and time the game was played;
b) The denomination played in the game, if it is a multiple denomination type game;
c) The screen associated with the final result of the game, either graphically or through a clear textual description;
d) The funds available for wagering at the beginning of the game and/or at the end of the game;
e) Total amount wagered, including bonus credits;
f) Total amount earned, including:

i. Any bonus credits and/or awards;
ii. Any progressive jackpot and/or incremental progressive jackpot;

g) Any non-wagered money that has been paid into the gaming account between the beginning and the end of the game;
h) The results of any player option involved in the outcome of the game;
i) The results of any intermediate game phase, such as doubling/risking or bonus games;
j) If a progressive jackpot and/or incremental progressive jackpot was won, an indication that the progressive jackpot was awarded; and
k) Any "player advice" offered to the player for games of skill.

5.14.3 Bonus Game Memory

The game memory must reflect at least the last fifty (50) events of the completed bonus games. If a bonus game consists of 'x number of events', each with separate outcomes, each of the 'x events', up to fifty, must be displayed with its corresponding outcome regardless of whether the outcome was a loss or win.

5.15 Deactivation Requirements

5.15.1 Game Disabled

When the Technology Platform disables a game or game activity while a game is in progress, all players playing that game are allowed to conclude play in their current game. Once the game has completely concluded, it is no longer accessible to a player.

5.15.2 Progressive Jackpot Disabled

For the cases in which a progressive jackpot or incremental progressive jackpot is disabled, either due to Holder intervention, error condition, time limit has expired, among others, the following conditions must be applied:

a) An indication is shown when the progressive jackpot is not available;
b) It is not possible for the progressive jackpot to be increased or won while disabled; and
c) After the resumption of the progressive jackpot, it is possible to reinstate the progressive jackpot with the same parameters as before the disabling, including the payout. The hidden triggered amount, if used to determine the progressive jackpot value for a mystery triggered progressive jackpot, will only be used to determine the progressive jackpot value for a mystery triggered progressive jackpot.

can be re-selected, if the selected amount is in the range of the current payment up to the upper limit.

5.16 Suspended Games

5.16.1 Games suspended

A game is considered suspended when the outcome of the game remains unresolved or the result cannot be properly transmitted to the player. Suspended games may result from the following:

a) Loss of communications between the Technology Platform and the gaming environment;
b) Restart of the Technological Platform;
c) Restarting or malfunctioning of a game medium;
d) Abnormal termination of the player's software; or
e) A command to disable the Technology Platform game.

5.16.2 Betting on Suspended Games

Bets associated with a suspended game that may continue are held on the Technology Platform until the game is completed. Player accounts reflect funds held in suspended games.

5.16.3 Completion of Suspended Games

The Technology Platform provides a mechanism for a player to complete a suspended game. A suspended game is resolved before a player can participate in another instance of the same game.

a) When player input is not required to complete the game, it is acceptable for the game to revert to a game completion state, provided that the game history and credit meter or game account balance reflect a completed game.
b) For single player games, where player input is required to complete the game, the game returns the player to the game state immediately prior to the interruption and allows the player to complete the game, unless there are rules and/or terms that supersede the game. The conditions for game recovery are disclosed to the player.
c) For multiplayer games, where player input is required to complete the game and the player is unable to complete an action required to allow a game to continue within the allotted time:

i. The Technology Platform completes the game on behalf of the player in accordance with the rules and/or terms and conditions of the game;
ii. The game history and credit meters or game account balances are updated accordingly;
iii. Game results are available to the player and indicate what decisions, if any, were made by the Technology Platform on behalf of the player; and
iv. The Technology Platform is designed so that a player who does not complete an action in the required time does not affect any other player in the same game session with respect to completing the game and being credited for what is won or lost.

5.17 Live Game Requirements

If the Technology Platforms support live casino games conducted by a gaming assistant (dealer or croupier, etc.) or in a live gaming environment, they must comply with the following requirements:

a) All players can see the whole process through remote audio and video transmission in real time. The transmission is done through a secure communication channel or other technology, and a graphical interface.

b) The Technology Platform can receive instructions from each player through the player interface or other communication channel to facilitate player decisions when necessary.

c) In addition to the requirements contained in this section, the Registrant or third party service provider maintaining these components, services and/or applications must comply with the operating procedures and controls outlined in the "Live Gaming Services" section contained in the approved Technical Standards.

Licensees must apply to MINCETUR for authorization to conduct live games.

5.17.1 Live Game Information

A live game must comply with the display requirements described in the "Game Information and Game Rules", "Information to be Displayed" and "Fair Play Requirements" sections of this Technical Standard. In addition, the following display requirements must apply:

a) The Technology Platform provides the player with the following information:

i. Description of the procedures established to deal with live game interruptions caused by discontinuity of data, video and voice flow from the network server during a game (interruption of the internet connection, malfunction of the simulcast control server, etc.);
ii. How errors are resolved in the possibility of human error by the game wizard and Technology Platform error by the specialized device; and
iii. Identifies any relationship between the player's wager through the Technology Platform and what is shown in the video (player's physical chips and their values).

b) The Technology Platform must not provide real-time information from the live game that would allow the player to gain an advantage:

i. Projecting or predicting the outcome of a game;
ii. For card games, tracking of cards played and cards remaining to play;
iii. Analyze the probability of a game-related event occurring; or
iv. Analyzing the strategy for the game or betting on a game, unless permitted by the rules of the game.

c) Players of any live game that relies on the monitoring of a 'live' event (roulette, bingo or similar) are informed that "live" transmissions may be subject to delay or interruption. When a delay is evident or created by the Technology Platform, the player is shown the extent of the delay.

5.17.2 Player Fairness in Live Gaming

The following rules apply when players participate in games through the Technology Platform with face-to-face players, who are playing in real time in a physical establishment:

a) The rules, artwork and functionality of the live game, as made available to the player through the Technology Platform, must be the same information as that made available to a player in person, where applicable; and
b) Players who play through a Technology Platform have the same probability of winning a game as players who participate in face-to-face games.

5.17.3 Game Result Data

The game result data refers to any result generated or detected by devices

The data of the game result is transmitted to the player immediately after its generation or detection (subject to natural limitations of live game processing and delays in Internet communication). Game outcome data is transmitted to the player immediately upon its generation or detection (subject to the natural limitations of platform processing and Internet communication delays). It is permitted that game result data may be automatically recorded by specialized devices, provided that the software used for automatic recognition complies with:

a) Ensure a high degree of accuracy in identifying and reporting game outcome data to the Technology Platform and that game rules are programmed into the Technology Platform;
b) Do not provide any information that could be used to compromise the device and its components (cards contained in the current deck or dealer);
c) Do not interfere with or modify the behavior of the device beyond the functionality associated with that software; and
d) Include a manual operation mode to allow corrections of an erroneous result (the device misreads a card, the ball position is incorrect, etc.) if such corrections are not made directly on the Technology Platform. The player must know that the manual operation mode is being used.

5.17.4 Physical Randomness Devices

Live games may use physical randomness devices, as described in the "Mechanical GNA (Physical Randomness Devices)" section, and must meet the following requirements to generate game results:

a) The results of the physical randomness device are digitized into the game results data and securely transmitted to the Technology Platform via specialized devices for processing without modification.
b) The Technology Platform records game result data and makes it available to the player for review immediately upon generation (subject to the natural limitations of platform processing and network communication delays).
c) Except for human error or a manually correctable error, at any time during the game, the game outcome data matches the outcome generated by the physical randomness device. When there is a discrepancy between the physical randomness device and the game outcome data, the outcome of the physical randomness device is considered correct.

TECHNICAL STANDARDS II
FOR REMOTE SPORTS BETTING TECHNOLOGY PLATFORMS

Section 6. Evaluation and Technical Testing of Technology Platforms

The Technological Platform for remote sports betting, progressive systems, integration between platforms, game modalities, among other components and services, prior to its authorization and registration (homologation) must undergo a technical evaluation by a Certification Laboratory authorized by MINCETUR.

The Remote Sports Betting Technology Platform Holder, as well as the linked service providers are responsible for all costs associated with testing and obtaining the certificate of compliance. To that end:

a) The Authorized Certification Laboratory must have access to the source code of the Technology Platform software, progressive systems, integration between platforms, game modes, among other components and services, as well as the means to verify the compilation of the source code. The result of the compiled source code must be identical to that of the software submitted for evaluation.

b) In order for the authorized Certification Laboratory to issue the respective certificate of compliance, the Technological Platform for remote sports betting, progressive systems, integration between Technological Platforms, game modalities, among other components and services, must comply at least with the technical specifications established in these Regulations and their respective approved Technical Standards, as well as with the established mandatory Directives.

c) For the approval of an authorization for the operation of Remote Sports Betting Technological Platforms, the Licensee must submit to MINCETUR, the description of the change management processes detailing the evaluation procedures to identify the criticality of the updates and determine the updates that must be submitted to the authorized Certification Laboratory for review and certification. These change management processes must be:

i. Communicated to MINCETUR prior to implementation; and

ii. Audited at least once (01) a year by an authorized Certification Laboratory or by an independent area, not directly related to the operation of remote gaming and/or remote sports betting of the Holder, acting as external auditor.

Section 7. Integration with the Technological Platforms

a) The Holder is responsible for remote sports bets made through its related service providers.

b) The servers and other equipment of the service providers are considered, for the purposes of these Regulations, as part of the Technological Platform, and the Contractor shall be responsible for ensuring compliance with the technical specifications set forth in these Regulations and their respective approved Technical Standards, as well as with the mandatory Directives.

c) The Contractor must ensure that any integration with the servers and other equipment of a Technology Platform is carried out in a manner that complies with the specifications set forth in these Regulations and their respective approved Technical Standards, as well as those established in mandatory Directives.

d) An authorized Certification Laboratory must perform integration and certification tests of each server and other equipment with the Licensee's Technology Platform, prior to its implementation and authorization by MINCETUR. For example, integration and certification tests must be performed between the remote sports betting servers and the Technological Platform, as well as between the payment processing and the Technological Platform. Remote sports betting servers should be understood as the hardware and software that drives the features common to remote sports betting offers, remote sports betting configurations, the Random Number Generator (RNG), reports, reports, etc.

Section 8. Technology Platform Requirements

The Technological Platform may be made up of multiple Technological Platforms installed in one or several data centers. The Technological Platform, as well as the communication between its components must guarantee the adequate operation and integration of its components and services, and have high availability connections and access and information security controls. Likewise, they must comply with all the technical requirements contained in the approved Technical Standards II and III.

8.1 Technology Platform Clock Requirements

8.1.1 Technology Platform Clock

The Technology Platform including its components, services, applications and computer media must be synchronized with a single clock that reflects the current date (dd/mm/yyyy) and time (hh/mm/ss), which is used for:

a) The record of all transactions, games and events;
b) Recording of significant data and events;
c) Report generation; and
d) Transmission of economic and technical data to MINCETUR's Data Center.

8.1.2 Time synchronization

The Technology Platform must have a mechanism to ensure that the date and time is the same (synchronized and configured) in all its components, applications and computer media. The Technology Platform must be synchronized with the official Peruvian time GMT-5, for the registration of all transactions and occurrences, as well as for the generation of reports.

8.2 Control program requirements

In addition to the requirements contained in this section, the requirements contained in the "Verification Procedures" section of the approved Technical Standards III must also be complied with.

8.2.1 Automatic verification of the control program

The Technology Platform must have a self-diagnosis method, which at least every 24 hours, verifies and authenticates that all the components of the critical control programs or critical files that may affect gaming operations (executables, libraries, Technology Platform or sports betting configuration, operating system files, components that control the required reports of the Technology Platform, and the database elements that may affect the Technology Platform operations) are identical to those evaluated and approved by the authorized certification laboratory that performed the corresponding technical evaluation.

Likewise, by means of user and password, the Holder, MINCETUR or the entity authorized by MINCETUR, may audit by means of remote or on-site access the Technological Platform, applications, software, services, databases, critical components and critical control programs.

The authentication method for control programs or files rated as critical must:

a) Use a hash algorithm that generates a message digest of at least 160 bits (40 digits). If other algorithms or methodologies are used, the authorized Certification Laboratory shall evaluate them and authorize their use, if applicable; and

b) Generate and display an authentication error message when any critical component of the control program is determined to be invalid.

8.2.2 Independent verification of the control program

a) The hashing algorithm used for the verification of each component of the critical control program or critical file must meet the following requirements:

i. Minimum of 160 bits (40 digits)

ii. Allow its use from a personal computer. You can also use installation media such as; USB, DVD or CD or other similar media.

b) If the hash algorithm used is owned by the authorized Certification Laboratory, a copy must be provided at MINCETUR's request, free of charge, attaching its operation manual, operation or use, as well as the information corresponding to any update of the algorithm.

c) For the purposes of this Regulation, the SHA-1 Algorithm is considered approved ex officio by MINCETUR as a means of verification of the control program or other components, software, applications, database model. Any other algorithm to be used for such purpose must comply with the provisions of paragraph a) of 8.2.2. of this Technical Standard.

d) The impossibility of determining the electronic fingerprint (digital signature) does not lead to deny the authorization and registration of a Technology Platform. When, due to the nature of the storage medium, it is not possible to determine an electronic fingerprint, the authorized Certification Laboratory must state this fact in the respective Certificate of Compliance and indicate the reasons why such electronic fingerprint cannot be generated; it shall also indicate the control mechanism to be used to ensure the integrity of each component of the critical control program of the Technology Platform or other components, software, applications, database model.

e) Together with the submission of the request for authorization and registration (homologation) of the Technology Platform, the Technology Platform Holder provides any adapter, device or special interface used for reading the electronic fingerprint. Likewise, in case of updates of the authorized and registered (homologated) Technological Platforms, the authorized Certification Laboratories and the Technological Platform Holder must comply with submitting to MINCETUR the adapter, device or special interface, if applicable. Such delivery must be free of charge for MINCETUR.

8.3 Bet Management

8.3.1 Bet Management

The Technology Platform must have a secure mechanism that allows the Registrant to interrupt through the use of username and password or other secure method the following:

a) All gambling activities;
b) Event or individual market;
c) Access to each player's session; and
d) Betting Terminal, if applicable;

The Technology Platform must keep a record that identifies the time (hh/mm/ss), date (dd/mm/yyyy), and description of the interruption.

8.4 Player account management

The Technology Platform must have a method that allows each player to register his or her data, creating a user account and a game account, which are associated and must comply with the requirements contained in the section "Game Account Controls" contained in the approved Technical Standards III.

8.4.1 Registration and verification

For the creation of the game account on the Technology Platform, the player must first register his personal data. The process of registration of personal data and verification of the user account, as well as the game account must be supported directly by the Technology Platform or through the software of a related service provider, and must comply with the following requirements:

a) To create a game account in the Technological Platform, the player must register at least the following data:

i. Full name(s) and last name(s);
ii. Type of identity document
iii. Identity card number;
iv. Date of birth;
v. Nationality;
vi. Address (address, district, province and department);
vii. Sworn statement regarding their status as Politically Exposed Person (PEP), in accordance with the regulations in force, if applicable.

b) Only persons of legal age (18 years or older) may register and access a user account and game account. During the registration process the player must be informed of the following:

i. You cannot access a gaming account if you are validated as a minor according to your date of birth.
ii. You cannot access a user account and a game account without completing the required fields of the electronic registration form.
iii. You must accept the terms and conditions, as well as the privacy policy.
iv. That it is forbidden for any person to access or use the game account without authorization and/or in violation of the permitted accesses.
v. That the Registrant and/or MINCETUR may monitor the user account and the gaming account;
vi. That your registered data is validated for the opening of the gaming account; and
vii. A gaming account may not be created if the player is registered in the Registry of Persons Prohibited from Accessing Establishments Intended for the Operation of Casino Games and Slot Machines, under the responsibility of the General Directorate of Casino Games and Slot Machines, or those acting in its stead, under MINCETUR.

c) The Holders must restrict the bets of individuals in remote sports betting games until the validation process of the information and data registered is concluded:

i. Verification of the person's identity must include at a minimum, first name(s), last name(s), type of identity document, identity document number, age and nationality;
ii. The verification of the identity of the person must also verify that the player is not registered in any exclusion list of the Technological Platform and registered in the Registry of Persons Prohibited from Accessing Establishments Intended for the Operation of Casino Games and Slot Machines, in charge of the General Directorate of Casino Games and Slot Machines, or those acting in its stead, under the MINCETUR; or prohibited from establishing or maintaining a player account for any other reason;
iii. The individual's identity verification data must be recorded and stored in a secure manner, in compliance with the Personal Data Protection Act; and
iv. The user account data must be kept during the period of validity of the user account, such period being computed from the authorization granted by MINCETUR to the Holder and during the five (5) years following its cancellation or annulment, or during the statute of limitations period for the Remote Gaming and Remote Sports Betting Tax as provided for in the Tax Code, whichever is greater.

d) The gaming account is blocked when the verification of the identity of the person is unsuccessful or it is determined that the player is registered in any exclusion list, or registered in the Registry of Persons Prohibited from Accessing Establishments Intended for the Operation of Casino Games and Slot Machines, in charge of the General Directorate of Casino Games and Slot Machines, or those in its stead, dependent upon the General Directorate of Casino Games and Slot Machines, or those in its stead, dependent upon the General Directorate of Casino Games and Slot Machines.

MINCETUR and the player has accepted the terms, conditions and privacy policies.

e) A player can have only one active user account and game account per Cardholder.

f) The Technology Platform must have the capability to update per player authentication credentials, person identity record information, and the player account used for financial transactions. Multi-factor authentication may be used for this purpose; and

g) The user account and the game account created in the Technological Platform are considered personal and non-transferable, as well as the funds associated with them.

8.4.2 Player access

The player must access his game account through username and password (authentication credentials) or through another secure authentication method approved by the authorized Certification Laboratory. The Technology Platform may present more than one authentication method for the player to access his/her gaming account.

a) If the Technology Platform does not recognize the authentication credentials entered, an informative message is displayed to the player requiring the credentials to be re-entered. The message is always the same as long as incorrect authentication credentials are entered.

b) When the player forgets his authentication credentials, a multi-factor validation process is used to recover or restore his credentials.

c) Current game account balance information, including any bonus credits, and transaction options must be available to the player upon authentication. All restricted bonus credits and bonus credits that have a stated expiration are detailed separately.

d) The Technology Platform must have a mechanism that allows a gaming account to be blocked when suspicious activity is detected, such as three (3) consecutive failed login attempts within a thirty (30) minute period. A multi-factor authentication process must be used to unlock the game account.

e) Authentication credentials must be at least eight (8) characters long according to the security measures determined by the Holder.

8.4.3 Player inactivity

After thirty (30) minutes of inactivity in the game environment, the player must re-authenticate to access his/her game account.

a) No gaming or financial transactions are allowed in the Gaming Environment until the player re-authenticates.

b) The player may be offered a simpler method to re-authenticate to the Gaming Environment, such as, authentication at the operating system level (biometrics) or a personal identification number (PIN). Each re-authentication method must be evaluated and approved by the authorized Certification Laboratory:

i. This functionality can be disabled according to the player's preference.

ii. Once every thirty (30) days the player is required to complete authentication of the Game Media.

8.4.4 Limitations and exclusions

The Technological Platform must have the capacity to correctly implement any limitation and/or exclusion established by the player and/or Holder, and in accordance with the Registers established by MINCETUR:

a) The Technology Platform must comply with allowing and managing limitations and/or exclusions, complying with the requirements established in the "Limitations" and "Exclusions" section contained in the approved Technical Standards III.

b) Limitations established by the player do not override more restrictive limitations imposed by the Holder. The more restrictive limitations must take precedence; and

c) Limitations should not be compromised by the status of internal events, as well as self-imposed exclusion orders and revocations.

8.4.5 Financial Transactions

When financial transactions can be performed automatically by the Technology Platform, the following requirements apply:

a) The Technology Platform must support the confirmation or rejection of each financial transaction initiated, including

i. The type of transaction (deposit/withdrawal);

ii. The value of the transaction; and

iii. For declined transactions, a message describing why the transaction was not completed will be displayed.

b) The deposit made by the player to his gaming account is made by means of a transaction of circulating money, debit card, credit card or other means of payment accepted by the Holder, with the exception of cryptocurrency, which produce a proper audit trail.

c) Player funds are not available for play until a confirmation of authorization for their use is received. The authorization number generated as a result of the transaction confirmation is stored in the audit trail.

d) Payments from a gaming account must be sent directly to an account at a financial institution in the player's name, payment method of the player's choice or such other place as the Holder and the player may agree.

e) If a player initiates a transaction in the gaming account that exceeds the limits established by the Holder and/or MINCETUR in these Regulations or in a mandatory Directive, this transaction is processed only up to the maximum limit established, and the player is notified of this situation.

f) Transferring funds between two gaming accounts is not allowed.

8.4.6 Transaction record or gaming account summary

The Technological Platform must have the capacity to generate a record of the transactions or history of the gaming account summary, when required by the player. The information must be available to the player for at least two (02) years, and must include at least the following types of transactions:

a) Financial transactions (unique identification of the transaction with date and time):

i. Deposits to the gaming account;

ii. Withdrawals from the gaming account;

iii. Bonus credits added to/withdrawn from the gaming account;

iv. Adjustment of balances in the gaming account;

v. Any deposit of money to the gaming account without wagering;

vi. Total amount won for entire games, including, any bonus credits and/or prizes, and any progressive jackpot and/or incremental progressive jackpot (if applicable).

vii. Total number of cancellations.

b) Betting transactions:

i. Unique identification number of the bet;
ii. The date and time the bet was placed;
iii. The date and time each event began and ended or when it occurs in the case of future events;
iv. The date and time the bet was settled;
v. All player options included in the wager, including market line and odds, wager selection, and any special condition(s) applicable to the wager;
vi. The results of the bet;
vii. Total amount wagered, including any bonus credits;
viii. Total amount paid, including any bonus credits, and any progressive jackpot and/or incremental progressive jackpot.
ix. The date and time the prize was paid to the player.
x. Total number of cancellations.

8.4.7 Player loyalty programs

Player loyalty programs are those that allow the delivery of bonuses to players based on the volume of play or revenue received from a player. If the Technology Platform features player loyalty programs, it must comply with the following:

a) All prizes, on an equitable basis, are available to those players who reach the qualifying level defined for player loyalty points;
b) The redemption of player loyalty points earned must be a secure transaction that automatically adds the value of the redeemed award to the points balance; and
c) All player loyalty point transactions must be recorded by the Technology Platform in the gaming account.

8.5 Player Software

The player software allows the Gaming Media to interact with the Technology Platform, so that the player can participate in sports betting and perform financial transactions. The player software is downloaded and installed on the Gaming Media, run from the Technology Platform, accessed from the Gaming Media or a combination of the two.

8.5.1 Software identification

The player software must have the necessary information to identify the software and its versions.

8.5.2 Software validation

The software for the player installed in the Gaming Media, each time it is loaded for use, and when the Technology Platform supports it, must authenticate that all its critical components are correct. Critical software components may include, but are not limited to, game rules, paytable information, elements that control communications between the Gaming Media and the Technology Platform or other software components that are necessary to ensure the proper functioning of the software. In the event of a failed authentication (program incompatibility or authentication failure), the software prevents gaming operations and displays a clear, simple and unambiguous error message.

Program verification mechanisms are evaluated by the authorized Certification Laboratory on a case-by-case basis, according to the standard security practices of the remote sports betting industry.

8.5.3 Communications

The player software must be designed in such a way that it can only communicate with authorized components via secure communication. If communication between the Technology Platform and the Gaming Medium is lost, the software must prevent further gaming operations and must display a clear, simple and unambiguous error message. It is acceptable for the software to detect this error when the Gaming Medium attempts to communicate with the Technology Platform.

8.5.4 Client-server interactions

The player may engage in sports betting and financial transactions with the Technology Platform by downloading an application or software package containing the software to the player on the Gaming Environment or accessing the software through a browser.

a) The software must not allow players to transfer data between each other, except for chat functions (text, voice, video, etc.) and approved files (user profile pictures, photos, etc.);
b) The software does not automatically disable any virus scanners, detection programs or alter the firewall rules specified by the Gaming Environment to open ports that are blocked by a hardware or software firewall;
c) The software must only access the port (TCP/UDP) that is necessary for communication between the Gaming Media and the Technology Platform server;
d) If the software includes additional functionality unrelated to sports betting, this additional functionality does not alter the integrity of the software in any way;
e) The software must not have the ability to override the volume setting of the Play Medium;
f) The software is not used to store confidential information. Autofill, password storage or other methods that populate the password field must be disabled by default in the software; and
g) The Software does not have any logic used to generate the outcome of any type of game or event. All critical functions, including the generation of any game outcome, are generated by the Technology Platform and are independent of the Gaming Media.

8.5.5 Compatibility check

In the installation or initialization process and before starting a game or event operation, the player software to be used in conjunction with the Technology Platform must have the ability to detect any incompatibilities or resource limitations of the Gaming Environment that prevent the correct operation of the software (software version, non-compliance with minimum specifications, browser type, browser version, plug-in version, etc.). If incompatibilities or resource limitations are detected, the software must prevent game operations and display a clear, simple and unambiguous error message.

8.5.6 Software content

Player software must not contain malicious code or functionality. This includes, and is not limited to, unauthorized file extraction/transfer, unauthorized device modifications, unauthorized access to any locally stored personal information (contacts, calendar, etc.) and malware (malicious program).

8.5.7 Cookies

Where the use of cookies is mandatory for gambling, bets may not be accepted until the player agrees to their use in the game environment. Players must be informed about the use of cookies after installation of the game software or during player registration. All cookies used must not contain malicious code.

8.5.8 Access to information

The player software must have the capability to display directly from the user interface or through a page accessible to the player, the sections detailed below:

a) Game rules and content;
b) Information for the protection of the player;
c) Terms and Conditions; and
d) Privacy policy.

8.5.9 Information in Several Languages

The information provided through the player software must be offered in the English language. When the information available to the player is provided in different languages, the following principles should be applied:

a) Each language option of the same activity must offer the same payout percentages or odds/payouts and prices, as the case may be.
b) When a player chooses to participate in different languages of an activity, he/she should have the same probability of winning, regardless of the language option he/she chooses.
c) Each language variant must be consistent with the information in that variant.
d) All information must be provided in the language specified for that variant.
e) Information should have the same meaning in all languages, so that no variant is favored or disfavored.
f) It is not mandatory to translate common sports betting terms used internationally. In case of including commercial words in a language other than English, they must be included in a glossary available to the player.

8.5.10 The home page of the Holder's website

The Holders must include on the home page of the Technological Platforms of remote sports betting:

a) A link to the MINCETUR Web Portal for registration in the Registry of Persons Prohibited from Accessing Establishments for the Operation of Casino Games and Slot Machines.
b) The phrase "Excessive remote gambling and sports betting may cause compulsive gambling" must be displayed in legible and easily visible characters, in proportion to the rest of the information.

8.6 Information to be maintained

The Holder or the technological platforms of its related service providers must register, store and have a backup of the data and information in this section. In case the information is stored by the related service providers, the Holder is responsible that such information is available to MINCETUR and/or SUNAT.

8.6.1 Data storage and date and time stamping

The Technological Platform must have the capacity to store and have a backup of the data and information registered for a minimum period of five (05) years, counted from the granting of the authorization by MINCETUR to the Holder, or during the period of prescription of the Tax on Remote Gaming and Gambling. Remote Sports Betting as provided in the Tax Code, whichever is greater:

a) The clock should be used in recording all data and events; and
b) It must have a mechanism that allows exporting data to be analyzed, audited and verified, using CSV, XLS or compatible formats.

8.6.2 Bet registration information

In the Technological Platform of the Holder or its related service providers, a backup must be registered, stored and maintained independently for each player and for each game played individually or with multiple players. In case the information is stored by the related service providers, the Holder is responsible for making such information available to MINCETUR. At least the following information must be available:

a) The date and time the bet was placed;
b) Any player option included in the wager:

i. Market line and odds (such as single bet, spread bets, over/under bets, win/place/show);
ii. Bet selection (athlete or team name and number);

c) The results of the bet (blank until confirmed);
d) Total amount wagered, including bonus credits;
e) Total amount earned, including bonus credits
f) The date and time the winning bet was paid to the player;
g) Unique identification number of the bet;
h) If a progressive jackpot and/or incremental progressive jackpot was won, an indication that the jackpot was awarded, if applicable;
i) Contributions to progressive jackpot or incremental progressive jackpot (if applicable);
j) Unique identification of the Betting Terminal that issued the wagering coupon, if applicable;
k) Event and market identifiers;
l) State of the current bet;
m) Unique player identification; and
n) Open text field for the wizard to enter the description of the player or image file, if applicable.

8.6.3 Market information

The Technological Platform must register, store and maintain an independent backup per event and individual market available to place bets, and at least the following information must be available:

a) The date and time the betting period began and ended;
b) The date and time the event started and ended or is scheduled to occur for future events (if known);
c) The date and time the results were confirmed (blank until confirmed);
d) Total amount of bets collected, including all bonus credits;
e) The quota lines that were available throughout the duration of a market (with date and time) and the confirmed result (won/lost/tied);
f) Total amount of prizes paid to players, including all bonus credits;
g) Total amount of cancelled bets, including all bonus credits;
h) Event status (in progress, completed, confirmed, etc.); and

i) Event and market identifiers.

8.6.4 Competition/Tournament Information

The Technology Platform that supports the competition/tournament must record, store and maintain a separate backup for each competition(s)/tournament(s) and at a minimum the following information must be available:

a) Name or identification of the competition/tournament;
b) The date and time the competition/tournament occurred or takes place (if known);
c) Identification of event(s) y participating market(s);
d) For each registered player:

i. Unique player identification;
ii. Total amount for competition/tournament entry fee, including all bonus credits, and the date of collection;
iii. Player ratings/rankings;
iv. Amount of awards paid, including all bonus credits, and the date of payment;

e) Total amount for competition/tournament entry fee, including all bonus credits;
f) Total amount of prizes paid to players, including all bonus credits;
g) Total amount of the service fee, if applicable; and,
h) The current state of the competition/tournament.

8.6.5 Game account information

In the Technological Platform a backup must be registered, stored and maintained independently for each gaming account and at least the following information must be available:

a) Unique player ID and player name (if different);
b) Player's personal identification information, such as:

i. The information collected by the Registrant in the registration of the player and that creates the user account, which includes the first name(s), last name(s), type of identity document, identity document number, age, nationality, telephone number and address;
ii. The player's personal identity must be encrypted, including identity document type and number, authentication credential (password, PIN, etc.) and personal financial information (debit card numbers, credit card numbers, bank account numbers, etc.);

c) The date and method of identity verification, including, where applicable, a description of the identity document provided by a player to confirm his identity;
d) The date the player accepted the Holder's terms and conditions and privacy policy;
e) Account details and current balance, including deposits, awards, bonus credits, balance adjustment and returns. All restricted bonus credits and bonus credits that have an expiration date are recorded separately;
f) The date and time of the cancellation of the bets, as well as the reason for the cancellation.
g) Previous game accounts, if any, and reason for deactivation;
h) The date and method where the account was registered (Gaming Media or Remote Sports Betting Gaming Room);
i) The date and time of entry to the account (player, Holder or MINCETUR), including the IP address;
j) Exclusions/limitations information:

i. The date and time of the request;
ii. Description and reason for exclusion/limitation;
iii. Type of exclusion/limitation (exclusion imposed by the Registrant, self-imposed deposit limitation, among others);
iv. The exclusion/limitation start date
v. The date of exclusion/limitation completed;

k) Financial transaction information:

i. Type of transaction (deposit, withdrawal, balance adjustment, refunds, prizes and the deposit of money to the non-gambling account);
ii. The date and time of the transaction;
iii. Unique transaction identifier;
iv. Transaction amount;
v. Total account balance before/after the transaction;
vi. Total amount of cost per transaction (use of credit card, debit card, etc.), if applicable;
vii. Identification of the user who processed the transaction, if applicable;
viii. Transaction status (pending, complete, etc.);
ix. Deposit/withdrawal method (cash, personal check, cashier's check, wire transfer, debit card, credit card, electronic funds transfer, etc.);
x. Deposit authorization number;

l) The current status of the game account (active, inactive, closed, excluded, etc.).

8.6.6 Bonus information

The Technology Platform that supports bonus awards that may be redeemable in cash, wagering credits, must record, store and support the following information for each bonus award offered, as applicable:

a) Unique identifier of the bonus offer;
b) The date and time the bonus was made available;
c) Current balance for bonuses;
d) Total number of bonuses granted;
e) Total number of bonus awards redeemed;
f) Total number of expired bonuses granted;
g) Total number of bonus adjustments granted;
h) The current status of the bonus; and
i) The date and time the bonus was or is scheduled to be terminated (blank until known).

8.6.7 Progressive jackpot and incremental progressive jackpot information

The Technology Platform that supports the progressive jackpot or incremental progressive jackpot must record, store and support the following information for each progressive jackpot offered, as applicable:

a) Unique identification of the progressive jackpot;
b) The date and time the progressive jackpot became available;
c) Identification of the game modality;
d) Unique identifier(s) of player(s), if the progressive jackpot is linked to a player(s);
e) Current value of the progressive jackpot;
f) Any other jackpots containing progressive jackpot contributions, as applicable;

i. Current value of the amount exceeding the limit, as established by MINCETUR in this Regulation or Directive of mandatory compliance;
ii. Current value of the progressive jackpot diversion scheme (diversion fund);

g) Reset value of the current progressive jackpot if different from the initial value (reset value);

h) When parameters are configurable after initial configuration, the following information must be recorded, stored and backed up:

i. Initial value of the progressive jackpot;
ii. Percentage rate of increase;
iii. Limit value of the progressive jackpot;
iv. Percentage rate of increase after reaching the maximum;
v. Percentage rate of increase for the diversion fund;
vi. Limit value of the diversion fund;
vii. The odds of triggering the progressive jackpot;
viii. Any parameter that indicates the time periods in which the progressive jackpot is available for a trigger;
ix. Any additional information to reconcile the progressive jackpot properly;

i) The current status of the progressive jackpot; and

j) The date and time the progressive jackpot was or is scheduled to be paid.

8.6.8 Gaming Terminal Information

The Technology Platform must record, store and maintain an independent backup for each gaming account with respect to the transactions made in the betting terminal and, as a minimum, must record the following information:

a) Unique identification of the Betting Terminal;
b) Identification of the user and information of the session carried out in the Betting Terminal;
c) Record of bets placed;
d) Record of winning bet payments; and
e) Registration of cancelled bets;

8.6.9 Significant event information

The Holder or the technological platforms of its related service providers must record, store and permanently have a backup of the information of significant events. In case, the information is stored by the related service providers, the Holder is responsible that such information is available to MINCETUR and/or SUNAT, as appropriate:

a) Unsuccessful attempts to access the game account or the Cardholder's account, including the IP address;
b) Authentication error or discrepancy;
c) Significant periods of unavailability of any critical component of the Technology Platform (any period of time that the game is stopped for all players, and/or transactions cannot be successfully completed for any user);
d) Major prizes (unique and aggregated in a defined period of time) that exceed the values that may be established in these Regulations and mandatory Directives, including the information of the game played;
e) Major wagers (single and aggregated in a defined period of time) that exceed the values that may be established in these Regulations and mandatory Directives, including the information of the game played;
f) Cancellations and adjustments of balances of the Technology Platform;
g) Changes in live data files occurring outside the normal execution of the program and Technology Platform;
h) Changes made to the data download library, including the addition, change or deletion of software, if applicable;
i) Changes in policies and parameters for Technology Platforms, databases, networks and applications (audit settings, password complexity settings, Technology Platform security levels, manual database updates, etc.);
j) Date/time changes on the main server;
k) Changes in the criteria previously established for an event or market (does not include changes in the quota line for active markets);
l) Changes in the results of an event or market;
m) Changes in the parameters of the progressive jackpot or progressive jackpot increase;
n) Changes in the bonus parameters (startup/ purpose, value, eligibility, restrictions, etc.);
o) Gaming account management:

i. Gaming account balance adjustments;
ii. Changes made to the player's personal identity information and other confidential information recorded in a game account/user account;
iii. Deactivation of a game account;
iv. Major financial transactions (unique and aggregated in a defined period of time) that exceed the values that may be established by these Regulations and Directives of mandatory compliance, including the information of the transaction;
v. Negative balance of the gaming account (due to balance adjustments);

p) Loss without recovery of the player's personal identity information and other confidential information;
q) Any other activity that requires the user's intervention and that occurs outside the normal scope of the Registrant; and
r) Other significant or unusual events that may be specified in mandatory Directives.

8.6.10 Holder Access Information

The Technological Platform must register, store and maintain a backup independently for each account of the Holder that allows access to the Technological Platform and at least the following information must be registered:

a) Name of the employee of the Holder who accessed, as well as his or her position;
b) Identification of the Holder's employee;
c) Complete list and description of the roles and permissions that each Holder account or group can execute;
d) The date and time when the Holder's worker account was created;
e) The date and time of the last access, including the IP address;
f) The date and time of the last password change;
g) The date and time when the Holder's worker account was disabled/deactivated;
h) Members of the Registrant's group or account, if applicable; and
i) The current status of the worker's account (active, inactive, closed, suspended, etc.).

8.7 Reporting requirements

8.7.1 General reporting requirements

The Technological Platform must have the capacity to generate online reports, as required by MINCETUR through a WEB Application or other secure access method using a user name and password, which are provided by the Holder at the request of MINCETUR and SUNAT.

In addition to complying with the provisions of the section "Data storage and date and time stamping", the following reporting requirements apply:

a) The Technology Platform must have the capacity to allow filters to be made on the content of the reports, on a daily, monthly (start and end date) and annual (start and end date) basis, as a minimum;

b) Each required report must contain:

i. Report title;

ii. The company name or corporate name of the Holder and identification code;

iii. Date and time of generation;

iv. The selected period;

v. Identification of the MINCETUR user who requested the report;

vi. An indication of "No activity" or a similar message if no data appear for the specified period;

vii. Labeled fields that must be clearly understood according to their function; and

viii. Ability to be exported to PDF or Excel files.

8.7.2 Holder's income report

The Technological Platform must have the capacity to generate online reports, according to MINCETUR's needs, on the Registrant's income for each event in full and for each individual market in this event. Access is through a WEB Application or other secure access method using a username and password, which are provided by the Holder at the request of MINCETUR and SUNAT:

a) The date and time at which each event began and he concluded;

b) Total amount of wagers collected, including separate amounts for bonus credits;

c) Total amount of prizes paid to players, including separate amounts for bonus credits and/or prizes;

d) Total amount of cancelled bets, including separate amounts for bonus credits;

e) Total amount of commissions per service, if applicable;

f) Event and market identifiers; and

g) Event status (in progress, completed, confirmed, etc.).

8.7.3 Report of the consolidated income of the Holder

The Technological Platform must have the capacity to generate online reports, as required by MINCETUR, on the Holder's consolidated income, as appropriate. Access is through a WEB Application or other secure access method using a username and password, which are provided by the Holder at the request of MINCETUR and SUNAT. The required report must at least allow daily, monthly (start and end date) and annual (start and end date) filters of:

a) Consolidated income generated daily (total bets received, total prize payments, total bonuses, total prizes associated with the progressive system, total cancellations, total refunds, total service fees, registration fees; among others, date and time, identifying the Holder, as well as any other counter necessary for the correct calculation of the daily production) by the Technological Platform, taking into consideration the operations of the day occurring between 00:00:00 hours of a day (start) and 23:59:59 hours of the same day.

b) The search is performed by the registration code granted by MINCETUR to the Holder.

8.7.4 Future events report

The Technological Platform must have the capacity to generate online reports for MINCETUR, on future game day events, as needed. Access is through a WEB Application or other secure access method using username and password, The same that are delivered by the Holder at the request of MINCETUR and SUNAT:

a) Bets placed before the day of play for future events (total and per bet);

b) Bets placed on the day of play for future events (total and per bet);

c) Bets placed before the day of play for events occurring on the same day (total and per bet);

d) Bets placed on the day of play for events occurring on the same day (total and per bet);

e) Bets cancelled on the day of play; and

f) Event and market identifiers.

8.7.5 Report from events events and alterations

The Technological Platform must have the capacity to generate online reports, as required by MINCETUR, on each significant event or alteration. Access to the report is made through a WEB Application or other secure access method using a user name and password, which are provided by the Holder at the request of MINCETUR and SUNAT:

a) The date and time of each significant event or disturbance;

b) Event/component identification;

c) Identification of the user(s) who performed and/or authorized the significant event or alteration;

d) Reason/description of the significant event or alteration, including the data or parameter altered;

e) Value of the data or parameter before the alteration; y

f) Value of the data or parameter after the alteration.

8.7.6 Jackpot Payment Reports (Progressive Systems)

The Technological Platform must have the capacity to generate online reports, according to MINCETUR's needs, on one or more progressive jackpots or incremental progressive jackpots that exceed the value established by MINCETUR. Access to the report is made through a WEB Application or other secure access method using a user name and password, which are provided by the Holder at the request of MINCETUR and SUNAT:

a) Unique identification of the jackpot (if the jackpot is not linked to a particular game theme, paytable or player);

b) Identification of the winning player;

c) Identification of the theme of the game/pay table;

d) Identification of the winning game cycle and/or game session identification (if different);

e) The date and time of the jackpot activation;

f) Winning jackpot and payment amount; and

8.7.7 Report of transactions made by players

The Holders of an authorization to operate Technological Platforms for remote sports betting, directly or through the service providers linked to the operation, provide MINCETUR with the necessary access through a WEB Application or other secure access method using a username and password, which are provided by the Holder at the request of MINCETUR and SUNAT, to obtain information contained in the section "Record of transaction or summary of gaming account" made by the players in their gaming accounts according to the following search filters:

a) Player identification:

i. Full name;

ii. Identity card;

iii. ID card number/foreigner's card number/passport number; and
iv. Unique player identifier.

b) Identifier of the place where the transaction took place (Technological Platform or physical establishment);
c) Transactions made (such as history of deposits, withdrawals, bets, prizes, bonuses, etc.) by each player, allowing filtering by date and time; and
d) Other filters that may be established by mandatory Directives.

8.7.8 Player account report

The Holders of an authorization to operate Technological Platforms for remote sports betting, directly or through the service providers linked to the operation, provide MINCETUR with the necessary access through a WEB Application or other secure access method using a username and password, which are provided by the Holder at the request of MINCETUR and SUNAT, to obtain information contained in the section "Gaming Account Information" made by the players in their gaming accounts according to the following search filters:

a) Player identification:

i. Full name;
ii. ID card number/foreigner's card number/passport number; and
iii. Unique player identifier.

b) Identifier of the place where the transaction took place (Technological Platform or physical establishment);
c) Transactions made (such as history of deposits, withdrawals, bets, prizes, bonuses, and items paid by the players in favor of the Holder, among others) for each player, allowing a filter by date and time; and
d) Other filters that may be established by mandatory Directives.

8.7.9 Platform Specific Report

The Technological Platform must have the capacity to generate online reports, as required by MINCETUR, which are delivered by the Holder at the request of MINCETUR and SUNAT, showing the following information:

a) Commercial name of the Technology Platform;
b) Version of the Technological Platform;
c) Detailed information on available sports bets by service provider, as applicable; and
d) Any other information that MINCETUR may require by means of a mandatory Directive.

8.7.10 Construction of new reports

Notwithstanding the reports described above, MINCETUR may request the Holder, upon prior notice, to prepare new complementary reports.

8.8 Physical and logical accesses to the Technology Platform

8.8.1 Audit

Holders of an operating authorization must provide MINCETUR and/or an entity authorized by MINCETUR with physical or logical access to the Technological Platform to perform a comprehensive audit of critical control components or programs, critical files, services, integration services between Technological platforms, databases, applications, among other software or hardware components that MINCETUR deems necessary.

In the case of logical access, the Registrant must provide a secure access method by means of user and password or other mechanism that allows for a comprehensive audit of the Technology Platform, taking into consideration the following:

a) The Holder must establish a secure communication mechanism to its Technological Platform and that of its related service providers, as well as allow and facilitate at all times the remote audit to MINCETUR and/or entity authorized by MINCETUR, regardless of the physical location of its data centers;
b) MINCETUR may inform the Registrant of the date scheduled for the audit of the Technological Platform, as well as provide information on the activities to be performed and, if necessary, require the specialized support of the Registrant's personnel.
c) The personnel designated by the Contractor must provide the necessary facilities, access, permits and privileges to MINCETUR in order to comply with the scheduled audit. MINCETUR may carry out the corresponding auditing activities and collect the necessary evidence in accordance with the provisions of the LPAG.
d) If not otherwise required, it should be understood that the access provided to MINCETUR is read-only and has the necessary permissions and privileges to access the entire Technology Platform, services, applications, databases, among other software or hardware components deemed necessary without any filter. Once the access is finished, the Holder must close the secure access.

8.8.2 Real-time monitoring and control of remote sports betting

The Licensees must deliver to MINCETUR the remote accesses to the Technological Platform where remote sports betting is exploited, in order to allow the control and supervision of the different modalities of remote games in operation. The accesses have secure communication channels by means of user and password or other secure access method that does not allow vulnerability of the Technological Platform's security. Likewise, the necessary privileges must be granted to carry out the control.

MINCETUR may require the specialized support of the Holder's personnel to carry out the inspection and control of the Technological Platform. MINCETUR may carry out the corresponding inspection activities and collect the necessary evidence in accordance with the provisions of the LPAG.

Section 9. Requirements for Remote Sports Betting

This section establishes the technical requirements for gaming operations, including but not limited to the rules for placing bets and the results for the markets of an event.

9.1 Event Categories and Betting Types

For the offering and acceptance of remote sports bets, the Holders must take into consideration the following:

a) MINCETUR reserves the right to prohibit the acceptance of any wager and may order the cancellation of wagers and require the return of the amount wagered on any sporting event or other category of event, event or type of wager for which the wagers are contrary to the public policies of Peru.
b) The Holder must not offer bets in any of the following cases:

i. Any event in which the majority of the contestants or athletes in the event are under eighteen (18) years of age;
ii. The injury of a participant in an event;

iii. Any event in which:

1. The event is not adequately supervised by a sports governing body or other oversight body;
2. There are no integrity safeguards.
3. The outcome of the event is not verifiable;
4. The outcome of the event is not generated by a reliable and independent process;
5. The outcome of the event may be affected by any wager;
6. The outcome of the event has already been determined and publicly known;
7. The event and the acceptance of the type of wager are not carried out in accordance with applicable laws; and

iv. Any category of event or type of wager that by its nature involves:

1. Violate the right to dignity, honor, privacy, image and non-discrimination, the right of children and adolescents, and any right or freedom recognized by the Constitution and by convention;
2. Are based on the commission of crimes, misdemeanors or administrative infractions;
3. Events not authorized by the Law, the Regulations or MINCETUR's mandatory Directives.

c) If it is determined that a Holder has offered an unauthorized or prohibited category of event, event or type of wager, the Holder must immediately void them and return the value of all associated wagers. The Holder must inform MINCETUR immediately after cancelling and returning the value of the wagers placed.
d) MINCETUR may use any information it deems appropriate, including, but not limited to, information received from a sports governing body, to determine whether to authorize or prohibit wagering on a particular event or type of wager.

9.2 Game display and information

9.2.1 Announcement of sports betting rules

The Holder must publish the complete sports betting rules for the types of markets and events offered. The following information must be made available to the player:

a) Rules of participation, including all game eligibility and scoring criteria, available events and markets, types of wagers accepted, line odds, all advertised prizes, and the effect of programming changes;
b) Payout information, including possible winning combinations, rating, results, along with their corresponding payouts for any available betting options;
c) Any restrictive game function, as well as the amount of the bet or the maximum value of the prizes;
d) Procedures for handling incorrect announcement of events, markets, odds/payouts, prices, wagers, or results;
e) A wager cancellation policy that includes betting on multiple events (parlays) and indicating any prohibition to cancel bets (after a fixed period of time);
f) Whether the odds/payouts are fixed at the time of wagering, or whether the odds/payouts can change dynamically prior to the start of the event and the method of announcing changes in the odds/payouts;
g) For bet types where the odds/payouts are fixed at the time the bet is placed, you must report any situations where the odds/payouts may be adjusted, such as atypical winning outcomes (technical ties), cancelled parts of multi-event bets (parlays), and prorating;
h) For types of bets in which individual bets are collected in funds, the rules for calculating dividends including the prevailing formula are as follows for the awarding of funds and the stipulations of the event being wagered;
i) For in-game betting, due to varying transmission speeds or transmission latency:

i. Updating the information displayed may result in disadvantaging a player with others who may have more current information; and
ii. There may be built-in delays in the recorded time of a wager during play to prevent before-after bets and voids.

j) A statement that the Registrant reserves the right to:

i. To refuse any wager or part of a wager or to refuse or limit selections prior to the acceptance of a wager for the reason stated to the player in these rules;
ii. Accepting a wager with terms different from those published;
iii. Close periods of play at your discretion;

k) If prizes are to be paid for combinations including other participants than the first place finisher (in an Olympic competition), the order of the participants is associated with these prizes (result 8-4-7);
l) The rules for any unusual betting options (perfect, trifecta, quinella, etc.) and the expected payouts;
m) What must occur when an event or market is cancelled or withdrawn, including the handling of multiple event betting selections and/or when one or more of the parties are cancelled or withdrawn;
n) How a winning bet is determined and the handling of a prize in case a tie is possible;
o) The payout of winning bets, including the redemption period and the method of calculation. Where the calculation of payouts may include rounding, information on the handling of these circumstances must be clearly explained:

i. Rounding up, rounding down (truncated), true rounding; and
ii. Rounding to what level.

9.2.2 Dynamic game information

The following information must be available without placing a wager. In a physical gaming room, this information may be displayed on a Betting Terminal and/or external indicator.

a) Information on the events and markets available for betting;
b) Current probabilities/payments and prices for available markets;
c) For types of markets in which individual bets are collected in funds:

i. Updated odds/payout information for simple market funds. For complex market funds, it is acceptable that there are reasonable limitations on the accuracy of the updated funds estimate shown to the player;
ii. Updated values of the total investment for all market funds; and
iii. Dividends from any given market.

9.2.3 Player resources/functions

Resources/features may be provided to the player, as well as offering advice, hints, or suggestions to a player, or a data stream that can be used to facilitate bet selection externally, if the following conditions are met:

a) The player should be informed of each resource/function that is available, the advantage it offers, and the options that exist to select from.

b) The method of obtaining each resource/feature must be disclosed to the player. All resources/features that are offered to the player for wagering must clearly show the cost.

c) The availability and functionality of player resources/functions must be consistent for all players.

d) For peer-to-peer betting, the player should be provided with sufficient information to make informed decisions, prior to participation, as to whether to participate with the player(s) who may have these resources/features.

9.3 Placement of bets

All wagers and transactions of the player must be recorded in his gaming account, regardless of whether the wager is placed by an attendant in a gaming room or in a Betting Terminal or any other Gaming Media.

9.3.1 Placement of bets

The following rules apply only to the placement of a wager placed directly by the player in the Betting Terminal:

a) The method of placing a wager should be easy, with all selections identified (including the order, if applicable). When the wager consists of multiple events, this grouping must be identified.

b) Players must be enabled to select the desired market to place a bet.

c) Bets must not be automatically placed on behalf of the player without the player's consent/authorization.

d) Players must be given the opportunity to review and confirm their selections before completing the wager. This does not preclude making "one-click" bets if accepted by the player.

e) Situations should be identified where the player has placed a wager so that the odds/payouts or prices have changed, and unless the player has opted to automatically accept the changes, provide a notification to confirm the wager considering the new values.

f) The player must be told that the wager has been accepted or rejected (in whole or in part). Each wager must be acknowledged and clearly indicated separately so that there is no doubt as to which wagers have been accepted.

g) All types of wagers must be associated with the player's gaming account and, accordingly:

i. The account balance must be easily accessible.

ii. A wager that results in a negative balance for the player should not be accepted.

iii. The account balance must be debited when the wager is accepted by the Technology Platform.

9.3.2 Automatic acceptance of betting changes

The Technology Platform that supports a feature that allows a player to self-accept changes in odds/payouts or the cost of the wager while placing a wager must meet the following requirements:

a) All available self-acceptance options must be explained to the player;

b) The player must manually opt for the use of this; and

c) The player must have the ability to opt out at any time.

9.3.3 Betting coupon

After completing a gambling transaction, in the sports betting gaming rooms, the player must have access to a record of the wager, through the issuance of a virtual or printed coupon, which includes the following information:

a) The date and time the bet was placed;

b) The date and time the event is expected to occur (if known);

c) Any player selection included in the wager:

i. Market line and odds (single bet, spread bets, over/under bets, win/place/show, etc.);

ii. Bet selection (athlete or team name and number);

iii. Any special condition(s) that apply to the wager;

d) Total amount wagered, including any bonus credits (if applicable);

e) Player's first and last name or unique identification code given by the Holder;

f) Unique identifier number and/or bar code of the bet;

g) Unique identification of the Betting Terminal that issued the wagering coupon, if applicable;

h) Identification code of the remote sports betting gaming room granted by MINCETUR.

9.3.4 Closing of the betting period

It must not be possible to place bets once the betting period has closed.

9.3.5 Free bet mode

The Technology Platform may support the free betting mode, which allows a player to participate in betting without paying. The free betting mode must not mislead the player about the odds/payouts available in the paid version.

Paid bets that can be played with credits received from a bonus prize (promotion) are not considered free bets.

9.4 Results and payments

9.4.1 Display of results

The record of results must include access to all information that may affect the results of all types of bets offered for that event.

a) It must be possible for a player to obtain the results of his bets in any given market once the results have been confirmed.

b) Any changes in the results (due to statistics/line corrections) must be available.

9.4.2 Payment of prizes

Once the results of the event are recorded and confirmed, the player receives the prize payout. This does not exclude the player's option to receive an adjusted payout prior to the conclusion of the event when offered.

9.5 Virtual Sports Betting

Virtual sports betting allows the placement of wagers on simulations of sporting events, competitions and horse races whose results are based solely on the outcome of a Random Number Generator (RNG). In addition to this section, please note the "Remote Sports Betting Requirements" contained in Section
9 of this Technical Standard of the Regulation. The

virtual sports should not be interpreted as if it were a live betting event.

9.5.1 Randomness and Virtual Sports

The GNA used in virtual sports betting must comply with the requirements set forth in the sections "Random Number Generator (RNG) Requirements" and "Game Outcome Using a Random Number Generator (RNG)" contained in the approved Technical Standards I. The following requirements apply to virtual sports betting: The following requirements apply to virtual sports betting: The following requirements apply to virtual sports betting: The following requirements apply to virtual sports betting: The following requirements apply to virtual sports betting: The following requirements apply to virtual sports betting. Likewise, the following requirements apply to virtual sports betting:

a) It should not be possible to determine the results of a virtual sport prior to the start; and

b) After the start of the virtual sport, no actions or decisions should be taken that affect the functioning of any of the probability elements in the virtual sport, apart from the player's decisions.

9.5.2 Deployment of Virtual Sport

A virtual sports game must conform to the applicable display requirements for the "Game Information and Game Rules", "Game Display and Information", and "Fair Play Requirements" sections contained in the approved Technical Standard I. In addition, they must comply with the following requirements:

a) The statistical data available to the player with respect to the virtual sport should not influence the skills of any virtual participant. This does not preclude the use of an element of randomness from affecting the results of a virtual participant during the virtual sport.

b) For scheduled virtual sports, the player must be shown a countdown of the time remaining to place a wager. It must not be possible to place wagers on the event after the countdown has been completed; however, this requirement does not prohibit the placing of wagers during the game.

c) Each virtual participant must have a unique appearance, when it corresponds to a bet. If the wager is for one team to beat another, there is no need for the virtual participants themselves to have a unique appearance, however, the teams in which they participate must be clearly distinct from each other.

d) The result of a virtual sport must be evident, unambiguous, and must be displayed for an adequate period of time to give the player the opportunity to verify the result of the virtual sport.

9.5.3 Simulation of Physical Objects

When a game incorporates a graphical representation or simulation of a physical object that is used to determine the outcome of the game, the behavior represented by the simulation must be consistent with the real-world object, unless otherwise stated in the game rules. The following requirements apply to simulation:

a) The probability of any event occurring in the simulation that affects the outcome of the game will be analogous to the properties of the physical object, unless otherwise indicated to the player;

b) Where the game simulates multiple physical objects that are expected to be independent of each other according to the rules of the game, each simulation must be independent of the others; and

c) Where the game simulates physical objects with no history of previous events, the behavior of the simulated objects must be independent of their previous behavior, so as not to be predictable, unless otherwise instructed to the player.

9.5.4 Physical Engine

Games can use a "physics engine" which is specialized software that approximates or simulates a physical environment, including behaviors such as motion, gravity, velocity, acceleration, inertia, trajectory, etc. A physics engine shall be designed to maintain behaviors of the game and its environment, unless the rules of the game instruct the player otherwise. A physics engine may utilize the random properties of a GNA that impacts the game outcome, in this case, the "Random Number Generator (RNG) Requirements" section will apply, which are contained in the approved Technical Standards I.

Implementations of a physical engine in a Gaming Terminal will be evaluated on a case-by-case basis by the authorized Certification Laboratory.

9.6 External Technology Platforms

The Technology Platform communicating with an external Technology Platform must meet the following requirements in any of the following configurations:

a) The Technology Platform acts as the "host Technology Platform" that receives, for its own markets, bets from one or more external "client Technology Platforms"; or

b) The Technology Platform acts as a "client Technology Platform" sending bets to a "host Technology Platform" for that Technology Platform's markets.

The requirements of this section apply to the interoperability of the Technology Platform with the external Gaming Terminal, and are not a complete evaluation of the external gaming platform by itself. The external Technology Platform must undergo an evaluation by an authorized Certification Laboratory.

9.6.1 Information

The following requirements apply to information sent between the host Technology Platform and the client Technology Platform:

a) If the host Technology Platform provides pari-mutuel betting for the client Technology Platform, the Technology Platform must have the capability to:

i. When acting as the client Technology Platform, receive current bets for active funds sent from the host Technology Platform.

ii. When acting as the host Technology Platform, send current bets for active funds to all connected client Technology Platforms.

b) If the host Technology Platform provides fixed odds wagering for the client Technology Platform and where the odds for the payout of the prizes can be changed dynamically, the Technology Platform must have the ability to:

i. When acting as the client Technology Platform, receive the odds for payment of the current prizes sent from the host Technology Platform each time any odds/payment and price has changed.

ii. When acting as the host Technology Platform, send the odds for the current prize payout to all connected client Technology Platforms whenever any odds/payout and price has changed.

c) A change of event status information must be sent from the host Technology Platform to the client Technology Platform whenever any change occurs, including:

i. Selections withdrawn/reset;
ii. The start time of the event has changed;
iii. Individual markets open/closed;
iv. Results entered/modified;
v. Confirmed results; and
vi. Event cancelled.

9.6.2 Bets

The following requirements apply to wagers placed between the host Technology Platform and the client Technology Platform:

a) Bets placed on the client Technology Platform must receive clear acknowledgement of acceptance, partial acceptance (including details), or rejections sent from the host Technology Platform.

b) If the cost of the wager is determined by the host Technology Platform, a positive confirmation sequence must be established to enable the player to accept the cost of the wager, and the client Technology Platform to determine that there are sufficient funds in the account balance to cover the cost of the wager prior to making the offer to the host Technology Platform.

c) When wagers may be placed in bulk, the following requirements apply:

i. If the betting flow is interrupted for any reason, there must be a method available to determine when in the transmission the interruption occurred.

ii. No bet should be transmitted if it is greater than the account balance. If there is an attempt of this type of bet, the entire transmission must be stopped.

d) The account balance must be debited in an amount equal to the offer and cost from the host Technology Platform. The funds should remain as a pending transaction with the bid details recorded on the host Technology Platform. When the acknowledgement from the host Technology Platform is received, appropriate adjustments should be made to the "pending" account and the account balance on the client Technology Platform.

e) Cancellation requests from the client Technology Platform must clearly receive an acknowledgement of acceptance or rejection by the host Technology Platform. The player must not be credited by the client Technology Platform until final confirmation is received from the host Technology Platform including the amount of the cancelled wager.

9.6.3 Results

When the results are entered and confirmed on the host Technology Platform, each winning bet must be transferred to the client Technology Platform with the prize amount. Confirmation of receipt of winning bets must be acknowledged by the client Technology Platform.

9.7 Progressive systems (Incremental Progressive Jackpot)

This section applies to progressive systems that increase, depending on the game and/or wagers, as follows:

a) Progressive jackpots increase according to the credits wagered in the game and/or bets.

b) Incremental progressive jackpots behave identically to the progressive jackpot, except that they increase based on the occurrence of one or more specific conditions (defined events) established by the rules of the game rather than, or in addition to, increases based on credits wagered.

This section does not apply to restricted bonus credit awards, bonus, which offer awards of that may increase in a single game cycle or, static prizes whose probability of triggering changes as the game unfolds. This section also does not apply to persistence game features that increase as the game is played (number of free games, multipliers, various achievements towards triggering a bonus, or issuing a prize, etc.) or static prize "levels" available to be won based on the player's experience and/or achievements.

9.7.1 Progressive Systems Screen

The progressive system display is used to indicate the current amount of the progressive jackpot or the "payout" of each prize in credits or local currency format to all players who are participating in a game that can potentially trigger the progressive jackpot. If the progressive system offers a "mystery attraction", i.e., the actual reward is not shown to the player, the "Mystery Prizes" detailed in 5.8.6 of the Technical Standards I apply.

a) As the games progress, the current amount for each progressive jackpot is updated on the progressive system screen at least every thirty minutes.
(30) seconds from the incremental play event to reasonably reflect the actual payout amount. The use of the odometer and other "step" update screens is permitted.

b) When the progressive system screen has a maximum display limitation, that is, it can only display a certain number of digits, it is required that the maximum payout limit or "upper limit" must meet the requirements for "as a consequence of the verification of a winning play, to be exchanged for money, in whole or in part, at the sole will of the player".

9.7.2 Maximum Payment Limits

If a maximum payout limit or "upper limit" is supported by the progressive jackpot, once the payout reaches its upper limit, it remains at that value until a winning play or combination is verified.

a) The Registrant must inform MINCETUR of any additional contribution that constitutes an excess or a deviation scheme of the progressive jackpot, in which case it must indicate where they were diverted, in accordance with the provisions of numeral 5.13.4 of the Technical Standards I.

b) When the player is shown the artwork, the amount of the upper limit indicated must be accurate.

9.7.3 Linked Probabilities

In the event the player is notified of progressive jackpots linked to multiple game themes and/or wagers, the probability of winning such jackpot will be proportional to the player's monetary wager.

For this requirement, a variation of no more than five percent (5%) probability and no more than one percent (1%) tolerance in the calculation of theoretical expected percentage return is acceptable.

9.7.4 Deviation from the progressive jackpot

A progressive jackpot diversion scheme may be used, where a portion of the progressive jackpot contributions are diverted to another pool for the resetting of the next progressive jackpot or to be used as set forth in the progressive system design, such as the payment of simultaneous awards of such jackpots.

a) A progressive jackpot diversion scheme can be implemented so that it does not have a mathematical expectation of infinity.

b) Diversion funds are not truncated. Diverted contributions will be counted once the progressive jackpot pool has reached its upper limit.

c) When a diversion fund is used to fund the reset value of a progressive jackpot, the reset value assumes an empty diversion fund for purposes of the theoretical return percentage calculations.

9.7.5 Progressive Jackpot

The progressive jackpot can be awarded based on winning symbols, sporting event results or by other criteria, such as mystery triggered progressive jackpot, bad-beat jackpot, etc. When a progressive jackpot is triggered:

a) The player is informed at the end of the game of the prize won and its payment.

b) Contributions to the progressive jackpot are not forfeited. Progressive jackpot payments, when awarded, are not rounded or truncated, unless transferred to the reset amount.

c) When in use, the progressive jackpot payout may be added to the player's credit meter if:

i. The credit counter is maintained in the format of the amount in currency (Soles, US Dollars or other currency);

ii. The progressive jackpot payment is increased by full credit amounts; or

iii. The progressive jackpot payout in the format of the local currency amount is properly converted into credits upon transfer to the credit meter in a manner that does not mislead the player.

d) The progressive jackpot payout is updated to the reset value and continues with normal operations.

9.7.6 Progressive Jackpot Level Swapping

In progressive jackpots that offer multiple prize levels, when the player obtains a winning combination, result of sporting events, market lines, within more winning combinations available, the highest possible value must always be paid to the player, unless it has been explicitly defined in the game or sporting event rules.

9.7.7 Progressive Jackpot Triggered by Mystery Prize

To determine when the progressive jackpot triggered by a mystery prize that has a hidden trigger amount is awarded, it must be considered:

a) The hidden active amount is set randomly at each progressive jackpot reset and remains hidden at all times; and

b) It is not possible to obtain access to or knowledge of the hidden asset amount.

9.7.8 Multi-Player Progressive Jackpot Triggers

The Technology Platform is designed to accurately identify and record the order of the triggers when several players activate it at almost the same time, so that the total amount of the payout shown can be awarded to the winning player who activated it first. When this is not possible, or if several players activate it at the same time, it shall:

a) To deliver to each winning player the full amount of the payment shown; or

b) Communicate to the player the precise information on how the Progressive Jackpot is distributed.

9.7.9 Changes to the progressive jackpot parameters

When a progressive system is in use and received contributions based on player wagers, the modification of the progressive jackpot or the increase of the progressive jackpot parameter values must comply with the following requirements:

a) When the rate or factor of increase of the progressive jackpot is configurable and affects the percentage of theoretical return to the public or to the gaming programs, the changes made shall not come into operation until the progressive jackpot is awarded.

b) When the progressive jackpot presents a configurable maximum limit independent of the percentage of return to the public and of the game programs, the changes to the maximum limit may only be of a higher value than the current prize. In the event that a lower value is configured than the current progressive jackpot, the excess resulting from this reduction must be part of a new progressive jackpot. This new configuration of a lower value must be communicated to MINCETUR as established in article 39 of the Regulation.

c) Changes in the parameters should not affect the odds of being awarded the current progressive jackpot;

d) For an active mystery prize, whose winning progressive jackpot is based on a hidden active amount, the following must be taken into account:

i. The awarding of the prize must maintain its randomness, even if any parameter that may influence the result of the awarding of the prize is modified;

ii. The selected hidden active amount must be in the range of the current award up to the maximum limit and the award must not be surrendered as a result of the modification.

9.7.10 Modifications to the progressive jackpot

The Technology Platform must have a secure mechanism that allows:

a) The total or partial transfer of inactive progressive jackpot contributions (and any overflow or diversion of specific progressive jackpot funds);

b) Correct progressive jackpot errors; and

c) Any other modification requested by MINCETUR.

Section 10. Gaming Terminal Requirements

Within remote sports betting gaming rooms, a wager may be placed using one of the following types of Betting Terminals. Any other type of Betting Terminal is reviewed on a case-by-case basis by the authorized Certification Laboratory.

a) Sale Betting Terminal: An electronic module used by a remote sports betting gaming room worker to assist in the execution or formalization of a wager placed by a player on his gaming account.

b) Self-Service Betting Terminal: An electronic device located in the remote sports betting gaming room and used for the execution or formalization of bets placed directly by the player and which are recorded in his gaming account and, if supported, may be used for the collection of winning bets.

10.1 Betting Terminal Software

Gaming terminal software is used to participate in gaming and financial transactions on the Technology Platform, which based on its design, is downloaded or installed on the Gaming Terminal, executed from the Technology Platform that is accessed by the Betting Terminal, or a combination of both.

10.1.1 Identification of the Betting Terminal

The betting terminal software must contain sufficient information to identify the software and its version.

10.1.2 Software validation

For gaming software installed locally on the Gaming Terminal, it must be possible to authenticate that all critical components contained in the software are valid each time the software is loaded for use, and if it is supported by the Technology Platform. Critical components may include, but are not limited to, the game rules, elements that control the communication between the Gaming Terminal and the Technology Platform, or other components that are required to ensure the correct operation of the software. In case of failed authentication (program incompatibility or authentication failure), the software must prevent gaming operations and display an appropriate error message.

Program verification mechanisms are evaluated on a case-by-case basis by the authorized Certification Laboratory based on industry standard safety practices.

10.1.3 User interface requirements

The user interface is defined as an interface application or program through which the user can view and/or interact with the game software. The user interface must meet the following requirements:

a) The functions of all buttons, click points or touch points must be clearly indicated in the button area, or click/touch point or in the help menu. Functionality through any button or click/tap point on the user interface must not be available if it is undocumented.

b) Any resizing or overlaying of the user interface must be accurately mapped to reflect changes in the visual display and click/tap points.

c) User interface instructions, in addition to information about the functions and services provided by the software, must be clearly communicated to the user and must not be misleading or incorrect.

d) The visual display of instructions and information must be adapted to the user interface. For example, when a Betting Terminal implements technology with a smaller screen, it is permissible to present an abbreviated version of the game rules accessible directly from the game screen and make available the full version of the game rules through another method, as well as a secondary screen, help menu, or other interface that is easily identified on the game screen.

10.1.4 Simultaneous entries

The betting terminal software must not be adversely affected by the simultaneous or sequential activation of multiple inputs and outputs that may, intentionally or unintentionally, cause malfunction or invalid results.

10.1.5 Betting coupon printers

If the Betting Terminal uses a printer to issue a printed betting coupon to the player, the printed betting coupon must include the information indicated in the "Betting Coupon" section.

10.1.6 Communications

The software for the betting terminal must be designed or programmed in such a way that it can only communicate securely with authorized components.

a) After a program interruption, no communication with an external device should begin until the program resumption routine, including the self-test, has been successfully completed.

b) If communication between the Technology Platform and the Gambling Terminal is lost, the software must prevent further gambling operations and display a clear, simple and unambiguous error message. It is permissible for the software to detect this error when the device attempts to communicate with the Technology Platform.

10.1.7 Touch screens

Touch screens, if used by the Gaming Terminal software, must be accurate and as required by design, and must support a calibration method to maintain accuracy; alternatively, the visual display hardware may support automatic calibration.

10.1.8 Printed betting coupon

If the Betting Terminal connected to a printer to produce a printed betting coupon, the printer and/or terminal software must have the capability to detect and indicate the following error conditions, if applicable. It is permissible for the error condition to be detected when attempting to print:

a) Low battery (when the power supply is external to the Betting Terminal);
b) It ran out of paper/paper underneath;
c) Printer jam/failure; and
d) Printer disconnected.

10.2 Self-Service Betting Terminal software requirements

The player places a wager at a Self-Service Betting Terminal using funds from his/her gaming account or through placement of cash or any other means of payment. In addition to the requirements for "Gaming Software", the requirements set forth in this section shall apply to Self-Service Betting Terminals.

10.2.1 Critical Non-Volatile Memory (NV)

Non-volatile (NV) critical memory must be used to store all data elements that are considered vital to the continued operation of the Self-Service Gaming Terminal, including but not limited to configuration data and the operating status of the Self-Service Gaming Terminal. Critical NV memory must be maintained by the Self-Service Betting Terminal and/or the Technology Platform.

a) Self-service betting terminals whose operation includes local storage of NV critical memory must have the ability to back up or archive, which allows recovery of NV critical memory in the event of a failure.

b) NV critical memory storage must be maintained by a methodology that allows errors to be identified. This methodology may include signatures, checksums, redundant copies, database error checking, and/or other method(s) approved by MINCETUR.

c) Complete verification of critical NV memory data elements must be performed during power-up and program restart. Verification of NV memory that is not critical to the integrity of the Self-Service Gaming Terminal is not required.

d) Unrecoverable corruption of critical NV memory should result in an error. If it is detected, the terminal software should cease operation and display a message error message. In addition, the NV critical memory error must interrupt any external communication to the Self-Service Betting Terminal.

10.2.2 Configuration settings

Changes to any configuration settings for the regulatory operations of the Self-Service Betting Terminal must only be made in a secure manner.

10.2.3 Transaction limit

The terminal software must have the capability to set transaction limits. If a player attempts to make a transaction that exceeds these limits, the transaction is only processed provided that the player is clearly notified that the transaction was for less than requested.

10.2.4 Testing/diagnostic modality

The test/diagnostic mode (sometimes called demo or audit mode) allows the wizard to view or execute audit and/or diagnostic functions supported by the terminal software. If test/diagnostic mode is supported, the following rules should apply:

a) Access to the testing/diagnostic modality should only be possible by secure means.
b) If the Self-Service Betting Terminal is in testing/diagnostic mode:

i. The Self-Service Betting Terminal must clearly indicate that it is in this mode; and
ii. Any testing or diagnostics consisting of funds entering into or dispensed from the Self-Service Betting Terminal must be completed prior to resuming normal operation of the Self-Service Betting Terminal.

c) All funds in the Self-Service Betting Terminal that were obtained during the test/diagnostic mode should be automatically cleared upon exiting the mode.

10.2.5 Electronic counters and records

Electronic meters and records should only be accessed by authorized personnel and should have the ability to be securely displayed upon request.

a) Electronic counters for accounting must be at least ten (10) digits in length. Eight (8) digits must be used for the amount of Soles or US Dollars or other currency and two (2) digits used for the amount of centavos. The counter should automatically reset to zero once it has reached its maximum logical value. The counters must be labeled so that their function can be clearly understood. The required electronic accounting counters are as follows:

i. Banknote entered. The terminal software should have a counter that accumulates the total value of bills accepted;
ii. Paid Ticket. The terminal software must have a counter that accumulates the total value of tickets physically paid by the Self-Service Betting Terminal;
iii. Electronic Funds Transfer In (EFT In). The terminal software must have a counter that accumulates the total value of collectible credits electronically transferred to the Self-Service Gaming Terminal from a financial institution through a Technology Platform;
iv. WAT In (WAT In) Gaming Account Income Transfer. The terminal software must have a counter that accumulates the total value of collectible credits electronically transferred to the Self-Service Wagering Terminal. from a gaming account through a Technology Platform;
v. Gaming Account Payment Transfer (WAT Out). The terminal software must have a counter that accumulates the total value of collectible credits electronically transferred from the Self-Service Wagering Terminal to a gaming account through a Technology Platform;
vi. Other counters. For transactions related to the regulatory operations of the Self-Service Wagering Terminal that are not otherwise measured by any of the electronic accounting counters, the terminal software must maintain sufficient counters to correctly reconcile all such transactions.

b) Event counters must be at least eight (8) digits in length, however, they are not required to turn over automatically. Counters must be labeled so that their function can be clearly understood. The required electronic event counters are as follows:

i. External doors. The terminal software shall have counters that accumulate the number of times any external door (main or belly door, deposit box door, cash area with an external door, etc.) has been opened since the last NV memory clear, if the Self-Service Betting Terminal is provided with power supply;
ii. Stacker door. The terminal software shall have a counter that accumulates the number of times the stacker door has been opened since the last NV memory clear, if the Self-Service Betting Terminal is provided with power supply;
iii. Ticket denomination entered. The terminal software must have a specific event counter for each ticket denomination accepted by the Self-Service Betting Terminal;
iv. Denomination of ticket paid. The terminal software must have a specific event counter for each denomination of ticket dispensed by the Self-Service Betting Terminal;

c) The capability must be provided to display a complete transaction log with all thirty-five
(35) previous transactions that increased any of the counters related to bills, electronic funds transfers (EFTs), and gaming account transactions. The following information must be displayed, as applicable:

i. The value of the transaction in the local currency unit in numerical form;
ii. The time of the transaction, in twenty-four-hour format. (24) hours showing hours and minutes;
iii. The date of the transaction, in any recognized format, indicating the day, month, and year;
iv. The type of transaction (loading/unloading) including restrictions (chargeable or non-chargeable, etc.); and
v. The account number or a unique transaction number, either of which can be used to authenticate the origin of the funds (where the funds came from/where the funds were sent).

d) The last one hundred (100) significant events for Self-Service Wagering Terminals must be stored with appropriate time stamping in one or more secure records that are not accessible to the player and that include the following events as a minimum, as applicable:

i. Software verification errors or NV critical memory errors, if it is technically possible to log these events based on the type and/or severity of the error;
ii. Changes made to the configuration of the Self-Service Betting Terminal;
iii. Self-service Betting Terminal communication failure, if supported;
iv. Power restoration;

v. Access in secure areas or secure compartments; and

vi. Peripheral device errors, if supported.

10.3 Self-service Betting Terminal Hardware Requirements

This section establishes the technical requirements for the key attributes of a Self-Service Betting Terminal. All proprietary devices developed for Self-Service Betting Terminals must comply with the applicable Self-Service Betting Terminal requirements of this Technical Standard.

10.3.1 Physical hazards and electrical and environmental safety testing

The electrical and mechanical parts and major design elements of the Self-Service Betting Terminals terminals must not expose the player to any physical risk. The authorized Certification Laboratory should not make any determinations regarding electromagnetic compatibility (EMC) or radio frequency interference (RFI), as these are the responsibility of the Self-Service Gaming Terminal manufacturer. However, during the course of testing, the authorized Certification Laboratory inspects for markings or symbols indicating that a Self-Service Gaming Terminal has undergone product safety compliance testing or other third-party compliance testing.

10.3.2 Environmental effects on integrity

This section is only applicable for a Self-Service Betting Terminal that has locally stored non-volatile critical memory and/or software installed that has the ability to influence the regulatory operations of the Self-Service Betting Terminal. The authorized Certification Laboratory performs some tests to determine if an electrostatic discharge (ESD) or energy fluctuation affects the integrity of a Self-Service Gaming Terminal. Electrostatic discharge and energy fluctuation tests are intended only to simulate techniques observed in the field being used to attempt to disrupt the integrity of the Self Service Gaming Terminal.

a) Electrostatic discharge protection requires that the conductive cabinet of the Self-Service Gaming Terminal be grounded so that static discharge energy does not permanently damage or disable normal operation of the electronics or other components within the Self-Service Gaming Terminal terminal. Self-Service Betting Terminals may exhibit temporary disruption when subjected to significant electrostatic discharge with a severity level of up to 15kV air discharge. Self-Service Betting Terminals must exhibit the ability to recover after any temporary disruption and complete any interrupted operation without loss or corruption of any locally stored control information or critical data.

b) The Self-Service Betting Terminal terminal must not be adversely affected, other than by reboot, by fluctuations of ± 10% of the power supply voltage. It is acceptable for the Self-Service Betting Terminal to reboot provided that no damage occurs to the equipment or loss or corruption of locally stored data, which cannot be automatically retrieved in the Technology Platform. Alternatively, the Self-Service Betting Terminal terminal may be equipped with an uninterruptible power supply (UPS) or battery backup that, upon detection of power loss, allows completion of the current transaction before ceasing operation.

10.3.3 Identification information

The Self-Service Betting Terminal terminal must be identifiable by model number, manufacturer's identification, and any other information required by MINCETUR.

10.3.4 On/Off switch

An on/off switch that controls the electrical current supplied to the Self-Service Gaming Terminal terminal shall be located in a secure area of the Self-Service Gaming Terminal terminal. The on/off positions of the switch shall be clearly labeled.

10.3.5 Touch screens

Touch screens, if used for Self-Service Gaming Terminal regulatory operations, must be accurate and, as required by design, must support a calibration method to maintain their accuracy; alternatively, the visual display hardware may support self-calibration.

10.3.6 Customized and modified hardware

This section only applies to customized and modified hardware components that can potentially influence the regulatory operations of the Self-Service Betting Terminal.

a) Each Printed Circuit Board (PCB) should be clearly identified alphanumerically and, where applicable, with a revision number. If circuit breaks, connection wiring, or other circuit alterations are introduced on the PCB, a new revision number must be assigned.

b) If the Self-Service Betting Terminal includes switches and/or jumpers, these must be fully documented for evaluation by the authorized Certification Laboratory.

c) The design of the Self-Service Gaming Terminal terminal shall route power and data cables in and out of the Self-Service Gaming Terminal so that they are not accessible by the public.

d) Connected communication ports must be clearly labeled and must be securely housed in the Self-Service Gaming Terminal terminal to prevent unauthorized access of the ports or their associated connector cables.

e) The Self-Service Gaming Terminal shall support the use of an externally accessible charging mechanism, as well as a USB (Universal Serial Bus) charging port, or other similar technology (cables, inductive chargers, etc.). The mechanism can be used to provide external power or access for charging an electronic device, such as a smart phone, tablet, etc. If applicable, the charging mechanism shall:

i. Contain adequate fuses and/or be electrically protected;

ii. Not impact the integrity of the regulatory operations of the Self-Service Betting Terminal; and

iii. Do not allow data transmission between the Self-Service Betting Terminal and the loading mechanism.

10.3.7 Doors and security

This section only applies to Self-Service Gaming Terminal terminals that perform transactions using peripheral devices installed in the terminal and/or contain critical locally stored Non-Volatile (NV) memory and/or installed software with the potential to influence the regulatory operations of the Self-Service Gaming Terminal.

a) The terminal of the Self-Service Betting Terminal must be robust enough to withstand the forced entry into any secure area, doors, or compartments. In the event of the application of extreme material force on the cabinet causing a potential breach of the security of the Self-Service Betting Terminal terminal, this tampering must be evident. "Secure areas" or "secure compartments" shall include, if applicable, the external doors, as well as the front door, cash compartment door, as well as the deposit box door or stacker door, and/or other protected access areas of the Self-Service Betting Terminal terminal.

b) The following requirements apply to Self-Service Betting Terminal terminals that contain external doors to secure areas or compartments:

i. External doors must be made of materials that are suitable for only allowing legitimate access to the interior of the Self-Service Betting Terminal terminal.

ii. The external doors and their associated hinges must be capable of resisting determined and unauthorized efforts to access the interior of the Self-Service Betting Terminal terminal and must leave visible evidence of tampering in the event of an attempt;

iii. The seal between the Self-Service Betting Terminal terminal and the external door shall be designed to resist the entry of objects. It shall not be possible to insert an object into the Self-Service Gaming Terminal terminal that would disable a door open sensor when the Self-Service Gaming Terminal terminal door is fully closed, without leaving visible evidence of tampering; and

iv. All external doors must be secure and support the installation of locks.

c) All doors that provide access to the secure areas of the Self-Service Betting Terminal terminal shall be monitored by door access detection software.

i. The detection software shall register that a door is open when the door is moved from its fully locked position, if the Self-Service Betting Terminal is provided with power supply.

ii. When any door that provides access to a secure area or secure compartment registers that it is open, the Self-Service Betting Terminal shall cease operation and display an appropriate error message. This error condition shall be communicated to the Technology Platform if this functionality is supported.

10.3.8 Ticket Validators and Stackers

Ticket validators must be constructed in a manner that ensures proper handling of tickets and protects against vandalism, abuse or fraudulent activity. In addition, ticket validators must meet the following standards:

a) A bill validator must be electronics-based and configured to ensure that it detects valid bill entry, and provides a method to allow the terminal software to interpret and act appropriately on a valid or invalid entry;

b) Invalid tickets must be rejected and are returned to the player;

c) Each valid banknote must register in the credit counter the real monetary value in national currency.

d) Credits are only recorded when:

i. The bill has passed the point where it is accepted and stacked; and

ii. The ticket validator has sent the message "irrevocably stacked" to the Self-Service Betting Terminal.

e) Each bill validator must be designed to prevent the use of fraudulent methods such as stringing, stringing, stringing, stringing, stringing, stringing, stringing, stringing, stringing, stringing, stringing, stringing and stringing. insertion of foreign objects and any other manipulation that could be considered a fraud technique. Corresponding error conditions are generated and the bill validator is deactivated;

f) A counterfeit detection method should be implemented. Counterfeit bills must be rejected with a high degree of accuracy;

g) Acceptance of any ticket to be credited to the credit meter is only possible when the Self-Service Betting Terminal is enabled for use. Other states, such as error conditions, including door opening, cause the ticket validation system to be disabled; and

h) Each Self-Service Betting Terminal and/or ticket validator must have the ability to detect and display the error conditions listed below. The ticket validator disables itself and provides an appropriate error message that is communicated to the back-office platform when such functionality is supported. The error(s) is cleared by a wizard, or upon initiation of a new transaction subsequent to the clearing of the error.

i. Stacker full; it is recommended not to use an explicit "stacker full" error message as it may cause a security problem; rather a message such as "Banknote validator malfunction" or similar is suggested; it is acceptable to use flashing lights with respect to the banknote validator itself;

ii. Banknote jams; it is acceptable to use flashing lights with respect to the bill validator itself;

iii. Communication failure of the bill validator; it is acceptable to use flashing lights with respect to the bill validator itself;

iv. Stacker door open; the stacker door is the door immediately preceding access to the box/stacker assembly; the kiosk stops operating, provided power is supplied to the kiosk; and

v. Stacker removed; kiosk stops operating, provided power is supplied to the kiosk.

i) The bill validator must perform a self-test during each power-up. In case of failure of the self-test, the bill validator is automatically deactivated until the error condition has been cleared.

j) All ticket validators communicate with the Self-Service Betting Terminal through a bidirectional protocol.

k) It is only possible to perform preventive maintenance, or make the following changes or adjustments to the bill validators in the field:

i. The selection of the desired acceptance for banknotes and their limits;

ii. Changing the certified critical control program media or downloading the certified software;

iii. Adjusting the tolerance level of the bill validator to accept different quality bills outside the Self-Service Betting Terminal is not permitted. Tolerance level adjustments should only be allowed with appropriate levels of security. This may be achieved by lock and key, physical adjustments of switches, or other accepted methods approved on a case-by-case basis;

iv. Maintenance, adjustment and repair according to factory-approved procedures; and

v. Options that establish the direction or orientation of acceptance.

l) The ticket validator is located in a secure area of the Self-Service Betting Terminal. Only the ticket insertion area is accessible to the player.

m) If a power failure occurs during the acceptance of a ticket, the ticket validator must register the corresponding credits or return the ticket. There may be a small time interval in the that a power failure occurs and the corresponding credit cannot be recorded due to the validation time of the ticket. However, in this case, the time interval is less than one (1) second.

n) Each bill validator has a secure stacker and all accepted items are deposited in the receptacle of the secure stacker. The secure stacker and its receptacle must be attached to the Self-Service Wagering Terminal in such a manner that they cannot be easily removed by physical force and meet the following standards:

i. The bill validator device must have the ability to detect a full stacker condition;

ii. There shall be a separate key lock for access to the stacker area. This key lock is separate from the main door. In addition, a separate key lock is required to remove bills from the stacker.

10.3.9 Integrated player identification components

An integrated player identification component is an electronic device that is controlled by the critical control program of a Self-Service Wagering Terminal and supports a means for players to provide identification information.

a) Examples of such integrated components are a card reader, a bar code reader or a biometric scanner.

i. The integrated card readers are based on electronics and configured to ensure that they read only valid player cards.

ii. The integrated barcode readers must be capable of associating the barcode visible on a card, coupon, voucher, or a permitted electronic device such as a smart phone, as appropriate, with data stored in an external database as a means of identifying an account association, or for redemption purposes.

iii. Integrated biometric scanners must be capable of associating a person's physical characteristics with those recorded in an external database as a means of authenticating a player's identity and for gaming account association purposes.

b) An integrated player identification component must provide a method that allows the software to interpret and act appropriately on valid or invalid input.

c) The integrated player identification component hardware must be secured in a locked box or sealed enclosure, or located within an enclosed area of the Self-Service Wagering Terminal (i.e., an area that requires opening the front door for access). Only areas of the component that require physical interaction are accessible to the player.

d) Each integrated player identification component is designed to prevent tampering that could affect the integrity of the game. A counterfeit detection method is implemented.

e) Each Self-Service Gaming Terminal has the ability to detect and display an error condition related to a malfunction of any integrated player identification component. If a malfunction is identified, the Self-Service Gaming Terminal displays a clear, simple and unambiguous error message and disables the integrated player identification component. In the case of integrated player identification components, it is acceptable to use flashing lights with respect to the component itself. This error condition is communicated to the back-office platform when such functionality is supported.

TECHNICAL STANDARDS III FOR OPERATIONAL AUDITING OF TECHNOLOGY PLATFORMS

SECTION A

Section 11. Procedures and Practices for an Operational Audit

This section sets forth the procedures and practices for remote gaming and remote sports betting operations that are reviewed in an operational audit as part of the Technology Platform assessment, including, but not limited to, establishing game rules, game management, game monitoring and random number generator (RNG) results, processing various gaming and financial transactions, creating and managing progressive jackpots and incremental progressive jackpots, suspending or canceling or withdrawing sporting events, suspending or canceling or withdrawing markets, voiding bets, player account management, fundamental practices relevant to risk limitation and any other objectives established by MINCETUR.

11.1 Independent Audit of Procedures and Practices

The Proprietor must audit its internal control procedures independently at least once (01) a year with the results documented in a written report available to MINCETUR.

a) Independent audits may be performed by an authorized Certification Laboratory or by an independent area, not directly linked to the operation of remote gaming and/or remote sports betting of the Registrant, acting as an external auditor.

b) The external auditor is responsible for auditing compliance with the internal control system.

c) Documentation, including checklist, schedules, reports, corrective actions and other items, is prepared to demonstrate all independent audit work performed in relation to the requirements of this section, including all instances of non-compliance.

d) Independent audit reports include the objectives, procedures and scope, findings and conclusions, and recommendations.

e) The independent audit findings are communicated to the Registrant. The Registrant is required to respond to the independent audit findings and the corrective actions indicated, which are taken to prevent recurrence of the audit exception. These responses from the Registrant must be included in the final independent audit report.

f) Observations and follow-up reviews are conducted to verify that corrective action has been taken with respect to all instances of non-compliance cited by independent audits, or by MINCETUR. Verification is performed within six (6) months from the date of notification.

Section 12. Internal Controls Procedures

12.1 Internal control procedures.

The Registrant must establish, maintain, implement and comply with internal controls procedures for gaming operations, including wagering and financial transactions as outlined in the approved Technical Standards I and II.

12.2 Data management

The Registrant's internal controls must include processes for storing the information specified in the section "Information to be maintained" for a period of five (5) years.

12.3 Risk management

The Registrant's internal controls should include the details of the risk management framework, including, but not limited to:

a) Manual and automated risk management procedures;
b) Employee management, including access controls and segregation of duties;
c) Information regarding the identification and reporting of fraud and suspicious activity;
d) Controls to ensure regulatory compliance;
e) Description of anti-money laundering compliance standards (Money Laundering Monitoring) including procedures to detect structuring to circumvent reporting requirements;
f) Description of all software applications comprising the Technology Platform;
g) Description of all types of games and wagers available for the Holder's offers;
h) Description of the method to prevent collusion for peer-to-peer games and the placement of bets before/after;
i) Description of all third party service providers; and
j) Any other information required by MINCETUR.

12.4 Restricted Players

The Registrant's internal controls should describe the method to prevent:

a) Participation in remote gaming and remote sports betting by persons covered by Article 28 of the Law.
b) Players wagering on events in which they may have inside information. This includes preventing players identified as professional or collegiate athletes, team employees and owners, coaches, managers, managers, physical trainers, league officials and employees, referees, judges, sports agents, and employees of a players' or referees' union, as well as those in the same nucleus, from placing bets on any event in the sport in which they are participating or in which the athlete they represent is participating.

12.5 Test Accounts

The Registrant may establish test accounts that are used to test or have tested the various components and operation of a Technology Platform in accordance with the internal controls adopted by the Registrant, which, at a minimum, address the following procedures:

a) The procedures for authorizing test activity and assigning each test account for use;
b) The procedures for the issuance of funds used for testing, including identification of who is authorized to issue funds and the maximum amount of funds that can be issued;
c) Maintaining a record for all test accounts, to include when they are active and to whom they are issued; and
d) Procedures for auditing the testing activity to ensure accountability of funds used for testing and appropriate adjustments to reports and records.

Section 13. Gaming Account Controls

13.1 Registration and Verification

When the registration of the gaming account is performed manually by the attendant, procedures must be established to comply with the requirements for "Registration and Verification" set forth in the approved Technical Standards I and II.

13.2 Fraudulent accounts

The Holder must have a documented public policy for the prosecution of player accounts discovered being used fraudulently, including, but not limited to:

a) Maintaining information on account activity, so that if fraudulent activity is detected the Owner has the necessary information to take appropriate action;
b) The suspension of any account found to be used for fraudulent activity, as well as a player providing access to underage persons; and
c) The processing of deposits, wagers, and prizes associated with a fraudulent account.

13.3 Terms and Conditions

The terms and conditions must be available to the player and must be accepted by the player in the registration process, as well as when any significant update to them is made. The Technology Platform records the player's acceptance and the content of the terms and conditions. The terms and conditions must:

a) Provide clear and truthful information on the rules of the games, as well as the form and manner of charging credits to the game accounts and their collection;
b) Establish and publish limits on the minimum and maximum amounts that can be wagered and the prizes that are paid;
c) Declare that he/she is of legal age and has no impediment to participate in the game;
d) Recommend the player to keep his authentication credentials (password and username) secure;
e) Inform about the process to be followed in case of loss and/or change of authentication credentials and password security;
f) Indicate the conditions under which a user account is declared inactive and explain what actions are taken;
g) Clearly define what happens to player wagers whose results were not determined or are found to be interrupted prior to any self-imposed or Holder-imposed exclusion, including the return of all wagers, or the processing of all wagers, as applicable;
h) Display information on terms and limits with respect to deposits and/or withdrawals from the gaming account, including a clear and concise explanation of all fees (if applicable).
i) Establish that the Holder has the right to:

i. Refusal to establish a gaming account for duly motivated and justified reasons;
ii. Reject deposits and/or withdrawals from gaming accounts for duly motivated and justified causes; and
iii. Suspend or close at any time the game account, even if there is a pending investigation or dispute of the player initiated in accordance with the terms and conditions subscribed between the Holder and the player.

13.4 Privacy Policy

The privacy policy must be made available to the player on the Technology Platforms in a clear and understandable manner and must be accepted by the player in the user account registration process. Any significant modification of the privacy policies requires to be communicated to and accepted by the player. The privacy policy must inform the player:

a) The personal identity information (personal data) required and collected for user account registration;
b) The policy must comply with Peruvian requirements for the protection of personal data.

in accordance with Law No. 29733 - Personal Data Protection Law and its regulations,

c) The player is entitled to:

i. Access, export or transfer your personally identifiable information;

ii. Exercise their rights of access, rectification, opposition and cancellation with respect to personal identity information in accordance with Law No. 29733 - Personal Data Protection Law and its regulations;

d) The rights and the possibility for a player to file a complaint with MINCETUR; and

e) Report the use of algorithms for automated decision making based on the information collected, including profiling. At a minimum, the decision-making logic should be disclosed.

13.5 Security of personally identifiable information

Any information obtained with respect to the gaming account, including personal identification information and authentication credentials, must be obtained in accordance with the privacy policy and Law No. 29733 - Personal Data Protection Law and its regulations. Personally identifiable information and player funds are considered critical assets for risk assessment purposes.

a) Any personally identifiable information that is not subject to disclosure in accordance with the privacy policy must be kept confidential, except when disclosure of the information is required by law. This includes, but is not limited to:

i. The amount of money credited, debited or present in any particular gaming account;

ii. The amount of money wagered by a particular player in any game;

iii. The account number and authentication credentials identifying the player; and

iv. The name, address and other information in possession of the Holder that identifies the player to anyone other than MINCETUR.

b) Procedures should be established for the security and disclosure of personally identifiable information, funds in a gaming account, but not limited to:

i. The designation and identification of one or more employees with primary responsibility for the design, implementation and ongoing evaluation of these procedures and practices;

ii. The procedures used to determine the nature and extent of all information collected, the location of all information stored, and the storage devices on which such information may be stored for the purpose of storage or transfer;

iii. The measures to be used to protect the information against unauthorized access; and

iv. The procedures used in the event that the Data Controller determines that a data security breach has occurred, including notification to the competent authority for the protection of personal data.

c) Players are given a method to apply:

i. Confirm that your personal identity information is in process;

ii. Access to a copy of your personally identifiable information, as well as any other information about the processing of personally identifiable information;

iii. Updates to your personal identity information; and

iv. Your personally identifiable information deleted and/or to impose restrictions on the processing of your personally identifiable information.

d) There shall be procedures in place to register and process player requests, including keeping records of such requests and providing reasons to the player when requests are denied or rejected. The Registrant must explain to the player the reasons why the request was not attended and also provide him/her with the necessary information on the possibility of filing a complaint before MINCETUR whenever it is linked to the operation of remote gaming and remote sports betting.

e) At the player's request, the Holder sends the player the personal identity information they have received from the same player, in a structured, commonly used and readable format. This only applies to:

i. Personal identity information that the player has provided to the Registrant or personal identity information that is processed by automated means (this excludes any paper records); and

ii. Cases where the basis for the processing is the consent of personal identity information, or that the data is in the process of fulfilling a contract or preparatory steps for a contract.

f) The player has the right to object to the processing of personal identity information:

i. Based on legitimate interests or the performance of a task in the public interest or in the exercise of official authority;

ii. Used in marketing directly, including profiling to the extent it is related to such marketing activities; and

iii. For scientific or historical research purposes or with statistical purposes.

g) There will be procedures in place for the Registrant to comply with requests from players to have personally identifiable information deleted and/or to prevent or restrict the processing of personally identifiable information, including, in the following circumstances:

i. Where personally identifiable information is no longer needed in connection with the purpose for which it was originally collected/processed;

ii. When the player withdraws consent;

iii. When the player objects to the processing of personally identifiable information and there is no overriding legitimate interest in continuing the processing;

iv. The personally identifiable information was unlawfully processed; or

v. Personally identifiable information must be deleted to comply with a legal obligation.

h) MINCETUR prohibits the Holder from using automated decision making through algorithms that:

i. Produces legal effects for the player; or

ii. Affect the player's decisions, behavior and choices that condition him/her to take a certain action.

13.6 Maintenance of Player Funds

Procedures should be established to ensure that all financial transactions are conducted in accordance with local trade regulations and requirements established in the approved Technical Standards.

a) When financial transactions cannot be performed automatically by the Technology Platform, procedures for "Financial Transactions" contained in the approved Technical Standards must be established.

b) When financial transactions are permitted through electronic funds transfer (EFT), the Holder must have measures and controls in place to security measures to prevent EFT fraud. A failed EFT attempt may not be considered fraudulent if the player has successfully performed an EFT on a previous occasion with no outstanding counter charges. Otherwise, the Holder must do all of the following:

i. Temporarily block the gaming account for fraud investigation after five consecutive failed EFT attempts within a ten-minute time period or a period determined by MINCETUR. If there is no evidence of fraud, the block may be removed; and

ii. Suspend the gaming account after five additional consecutive unsuccessful EFT attempts within a ten-minute period or a period to be determined by MINCETUR.

c) Positive player identification or authentication must be completed before the player can withdraw funds.

d) The Holder does not allow a player account to be overdrawn unless caused by payment processing problems beyond the control of the Holder.

e) A player's request to withdraw funds (deposited and authorized funds or wagers won) must be completed by the Holder within a reasonable period of time, unless there is an unresolved player claim/dispute or pending investigation. This investigation must be documented by the Holder and must be available for review by MINCETUR.

f) The Registrant must establish authorization or security procedures to ensure that adjustments to the gaming account can only be made with authorization, and these changes can be audited.

13.7 Limitations

The Technological Platform has methods for the player to impose limitations on deposits and bets.

Likewise, the Technology Platform must establish a method for the Registrant to impose limitations on the game parameters:

a) Established by the player and implemented by the Holder, it is only possible to reduce the severity of limitations after a period of twenty-four (24) hours has elapsed, which change is made known to the player.

b) Players must be previously informed of all limits imposed by the Holder, as well as their effective date. The updating of the limits imposed by the Holder must be consistent with what the player has been informed.

c) After receiving a self-imposed or imposed limitation order from the Holder, the latter must ensure that all specified limits are immediately implemented or at the time indicated to the player (next session, next day).

13.8 Exclusions

The Technology Platform has methods for the player to exclude himself from the game for a specific or indefinite period. Likewise, the Technology Platform must establish a method for the Holder to exclude the player:

a) Players should receive a communication about the status of the exclusion.

b) Immediately after receiving the exclusion order, the Technology Platform must not accept any wager or deposit from the player until the exclusion is withdrawn.

c) For the duration of the exclusion, the player should not be prevented from withdrawing part or all of his account balance as long as the Holder proves that the funds are authorized and that the reason(s) for the exclusion does not prohibit a withdrawal (scam, fraud, etc.).

d) No advertising or marketing content is directed to players excluded from the game.

e) The information regarding the player's self-exclusion period must be stored in the game account.

13.9 Inactive accounts

A gaming account is considered inactive according to the conditions specified in the terms and conditions. Procedures must be established for:

a) Allow player access to their inactive account only after additional identity verification;

b) Protect inactive player accounts containing funds against unauthorized access, changes or deletion; and

c) Process unclaimed funds from inactive player accounts, including returning remaining funds to the player if possible.

13.10 Account Closing

Players are given a method to close their player account at any time, unless the Holder has temporarily excluded a player from the game. Any remaining balance is returned to the game account.

Section 14. General operating procedure

14.1 Holder Reservations

The Registrant must establish processes to maintain and protect adequate cash reserves, as determined by MINCETUR, including separate accounts to ensure segregation between player accounts and operational funds used to cover any liability of the Registrant.

14.2 Protection of player funds

The Holder must maintain an account opened in a financial or banking institution under the supervision of the Superintendence of Banking, Insurance and Private Pension Fund Administrators (SBS), in which the deposits for bets made by the players are kept exclusively and the intangibility of the deposits made for the referred concept is guaranteed, The holder of the authorization of the technological platform shall be responsible for the costs for the opening and maintenance of the financial or bank account, as well as for the payment of any taxes that may be levied on the movements of the deposits made.

14.3 Taxes

The Registrant must establish a process to identify all revenues that compose the taxable base of the Remote Gaming and Remote Sports Betting Tax and provide the necessary information in accordance with the requirements set forth in the current regulations.

14.4 Complaint/dispute process

The Holder must establish a method for the player to make a claim/dispute, and enable the player to notify MINCETUR if this claim/dispute has not been or cannot be dealt with by the Holder.

a) Players must be enabled to make a record of the claim/dispute on a 24/7 basis.

b) Records of all correspondence related to a claim/dispute must be maintained for a period of five (05) years or as specified by MINCETUR.

c) A documented process must be established between the Holder and MINCETUR for the process of reporting and resolution of the complaint/dispute.

14.5 Player protection information

Player protection information must be available to the player. Player protection information shall include at a minimum:

a) Information about the potential risks associated with excessive gambling, and where to get help for a gambling problem;
b) A statement that no person under the age of majority is permitted to participate in the game;
c) A list of available options for player protection that can be used by the player, as well as self-imposed exclusion, and information on how to use these options;
d) Mechanisms in place that can be used to detect unauthorized use of your account, as well as review of the financial statement against recognized deposits;
e) Contact information or other means to report a complaint/dispute related to the operation or services provided by the Technology Platform; and
f) MINCETUR's contact information and/or a link to its website for issues related to the operation of remote gaming and remote sports betting.

14.6 Responsible Gaming

The Registrant must have policies and procedures in place to facilitate interaction with players whenever their gambling behavior indicates a risk of developing a gambling problem. Employees who interact directly with gamblers should receive training to ensure that they understand the problems associated with gambling and know how to respond to them.

14.7 Lines of action for responsible gaming

The Holder must promote the following lines of action:

a) Awareness-raising: raising awareness and informing the population about the characteristics of pathological gambling and its risks. Disseminate preventive measures, as well as the availability of access to free treatment from assistance devices;
b) Prevention: implementing actions aimed at educating and raising awareness about responsible gambling behaviors, in order to minimize risks and ensure the protection of the most vulnerable groups. Also encouraging healthy gambling among children, adolescents and the elderly, through the creation of recreational spaces;
c) Guidance and Assistance: to guarantee access to information and interdisciplinary treatment of gambling addiction through different assistance devices;
d) Research: to develop lines of research on the expansion of gambling and the new modalities that arise as a result of market developments. To deepen studies on the prevalence of pathological gambling and gamblers' behaviors.

14.8 Chat Functions

There must be a defined procedure for cases where the Holder provides the use of chat functions that allow the player to communicate directly with the Holder and/or other players, including the maintenance of chat logs for a period of ninety days or as required by MINCETUR. In addition, email correspondence between the player and the Holder is also maintained for the same period of time.

Section 15. Rules of the game and content

15.1 Rules of the game

Rules of the game refers to any written, graphic, and audio information provided to the public with respect to the operations of remote gaming or remote sports betting. The Holder must adopt and adhere to the complete rules of the game offered.

a) The rules of the game must be complete, unambiguous, and not misleading or unfair to the player.
b) The rules of the game that must be presented aurally (by sound or voice) must also be shown in written form.
c) The rules of the game should be displayed in a color that contrasts with the background color to ensure that all information is clearly visible/legible.
d) The Holder must keep a record of any changes in the game rules related to the games.
e) When game rules are altered for games being offered, all rule changes must include a date and time stamp showing the applicable rule for each period. If multiple rules apply to a game, the Holder must apply the rules in effect when the wager was accepted.

15.2 Content of the rules of the game

The following information must be available to the player. The functionality to display the information required in this section must be displayed by the player interface or from a page accessible to the player:

a) The methods of applying funds to a player's account (cash, wire transfer, draft, debit instrument, credit card, electronic funds transfer, etc.), including a clear and concise explanation of all fees (if applicable);
b) Procedures addressing any unrecoverable hardware/software malfunction, including if this process results in the voiding of any wager, game or payout;
c) The procedures for resolving interruptions caused by a discontinuity.

i. Of the player in the Technology Platform where the outcome of a game is affected by the time to respond to a game event;
ii. In the transmission of data from the network server during an event;

d) What happens to bets placed by the player but which remain undecided in interrupted games, including how they are handled when they remain undecided beyond the specified time period;
e) A description of the restricted players, including any applicable limitations on their wagering (athletes must not bet on their sport);
f) For each progressive jackpot or incremental progressive jackpot:

i. The imperfections of the media for the game and how it may affect players in relation to the jackpot;
ii. Any maximum payout limit or "cap" and/or time limit that is compatible with the jackpot;
iii. How the jackpot is funded and determined; and
iv. Any planned or unplanned forfeiture of the jackpot, including how outstanding contribution amounts are treated to ensure player equity.

15.3 Bonus Awards (promotions)

A Holder may offer bonus prizes, which are credits and/or prizes not included in the paytable of a game and are based on predetermined events or criteria established by the parameters of the Technology Platform.

a) Players can access clear and unambiguous terms in the game rules related to the bonus prize offers available, which include the following as a minimum:

i. The date and time presented;
ii. The date and time the offer is active and expires;
iii. Player eligibility, including limitations on participation;
iv. Any restrictions or terms on withdrawals of funds;
v. Wagering requirements and limitations by game type, events, markets, game theme and/or paytable;
vi. How the player is notified when he/she has received a bonus award;
vii. The order in which the funds are used for wagering; and
viii. Cancellation rules.

b) A Holder provides a clear and visible method for a player to cancel participation in a bonus prize offer that uses restricted bonus credits.

i. Upon cancellation request, the Holder informs the player about the amount of his unrestricted funds that are returned upon cancellation and the value of the restricted bonus credits that are removed from the gaming account.
ii. If the player chooses to proceed with cancellation, the player's remaining unrestricted funds in a gaming account are returned in accordance with the terms of the offer.

c) Once a player has fulfilled the terms of a bonus prize offer, the Holder does not limit the prizes won while participating in the offer.

15.4 Competitions/Tournaments

A competition/tournament, which allows a player to acquire or be offered the opportunity to participate in competitive play against other players, may be admitted if it complies with the following rules:
.

a) The rules must be available for the player to review prior to registration for the competition/tournament and must include at a minimum:

i. All conditions that registered players must meet in order to register and advance in the competition/tournament;
ii. Specific information pertaining to a single competition/tournament including prizes and distribution of funds based on specific results;
iii. The name of the organization (or persons) that conducted the competition/tournament on behalf of, or in conjunction with the Holder (if applicable).

b) Procedures should be established to record the results of each competition/tournament and disseminate them to the public for review by registered players for a reasonable period of time. After being publicly announced, the results should include the following information:

i. Name of the competition/tournament;
ii. Date(s)/time(s) of competition/tournament;
iii. Total number of registrations;
iv. Total amount of competition/tournament entry fees;
v. Total prize fund;
vi. Amount paid for each winning category.

For free competitions/tournaments, the required information mentioned above must be recorded except for the number of entries, entry fee and total prize fund.

Section 16. Remote Gaming Procedures and Controls

16.1 Evaluation of Theoretical and Actual Return Percentages for the Player

The Registrant must maintain accurate and up-to-date documentation (PAR sheets) indicating the percentages Theoretical return to player (RTP) for each home banking game based on the appropriate levels of credits wagered, as well as the number of credits that can be played, the payout schedule and other descriptive information for the particular type of game. Additionally:

a) Records should be maintained for each game indicating the initial RTP player return percentage, the dates and type of changes made that affect the game's RTP player return percentage, and the recalculation of the RTP player return percentage due to the changes.
b) Each change to the return to player percentage RTP of a game, which includes adding and/or changing the progressive jackpot or increasing the jackpot, results in that game being treated as new for all reports and records.
c) If bonus prizes are included in game reports and records, it is in a manner that avoids distorting the actual return-to-player RTP percentages of the affected pay tables.
d) The Unitholder must have procedures in place to periodically compare the percentage of return to the RTP and actual player to identify, investigate and resolve large variations between these two values.

16.2 GNA Game Monitoring and GNA Results

The Registrant must have procedures in place to monitor GNA play and performance on a periodic or defined volume basis as required by MINCETUR. The purpose of monitoring is the early detection of abnormal behavior to allow for appropriate and timely corrective action. Any abnormality (Actual percentage return to the PRT player for the period falls outside the expected range) results in an error that is recorded and escalated for investigation. Best practice monitoring includes independent mapping between GNA output and game symbols verifying game symbol usage. GNA output game symbol records can be maintained and verified as a monitoring exercise.

16.3 Deactivation of the Game

Procedures are established for disabling a game or gaming activity. When a game or gaming activity is disabled, an entry must be made in an audit trail that includes the date and time it was disabled and the reason for it.

16.4 Suspended Game Management

Procedures for handling suspended games are established. If a game cannot continue due to an action of the Technology Platform, the Holder must:

a) Return all bets to the players of that game;
b) Update the credit meter(s) or game account balance(s) and game history accordingly;
c) Inform MINCETUR of the circumstances of the event; and
d) Disable the game if the game is likely to be affected by the same bug.

16.5 Progressive Jackpot or Incremental Progressive Jackpot Procedures

The Registrant must establish, maintain, implement and comply with internal control procedures for jackpot operations, including the following:

a) When jackpot contributions are part of the return-to-player (RRP) calculations, ensuring that the contributions are not assimilated into income;
b) Jackpot adjustments and transfer, as admitted.

c) For large jackpots exceeding a particular value as defined by MINCETUR:

i. Jackpot verification and payment procedures, including independent reconciliation and Holder's signature;
ii. Payment when multiple jackpot activations occur and there is no definitive way of knowing which trigger occurred first (unless handled automatically by the Technology Platform); and
iii. Disbursement options for major awards, including information for periodic payments;

d) For jackpot with parameters that can be configured after initial setup, performing an independent reconciliation of jackpot contributions and prizes to ensure that all jackpot increments are deducted:

i. They have been paid to players as jackpot rewards;
ii. Shown as part of jackpot payments; or
iii. They are held in separate accounts, which can be shown to be paid to players as part of future jackpot payments.

e) Jackpot dismantling procedures, including procedures for the distribution of contributions to another jackpot;
f) At least monthly, check:

i. The correct operation and the balances and movements of the jackpot;
ii. That, once the jackpot prize has been won, the conditions do not change until it has been credited to the winners' gaming account;
iii. That the procedure for determining winners works correctly. The procedure should not permit the introduction of winners who do not meet the conditions for being awarded prizes, nor should it not allow those who do meet the conditions to be considered winners; and
iv. Award prizes to the players listed as winners.

Section 17. Procedures and Controls for Peer-to-Peer (P2P) Gaming Sessions

17.1 Associated Players and Proposals

The Registrant must have processes in place to ensure that the player is not disadvantaged by players playing with house money (shills) or proposition players participating in a P2P gaming session. The following risks are expected to be mitigated:

a) The associated players and proposals must be clearly indicated to all other players for that P2P game session;
b) Holder controls mitigate the conflict between the role of the associated (shill) or proposal player and the role of the game assistant who has access to the operating environment (both physically and virtually) to be able to manipulate games or have information not available to all other players and be able to take advantage of it;
c) The Holder does not benefit from the move;
d) If the associated or proposed player's wager is funded by the Holder, neither the Holder nor the associated or proposed player can benefit from the game, the funds cannot be withdrawn, so they are ultimately lost/played; and
e) Procedures are established to address the risk that the associated or proposed player is motivated to protect personal wagers further from the stimulating gambling assignment. If the associated or proposed player risks private wagering, then the associated or proposed player does not have any knowledge of software or other Personally Identifiable Information (the associated or proposed player is a bona fide independent contractor with no prior relationship with the Registrant).

17.2 P2P Game Session Tracking

The Registrant has a process to track all P2P gaming sessions for each player, including tracking:

a) To the game information recorded for each game, including its opposing players; and
b) The player's choice of P2P game session, as well as instances where the player repeatedly enters and exits P2P game sessions without playing until he/she reaches his/her preferred P2P game session.

17.3 Reporting Suspicious Players

The Holder provides a method for a player to report suspected cheating, collusion or use of bots or other unauthorized player software by others to create an unfair advantage during the P2P gaming session.

Section 18. Procedures and Controls of Remote Sports Betting

18.1 Probabilities/Payments and Prices

Procedures should be established for setting and updating odds/payments and prices including providing the public with current odds/payments and prices, changing odds/payments and prices as necessary to handle exceptions, and correctly and periodically recording odds/payments and prices.

18.2 Statistics/Line Data

The Registrant must ensure that all statistics/line data that is available to the player with respect to an event is maintained accurately and appropriately updated. As required by MINCETUR, the Holder must implement controls for:

a) Reviewing the accuracy and currency of all line/statistical services; and
b) When an error occurs that results in the loss of communication with the line/statistical services, the error must be entered along with the date and time of occurrence, its duration, character, and a description of its impact on the operation of the Technology Platform. This information must be maintained for a period of ninety (90) days, or as specified by MINCETUR.

18.3 Suspend markets or events

Procedures should be established to suspend markets or events (stop accepting bets for the market(s) associated with this event). When play is suspended for an active event, an entry should be made in an audit trail that includes the date and time of the suspension and the reason.

18.4 Bet Cancellations

Betting transactions cannot be modified except to be cancelled according to the assumptions contemplated in paragraph l) of article 37 of these regulations and informed in the privacy policy published by the Holder. An additional period of time may be offered to allow players to request that placed bets be voided. The following requirements apply to the cancellation of bets:

a) Player-initiated cancellation requests may be authorized in accordance with the cancellation policy.

b) Cancellations initiated by the Holder must provide the player with a reason for the cancellation.

18.5 Betting Period

There must be documentation to indicate how the betting period is controlled. This includes all instances when the betting period is initially opened, when it is closed, or any time in this period when a bet cannot be placed (odds/payouts and prices are being updated).

18.6 Results

Prior to announcing the results publicly and declaring the winners, a policy should be established for confirmation of the results, unless this is automated by external transmission. If external transmission is used, procedures should be established for cases where access to external transmission is not available. A procedure for handling changes in results should also be established.

Section 19. Monitoring Procedures

19.1 Collusion and Fraud Monitoring

The Holder takes measures designed to reduce the risk of collusion or fraud, including procedures to:

a) Identify and/or refuse to accept suspicious wagers that may indicate cheating, manipulation, interference with the regular conduct of a game or violations of the integrity of any game or event on which wagers were placed;
b) Reasonable detection of irregular patterns or series of bets to prevent player collusion in P2P gaming sessions, including the following:

i. Throwing chips - two or more players help each other to stay in the game, leading to losses and, therefore, to an exchange of chips even with winning combinations certainly;
ii. Loose play - one or more players forfeit play against another player in situations where such behavior is unreasonable according to normal playing practices (a player drops out of the game even if the score is safe);
iii. Best hand game - Between two or more players, only the one who has the best score always plays, while the other or others leave the game; and
iv. Chat collusion - Collusion is achieved through the exchange of relevant information related to the progress of the game or series of games.

c) Reasonable detection and prevention of situations where in-game players may be using automated programs or other unauthorized player software to create an unfair advantage during game play, such as:

i. Projecting or predicting the outcome of a game;
ii. For card games, tracking of cards played and cards remaining to play;
iii. Analyze the probability of a game-related event occurring; or
iv. Analyzing the strategy for playing or betting on a game, unless permitted by the rules of the game

d) Monitor and detect events and/or irregularities in trading volume or changes in probabilities/payments and prices that may indicate suspicious activity, as well as all changes in probabilities/payments and prices and/or suspensions throughout an event.
e) Detect impersonation by analyzing sudden changes in a player's behavior, and in particular the value of deposits or withdrawals, to prevent the user's account from being accessed by a third party.

19.2 Money Laundering Monitoring (MLA)

The Registrant is required to develop and implement Money Laundering Monitoring procedures and policies that adequately address the risks posed by remote gaming or remote sports betting in accordance with the rules of the Money Laundering and Terrorism Financing System (SPLAFT) issued by the SBS. At a minimum, the Money Laundering Monitoring procedures and policies must provide for:

a) A system of internal controls to ensure ongoing compliance with the regulations applicable to Money Laundering Monitoring;
b) Up-to-date training of employees in the identification of unusual or suspicious transactions;
c) Assignment of a person or persons to be responsible for all areas of MLA by the Registrant, including the reporting of unusual or suspicious transactions;
d) Necessary mechanisms for the identification and notification of unusual or suspicious activities, including the concepts that originate credits in the gaming account in order to identify the origin of the funds;
e) Ensure that transactions aggregated over a defined period may require further due diligence checks and may be reported to MINCETUR, Financial Intelligence Unit (FIU) or other State entity, as appropriate; and
f) Use of any automated data processing system to help ensure compliance;

Section 20. Specifications of remote sports betting gaming halls

20.1 Remote sports betting gaming hall verification audit

The remote sports betting gaming room must comply with the applicable aspects of the appropriate policy and/or procedure documents as determined by the Registrant in consultation with MINCETUR.
To maintain the integrity of gaming operations, the premises may be subject to an additional verification audit as required by MINCETUR.

20.2 Sports betting equipment

The remote sports betting gaming venue must provide a secure facility for its operation, and use of sports betting equipment, including betting terminals, visual displays, and communication equipment. Safety policy and procedures must be established and reviewed periodically to ensure that risks are identified, mitigated and secured in emergency plans. In addition:

a) Sports betting equipment must be installed in accordance with a specific plan and records of all installed sports betting equipment must be maintained.
b) Sports betting equipment should be located or protected to reduce the risks of:

i. Opportunities for unauthorized access;
ii. Power failures; and
iii. Other interruptions caused by failures in support utilities.

c) Access to the sports betting equipment by an employee must be controlled by a secure registration procedure or other secure process approved by MINCETUR to ensure access by authorized employees only. It must not be possible to modify the configuration settings of the sports betting equipment without an authorized secure process.
d) A user session, when supported by the sports betting equipment, is initiated by the

employee by accessing their user account using their secure username and password or an alternative method of employee identification, as permitted by MINCETUR.

i. All available options presented to the employee must be related to their user account.
ii. If the sports betting equipment does not receive input from the employee within five minutes, or a period specified by MINCETUR, the user's session must go into timeout or lock, requiring the employee to re-establish access to continue.

e) To ensure its continued availability and integrity, sports betting equipment must be maintained, inspected and serviced at regular intervals to ensure that it is free of defects or mechanisms that may interfere with its operation.
f) Prior to removal or reuse, the sports betting equipment containing the storage media must be checked to ensure that any licensed software, gaming account information, and other confidential information has been securely removed or overwritten (not just erased).

20.3 Sports betting operations in remote sports betting parlors

The following procedures apply to sports bets placed in remote sports betting gaming halls:

a) Procedures that provide an adequate response to any security problem in the room;
b) Procedures to prevent any person from tampering or interfering with the operation of the betting or sports betting terminal;
c) Procedures to describe the operations and maintenance of betting terminals;
d) Procedures to ensure compliance with the security requirements established by MINCETUR for the operation of self-service betting devices (betting terminals).
e) Procedures for wagering transactions using a Sales Betting Terminal, including:

i. Accept bets from players only during the betting period;
ii. Notify players if their wagering attempt is rejected;
iii. Require the user's account ID or proceed to register the player, as appropriate;
iv. Notify any changes in odds/payments or prices that occur while a wager is being processed;
v. Associate the player's transactions to his gaming account;

f) Procedures for processing cancelled events and eliminated selections for bets with multiple events (parlays), including returns to players that were not automatically executed by the Technology Platform, and a record must be kept.

20.4 Security and recording

The remote sports betting gaming venue must install, maintain, and operate a security platform that has the capability to continuously monitor and record unobstructed views of all wagering and financial transactions in addition to dynamic visual displays of game information. Procedures should be established to ensure that the recording:

a) Cover the defined betting areas in sufficient detail to identify any discrepancies;
b) You must prevent third party interference or deletion of your information;
c) It may be reviewed by the Registrant and/or MINCETUR in case of a claim/dispute by the player or when MINCETUR so provides; and
d) It is maintained for at least fifteen (15) days as required by MINCETUR.

SECTION B

Section 21. Audit of Technical Security Controls

This section establishes the technical security controls that are reviewed by the authorized Certification Laboratory or MINCETUR in an operational audit as part of the evaluation of the Technology Platform, including, but not limited to the review of operational processes that are critical for regulatory compliance and the proper functioning of the Technology Platform, as well as penetration tests focused on the external and internal infrastructure, in addition to applications that transfer, store and/or process personal identity information and/or other confidential information, the evaluation of information security services, cloud services, and payment services (financial institutions, payment processors, etc.), among other requirements that may be established in mandatory Directives. The security controls defined in this Technical Standard apply to the following critical components of the Technology Platform:

a) Components that record, store, process, share, transmit or obtain personally identifiable information and other sensitive information (validation numbers, authentication credentials, etc.);
b) Components that generate, transmit, or process the random numbers used to determine the outcome of gaming events;
c) The system for the transmission of economic and technical data to MINCETUR's Data Center;
d) The system, applications, views, queries, scripts that generate MINCETUR reports.
e) Components that store the results or current status of a player's bet;
f) Entry and exit points of the above mentioned components (other Technology Platforms with the ability to communicate directly with the main critical Technology Platforms); and
g) Communication networks that transmit personally identifiable and other confidential information.

21.1 Integrity and Security Assessment

The Holder must, within ninety (90) days after the commencement of its operations, and at least one (1) day after the commencement of its operations, and at least one (1) year after the commencement of its operations
(01) once a year, perform an integrity and security assessment of the Technology Platform with an authorized Certification Laboratory, taking into account the following:

a) The scope of the integrity and security assessment of the Technology Platform should include, at a minimum, the following:

i. A vulnerability assessment of all digital platforms, mobile applications and internal, external and wireless networks, in order to identify vulnerabilities of all devices, Technology Platforms and applications that transfer, store and/or process personally identifiable and/or other sensitive information connected to or present on the networks;
ii. A penetration test of all digital systems, mobile applications, internal, external and wireless networks to confirm whether the identified vulnerabilities of all devices, systems and applications are susceptible to breach;
iii. A review of the firewall rules to verify the firewall's operational status and effectiveness.

of your security configuration and rule sets made on all perimeter firewalls and internal firewalls;

iv. An evaluation of information security controls in accordance with the technical standards of the security industry, Law No. 31557, these Regulations and mandatory Directives;

v. If the Registrant uses a cloud service provider, an assessment is performed on the access controls, account management, logging and monitoring, and on the security configurations of the Technology Platform its components and services hosted in the cloud;

vi. An evaluation of information security services, payment services (financial institutions, payment processors, etc.), and any other remote gaming services or sporting events that may be offered directly by the Registrant or that involve the use of third parties in accordance with the provisions set forth herein; and

vii. Any other specific criteria or standards for the evaluation of the integrity and security of the Technological Platform that may be established by MINCETUR by means of Directives.

b) The complete report of the authorized Certification Laboratory on the evaluation must be submitted to MINCETUR within thirty (30) days from the completion of the evaluation and must include the following:

i. Scope of the review;

ii. Name of the authorized Certification Laboratory, professional responsible for the evaluation;

iii. Date of evaluation;

iv. Findings;

v. Recommended corrective actions, if applicable; and

vi. The measures adopted by the owner in response to the findings and the recommended corrective action.

c) If the report of the authorized Certification Laboratory recommends a corrective action, the Contractor must provide MINCETUR with an action plan and any risk mitigation plan detailing the Contractor's actions and the timeline to implement the corrective action. Once the corrective action has been taken, the Registrant provides MINCETUR with documentation demonstrating its implementation.

Section 22. Operation and Security of the Technology Platform

The Technological Platforms of remote gaming and sports betting must have the necessary physical and logical access controls, network security and risk management in accordance with the regulations in force regarding information security and/or comply with international standards and/or good practices, in order to comply with the provisions of Law No. 31557, these Regulations and mandatory Directives.

The Registrant must provide MINCETUR with information on the location of all servers and other equipment used for remote gaming or remote sports betting, which must be located in one or more data centers with a guaranteed availability of 99.982%.

22.1 Technology Platform Procedures

The Holder is responsible for documenting and following the procedures and international security standards applicable to the Technology Platform, including the following procedures:

a) Monitor all critical components and data transmission of the Technology Platform, including communication, data packets, networks, in addition to the components and data transmission of any third-party services used, with the objective of ensuring integrity, reliability and availability;

b) Maintain all security aspects of the Technology Platform to ensure secure and reliable communication, including protection against hacking or tampering;

c) Define, monitor and document, as well as report, investigate, respond and resolve security occurrences, including detecting non-compliance and possible or actual hacking or tampering of the Technology Platform;

d) Monitor and optimize resource utilization and maintain a record of the Technology Platform's performance, including a function to collect performance reports;

e) Investigate, document and resolve the malfunction, including the following:

i. Determination of the cause of the malfunction;

ii. Review of applicable records, reports, files and security logs;

iii. Restoration or replacement of the critical component;

iv. Verification of the integrity of the critical component before restoring its operation;

v. Complete an occurrence report for MINCETUR documenting the date, time and reason for the malfunction with the date and time of platform recovery; and

vi. Cancel games, fees and payments if full recovery is impossible.

22.2 Physical location of servers

The Technology Platform servers may be hosted in one or more secure data centers, within one or more facilities and must:

a) Have sufficient protection against alteration, tampering or unauthorized access;

b) To be equipped with a surveillance system;

c) Be protected by security perimeters and appropriate access controls to ensure that access is restricted to authorized personnel only;

i. Physical access must have a multi-factor authentication process unless the facility is staffed at all times;

ii. Any physical access attempt is recorded in a secure file; and

d) Be equipped with controls to provide physical protection against damage from fire, flood and other forms of natural or man-made disasters (hurricane, earthquake, etc.).

22.3 Logical access control

The Technology Platform must have logical access controls against unauthorized access by authentication credentials, such as passwords, multi-factor authentication, digital certificates, biometrics, and other access methods (magnetic stripe, proximity cards, integrated chip cards).

a) Each user account should have its own authentication credentials, the delivery of which should be controlled by a formal process, including a periodic review of access rights and privileges. The use of generic accounts is limited and, when used, the reasons for their use should be formally documented.

b) Registration of authentication credentials for secret information must be done manually or by services that automatically register authentication changes and force changes to authentication credentials.

c) Any authentication credentials stored on the Technology Platform must be encrypted or subjected to cryptographic algorithms that comply with current industry-accepted standards, such as ISO/IEC 19790, FIPS 140-2 or equivalent.

d) A workaround for resetting authentication credentials (lost password) must also be secure, just like the primary method. A multi-factor authentication process is used for these purposes.

e) Lost or compromised authentication credentials and authentication credentials of non-active users should be deactivated, secured or deleted as soon as possible.

f) The Technology Platform should have multiple levels of security access to control and restrict different types of access to the server, including viewing, changing, or deleting critical files and directories. Procedures should be established to assign, review, modify, and remove access rights and privileges for each user, including:

i. The ability of user account management to provide adequate segregation of duties;

ii. Limitation of users who have the required permissions to adjust critical parameters of the Technology Platform;

iii. The application of appropriate authentication credential parameters, such as minimum length and expiration period.

g) Procedures should be established to identify and flag suspicious accounts to prevent unauthorized access, including:

i. Have platform administrator notification and user blocking or audit trail entry, after a maximum number of three incorrect authentication attempts;

ii. Alerting of suspicious accounts where authentication credentials may have been stolen; and

iii. Invalidate accounts and transfer critical information from the stored account to a new account.

h) Any attempt to logically access the Technology Platform and its components must be recorded in a secure file.

i) The use of utilities that may override the controls of the application or operating platform must be strictly restricted and controlled.

j) Restrictions on connection time, as well as on session timeout and remote access, among others, should be used to provide additional security for high-risk applications.

22.4 User authorization

The Technology Platform must have the following user authorization requirements implemented:

a) A secure and controlled mechanism must be used to verify that the critical component is being accessed by authorized personnel on a regular basis.

b) When used, automated equipment identification methods to authenticate connections from specific locations and equipment should be documented and should be included in the review of access rights and privileges.

c) Any authorization data communicated by the Technology Platform for the purpose of identification must be obtained at the time of requesting the platform and must not be stored in the platform component.

d) When user sessions are tracked for authorization, user session authorization information is always created randomly, in memory, and deleted after the user session has ended.

e) A secure and controlled mechanism should be used to verify that the critical component has been accessed by authorized personnel on a regular basis upon request.

f) When used, automated equipment identification methods for authenticating connections from specific locations and equipment are documented and included in the review of access rights and entitlements.

g) Any information relating to the authorization communicated by the Platform for identification purposes must be obtained at the time of the Platform request and not stored in the same component.

h) In order to authorize user sessions, authorization information is always randomly created and stored in memory, and is deleted after the user session has ended.

22.5 Server programming

The Technology Platform must be sufficiently secure in order to prevent any server-side programming capabilities that may result in database modifications. However, network or system administrators perform authorized network infrastructure maintenance or troubleshooting of the application, with sufficient access rights. The server is also protected from unauthorized execution of mobile code.

22.6 Verification procedures

This section establishes the obligation of the Contractor to verify that the critical components of the control program of the Technology Platform in the production environment are identical to those approved by the authorized Certification Laboratory as stated in the certificate of compliance.

The verification procedure:

a) Digital signatures of the critical components of the control program must be obtained in the production environment using a process reviewed and validated by the authorized Certification Laboratory, and must be carried out:

i. After installation/upgrade of components;
ii. On power-up or recovery from a shutdown state;
iii. At least once every 24 hours; and
iv. On request.

b) The process should include one or more analytical steps to compare the signatures obtained from the critical components of the control program in the production environment with the signatures described in the certificate of compliance.

c) The result of this process must include the signature results obtained and the signatures described in the certificate of compliance, with the details of the result of the verification of each authentication of the critical control program and:

i. Be recorded in a Technology Platform file or report to be stored for a period of ninety (90) days;

ii. Be accessible by MINCETUR in a format that allows its recording, analysis and verification; and

iii. Be part of the Platform's records that are recovered in the event of a disaster or failure of equipment or software.

d) A communication failure of any component of the Technology Platform requires a notification of the authentication failure being communicated to the Holder and MINCETUR, as required.

e) A process should be established to respond to authentication failures, including determining the cause of the failure and performing the required corrections or reinstallations in a timely manner.

22.7 Electronic document retention system

The reports listed under "Reporting requirements" and "physical and logical access" contained in Technical Standards I and II and required by MINCETUR may be stored in a retention system.

electronic documents, provided in the Technological Platform:

a) It is correctly configured to maintain the original version along with all subsequent versions reflecting all report changes for reports that are stored in a modifiable format;
b) Maintains a unique verification signature for each version of the report, including the original;
c) You can retain and report a complete change log of all reports including who (user ID) made the changes and when (date and time);
d) Provides an indexing method to easily identify the report, including the following as a minimum (which can be entered by the user):

i. Date and time the report was generated;
ii. Application or platform that generated the report;
iii. Title and description of the report;
iv. User ID of the person generating the report;
v. Any other information that may assist in identifying the report and its purpose;

e) It is configured to limit access to modify or add reports to the Technology Platform by securing specific user account logic;
f) It is configured to provide a complete audit trail of all administrative user account activity;
g) It is adequately secured through the use of logical security measures (user accounts with appropriate access, adequate event log levels, and version control documentation, etc.);
h) Is physically secured with all other critical components of the Technology Platform; and
i) It is equipped to prevent interruption of reporting availability and data loss through best practice hardware and software redundancy and backup processes.

22.8 Team Management

All physical or logical equipment that houses, processes or communicates confidential information, including the equipment that constitutes the operating environment of the Technology Platform and/or its components, must be accounted for.

a) Procedures should be in place for adding new assets and removing assets from service.
b) Assets are disposed of safely using documented procedures.
c) A policy on the acceptable use of the equipment associated with the Technology Platform and its operating environment must be included.
d) The designated "owner" of each team is responsible for:

i. Ensure that information and equipment are properly classified in terms of their confidentiality, integrity, accountability and availability; and
ii. Define and periodically review access restriction and classification.

e) A procedure should be established to ensure that the recorded accounting for the equipment is compared with the actual equipment at least annually and appropriate action is taken with respect to discrepancies.
f) Copy protection can be implemented to prevent unauthorized duplication or modification of software, provided that:

i. The copy protection method is fully documented and submitted to the authorized Certification Laboratory to verify that the protection is functioning as provided; or
ii. The program or component responsible for applying copy protection can be checked individually.

g) Prior to disposal or reuse, assets containing storage media should be verified to ensure that any licensed software, as well as personal identity information and other confidential information has been securely removed or overwritten (i.e., not just deleted).

22.9 Critical Asset Register

A Critical Asset Register is maintained for any asset that affects the functionality of the Technology Platform or has an influence on how the platform stores/handles Personally Identifiable Information and other confidential information. The structure of the Critical Asset Register includes hardware and software components and the interrelationships and dependencies of the components. The following minimum elements must be documented for each asset:

a) The name/definition of each asset;
b) A unique identification that is assigned to each individual asset;
c) A version number of the asset listed;
d) Identify asset characteristics (platform component, database, virtual machine, hardware);
e) The "owner" responsible for the asset;
f) The geographical location of the hardware assets;
g) Relevance codes on the role of the asset in achieving or ensuring the following classification criteria:

i. Confidentiality of Personally Identifiable Information and other confidential information (identifying and transaction information);
ii. Integrity of the Technology Platform, specifically any assets that affect the functionality of the platform and/or influence how personal identity information and other confidential information is stored and/or handled;
iii. Availability of personal identity information and other confidential information; and
iv. Responsibility for user activity and how much influence the asset has on user activity.

22.10 Physical and logical accesses to the Technological Platform

22.10.1 Audit

The Holders must provide MINCETUR and/or entity authorized by MINCETUR, physical or logical access to the Technological Platform to perform a comprehensive audit of critical control components or programs, critical files, services, integration services between Technological Platforms, Databases, applications, among other software or hardware components that MINCETUR deems necessary.

In the case of logical access, the Registrant must provide a secure access method by means of user and password or other mechanism that allows for a comprehensive audit of the Technology Platform, taking into consideration the following:

a) The Holder must establish a secure communication mechanism to its Technological Platform and that of its related service providers, as well as allow and facilitate at all times the remote audit to MINCETUR and/or entity authorized by MINCETUR, regardless of the physical location of its data centers;
b) MINCETUR may inform the Registrant of the date scheduled for the audit of the Technological Platform, as well as provide information on the activities to be performed and, if necessary, require the specialized support of the Registrant's personnel.
c) The personnel designated by the Contractor must provide the necessary facilities, access, permits and privileges to MINCETUR in order to comply with the scheduled audit. MINCETUR may carry out auditing activities

The corresponding means of proof must be obtained in accordance with the provisions of the LPAG.

d) If not otherwise required, it should be understood that the access provided to MINCETUR is read-only and has the necessary permissions and privileges to access the entire Technology Platform, services, applications, databases, among other software or hardware components deemed necessary without any filter. Once the access is finished, the Holder must close the secure access.

22.10.2 Real-time control and supervision of remote gaming and remote sports betting.

The Licensees must deliver to MINCETUR the remote accesses to the Technological Platform where the remote games and/or remote sports bets are exploited, in order to allow the control and supervision of the different modalities of remote games and/or remote sports bets in operation. The accesses have secure communication channels by means of user and password or other secure access method that does not allow vulnerability of the Technological Platform security. Likewise, the necessary privileges must be granted to carry out the control.

MINCETUR may require the specialized support of the Holder's personnel to carry out the inspection and control of the Technological Platform. MINCETUR may carry out the corresponding inspection activities and collect the necessary evidence in accordance with the provisions of the LPAG.

Section 23. Data Integrity

23.1 Data security

The Holder must provide a security approach within the production environment to ensure the secure storage and processing of data. The Technology Platform provides a logical means to secure personally identifiable and other confidential information, including accounting, reports, important events or other player and game data, against alteration, tampering or unauthorized access.

a) Methods for correct data processing, including validation of entries and rejection of corrupted data, must be implemented.

b) The number of workstations where critical applications or associated databases can be accessed is limited.

c) Encryption or password protection or equivalent security must be used for the files and directories containing the data. If encryption is not used, the Registrant shall restrict the view of the contents of such files and directories to users, and at a minimum provide for segregation of platform functions and responsibilities as well as monitoring and logging of access to such files and directories by any person.

d) The normal operation of all equipment containing the information must not include any option or mechanism that could compromise the data.

e) No equipment should have a mechanism in which an error results in the automatic deletion of data.

f) No equipment that maintains data in its memory should allow the removal of the information unless it has been transferred to the database or other secure component(s) of the Technology Platform.

g) Personal identity identification and other sensitive information must be stored in areas of the server that are encrypted and secured against unauthorized access, both externally and internally.

h) The production databases containing the data must be part of a network separate from the server of any player interface.

i) Data must be maintained at all times regardless of whether the server has power.

j) Data must be stored in a way to prevent data loss when parts or modules are replaced during normal maintenance.

23.2 Alteration of data

Alteration of accounting data, reports or significant events is not permitted without supervised access controls. In the event of any change in data, the following information must be documented or recorded:

a) Unique identification number for the alteration;
b) Data element altered;
c) Value of the data element before the alteration;
d) Value of the data element after alteration;
e) Date and time of the alteration; and
f) Personnel who made the alteration (user identification).

23.3 Frequency of backup

Implementation of the backup plan should occur at least daily or as specified by MINCETUR, however, all methods are reviewed on a case-by-case basis.

23.4 Storage Media Backup

Audit logs, Technology Platform databases, and any other relevant personal identity information or game data must be stored using reasonable protection methods. The Technology Platform must be designed to protect the integrity of this data in the event of a failure. Redundant copies of this data must be maintained on the platform with open support for backups and restoration, so that no failure of a single part of the platform can cause data loss or corruption.

a) The backup must be contained on non-volatile physical media, or an equivalent implementation of the architecture, so that, if the primary storage media fails, the Technology Platform functions and the auditing process of these functions can continue without loss of critical data. If hard disk drives are used as backup media, data integrity is guaranteed in the event of disk failure.

b) When the backup process is complete, the backup media are immediately transferred to a location physically separate from the location of the servers and data being backed up (for temporary and permanent storage).

i. The storage location must be secure to prevent unauthorized access and provide adequate protection to prevent permanent loss of data.

ii. Backup data files and data recovery components must be managed with at least the same level of security and access controls as the platform.

c) If the backup copy is stored on a Technology Cloud Platform, another copy can be stored on a different cloud platform or region.

23.5 Failure of the Technology Platform

The Technology Platform must have sufficient redundancy and modularity so that, if a single component or part of a component fails, the Technology Platform functions and the auditing process of these functions can continue without loss of critical data. When two or more components are linked, a procedure should be established so that the Technology Platform and the components are tested.

after installation, but before use in a production environment to verify that:

a) The process of all gaming operations between components must not be adversely affected by the restart or recovery of any component (transactions must not be lost or duplicated because of the recovery of one component or the other); and

b) After reboot or recovery, the components must synchronize the status of all transactions, data, and configurations.

23.6 Master reset accounting

The Holder must have the ability to correctly identify and process situations where a master reset of any component that affects gaming operations has occurred.

23.7 Requirements for recovery

In the event of a catastrophic failure in which the Technology Platform cannot be restarted in any other way, it must be possible to restore the Technology Platform from the last backup point and recover it in full. The contents of this backup must include the following critical information including, but not limited to:

a) The recorded information specified under the section "Information to be maintained" contained in the approved Technical Standards I and II;

b) Site or location specific information, as well as configuration, security accounts, etc..;

c) Current Technology Platform encryption keys; and

d) Any other platform parameters, modifications, reconfiguration (including participating sites or locations), additions, combinations, deletions, adjustments and parameter changes.

23.8 Uninterruptible Power Supply (UPS) Technology Platform Support

All components of the Technology Platform must be provided with adequate primary power. When the server is a stand-alone application, it must have an uninterruptible power supply (UPS) connected and must have sufficient capacity to allow for a proper shutdown that retains all personal identity information and other sensitive information during a loss of power. It is acceptable for the platform to be a component of a network that is supported by a network-wide UPS provided that the server is included as a UPS-protected device. A surge protection system should be used if it is not built into the UPS.

23.9 Business continuity and disaster recovery plan

A business continuity and disaster recovery plan must be in place to resume gaming operations if the Technology Platform's production environment becomes inoperable. Such plan considers disasters including, but not limited to, those caused by weather, water, floods, fires, environmental spills and accidents, malicious destruction, acts of terrorism or war, and contingencies such as strikes, epidemics, pandemics, etc. The business continuity and disaster recovery plan should:

a) Include a method of storing personal identity information and other sensitive information, including game data, to minimize loss. If asynchronous playback is used, the method for retrieving the information should be described or the potential loss of information should be documented;

b) Define the circumstances under which the plan is invoked;

c) Include the establishment of a recovery site physically separate from the site. The use of cloud platforms for this purpose is evaluated on a case-by-case basis;

d) Contain recovery guidelines detailing the technical phases required to restore game functionality at the recovery site; and

e) Include the process required to resume administrative operations of the game activities after activation of the recovered platform in various scenarios suitable for the operational context of the platform.

Section 24. Communications

This section covers wired and wireless communication methods, including communications via the Internet or a public or third-party network.

24.1 Connectivity

Only authorized devices must be allowed to establish communication between critical components of the Technology Platform. The Technology Platform must provide a method for:

a) Register and deregister critical components;

b) Activate and deactivate specific critical components;

c) Ensure that only registered and activated critical components can participate in gaming operations; and

d) Ensure that the default condition for critical components is unregistered and disabled.

24.2 Communication protocol

Each component of the Technology Platform must function as indicated by a documented secure communication protocol.

a) All protocols must use communication technology that contains mechanisms for error detection and proper recovery, which is designed to prevent intrusion, interference, interception and tampering. All alternative implementations are reviewed on a case-by-case basis.

b) All data communications critical to gaming or gaming account management employ encryption and authentication.

c) Communications on the secure network should only be possible between approved critical components that have been registered and authenticated as valid on the network. Unauthorized communication between components and/or access points should not be allowed.

d) Communications are strengthened to be immune to all possible attacks from incorrectly formatted messages.

e) After an interruption or shutdown of the Technology Platform, communication with all components necessary for platform operation is not established and authenticated until the program resumption routine, including self-checks, is successfully completed.

24.3 Communication over the Internet/public networks

Communication between all components of the Technology Platform, including remote player devices, which is conducted over the internet/public networks, must be secured by either encrypting the data packets or using a secure communications protocol to ensure the integrity and confidentiality of the transmission. Personally identifiable information, confidential information, bets, wagers, scores, financial information, and player transaction information must always be encrypted over the Internet/public network and protected against transmission.

incomplete, misdirection, unauthorized modification of messages, disclosure, duplication or reproduction.

24.4 Network security management

Networks must be logically separated so that there is no traffic on a network link that cannot be maintained by the link host. The following requirements apply:

a) All network management functions must authenticate all users on the network and encrypt all network management communications.
b) Failure of a single item should not result in a denial of service.
c) An intrusion detection system/intrusion prevention system (IDS/IPS) must be installed which includes one or more components that can receive internal and external communications, as well as detect or prevent:

i. Distributed Denial of Service (DDOS) attacks;
ii. Set of programmed commands (shellcode) traversing the network;
iii. Address Resolution Protocol (ARP) spoofing; and
iv. Other "Intermediary" attack indicators and cut off communication immediately if detected.

d) In addition to the requirements in (c), an IDS/IPS installed on the WLAN must have the capability to:

i. Scan the network for clandestine or unauthorized access points or connected devices at any network access point at least quarterly;
ii. Automatically deactivate any unauthorized or clandestine device connected to the Technology Platform; and
iii. Maintain a log of the history of all wireless access for at least the previous ninety days or as specified by MINCETUR. This log must contain complete information on all wireless devices at the site or premises and can be reconciled with all other network devices within the site or location.

e) The network communication equipment (NCE) must meet the following requirements:

i. The NCE must be constructed so that it is resistant to physical damage to the hardware or corruption of the firmware/software contained therein by normal use.
ii. The NCE must be physically secured against unauthorized access.
iii. Technology Platform communications via the NCE must be logically secure against unauthorized access.
iv. The NCE with limited storage should, if the audit log is full, either disable all communication or offload the logs to a dedicated log server.

f) All network entry and exit points are identified, managed, controlled and monitored 24 hours a day, 7 days a week. In addition:

i. All network cores, services and connection ports must be secure to prevent unauthorized network access; and
ii. Unused services and non-essential ports should be physically blocked or disabled by software if possible.

g) In cloud and virtualized environments, redundant servers should not run under the same hypervisor. Additionally:

i. Each server instance can perform only one function; and
ii. Equivalent alternative security mechanisms are considered as technology advances.

h) Stateless protocols, such as the User Datagram Protocol (UDP), should not be used for confidential information without stateful transport. Please note that, although the hypertext transport protocol (HTTP) is technically stateless, when executed in the stateful transmission control protocol (TCP), it is allowed.
i) All changes to the network infrastructure (network communication equipment configuration) must be recorded.
j) Virus scanners and/or detection programs should be installed on all platforms. These programs should be updated regularly to scan for new strains of viruses.
k) The Holder must monitor the Technology Platform and network to prevent, detect, mitigate and respond to cyber attacks.

24.5 Active and Passive Attacks

Appropriate measures must be in place to detect, prevent, mitigate and respond to common active and passive technical attacks. The Registrant must have a procedure in place to gather information on cyber threats and act appropriately.

24.6 Mobile Computing and Communications

A formal policy is established and appropriate security measures are in place to protect against the risks of using mobile computing and communication facilities. Telecommuting is not permitted, except in circumstances where endpoint security can be assured.

Section 25. Third Party Service Providers

25.1 Third party communication

When implementing communication with third party providers, as well as player loyalty programs, information security services, cloud services, live gaming services and identity verification services, the following requirements apply:

a) The Technology Platform must have the capability for secure communication with third party service providers using encryption and strong authentication.
b) All logging events involving third party services must be recorded in the audit file.
c) Communication with third party service providers must not interfere with or impair the normal functions of the Technology Platform.

i. Data from third party service providers should not affect the player's communication.
ii. Third-party service providers must be on a segmented network separate from the network segments hosting player connections.
iii. The game must be disabled on all network connections except for those within the production environment.
iv. The Technology Platform must not send data packets from third party service providers directly to the production environment and vice versa.
v. The Technology Platform should not act as an IP router between the production environment and third party service providers.

25.2 Third party services

The security roles and responsibilities of third party service providers must be defined and documented. The Registrant should establish policies and procedures to manage them and monitor their compliance with applicable security requirements.

a) Agreements with third party service providers that include access, processing, communication or management of the Technology Platform and/or its components, or add products or services on the platform and/or its components must cover all applicable security requirements.

b) Services, reports and records provided by third party service providers must be monitored and reviewed annually or as required by MINCETUR.

c) Changes in the provision of third party service providers, including maintaining and enhancing existing security policy, procedures and controls, should be managed considering the criticality of the platforms and processes included and the reassessment of risks.

d) Access rights of third party service providers on the platform and/or its components must be removed after termination of the contract or agreement or adjusted after a change.

25.3 Third Party Data Processing

Unauthorized third party service providers should be prevented from viewing or altering personal identity information and other confidential information. When personal identity information and other confidential information is shared with third party service providers, formal data processing agreements are established that set forth the rights and obligations of each party with respect to the protection of personal identity information and other confidential information. Each data processing agreement must state:

a) The purpose and duration of the processing;
b) The nature and purpose of the processing;
c) The type of data to be processed;
d) How data is stored;
e) The security detail surrounding the data;
f) The means used to transfer data from one organization to another;
g) The means used to retrieve data on certain individuals;
h) The method for ensuring a retention program is met;
i) The means used to delete the data; and
j) Data categories.

Section 26. Technical controls

26.1 Redirection of Technological Platforms

The Holder establishes the necessary procedures and mechanisms to ensure that all connections made are redirected to the Technology Platform specified in this document.

The Holder must redirect the entry made by the player of a Technological Platform not authorized in the country, to a Technological Platform that has such authorization, in cases where both Technological Platforms belong to the same holder. The redirection must be made to the website (domain with the extension) communicated to MINCETUR in accordance with Article 12 of this Regulation.

These mechanisms must be clearly identified, recorded and audited.

26.2 Domain Name System (DNS) requirements

The following requirements apply to servers used to resolve public or external Domain Name System (DNS) queries used in association with the Technology Platform.

a) The Registrant must use a secure primary DNS server and a secure secondary DNS server that are logically and physically separated from each other.

b) The primary DNS server must be physically located in a secure data center or a virtualized host on a properly secured hypervisor or equivalent.

c) Physical and logical access to the DNS server(s) must be restricted to authorized personnel.

d) Zone transfers to arbitrary hosts should not be allowed.

e) A method to prevent cache poisoning, as well as DNS security extensions (DNSSEC), is required.

f) Multi-factor authentication must be established.

g) The registration lock must be set, so that any request to change the server(s) must be verified manually.

26.3 Cryptographic controls

A policy on the use of cryptographic controls for the protection of information must be developed and implemented.

a) Personally identifiable information and other confidential information must be encrypted if it traverses a network with a lower level of trust. Encryption also applies to such personally identifiable information and other confidential information stored on portable devices (laptops, USB devices, etc.).

b) Data that does not require hiding but is authenticated must use some type of message authentication technology.

c) Authentication must use a security certificate from an approved organization, containing information about who it belongs to, by whom it was issued, valid dates, a serial number or other unique identification that can be used to verify the contents of the certificate.

d) The level of encryption used must be appropriate for the sensitivity of the data.

e) The use of encryption algorithms should be periodically reviewed to verify that the current encryption algorithms are secure.

f) The encryption method includes the use of different encryption keys so that encryption algorithms can be changed or replaced to correct weaknesses as soon as practical. Other methodologies are reviewed on a case-by-case basis.

g) Encryption keys must be kept on a secure and redundant storage medium after they have been encrypted by a different encryption method and/or using a different encryption key.

26.4 Encryption key management

The management of encryption keys must use specific processes established by the Registrant and/or MINCETUR, which must cover the following:

a) Obtain or generate encryption keys and store them;
b) Encryption key expiration management, if applicable;
c) Revoke encryption keys;
d) Secure change of the encryption key set; and
e) Recover encrypted data with a revoked or expired encryption key for a specified period after the encryption key becomes invalid.

26.5 Reinforcement of Critical Components

Configuration procedures for critical components must address all known security vulnerabilities and be consistent with industry-accepted best practices for hardening the Technology Platform. The adequacy and effectiveness of the steps taken to strengthen critical components are periodically evaluated and, if appropriate, changes are made to improve the strengthening. These configuration procedures should include the following:

a) All standard or default settings are removed from all components where a safety risk is present;
b) Only one main function per server is implemented to prevent functions requiring different levels of security from coexisting on the same server;
c) Additional security features are implemented for any required service, protocol or daemon that is deemed insecure;
d) Platform security settings will be configured to prevent misuse; and
e) All unnecessary functionality such as unnecessary scripts, drivers, features, subsystems, file systems and web servers are removed.

26.6 Record Generation and Storage

Procedures should be in place to centrally monitor and manage user activities, exceptions and information security events. Logs that record these elements are:

a) Generated in each critical component of the Technology Platform to monitor and rectify anomalies, failures and alerts;
b) Stored for an appropriate period to aid in future investigations and access control monitoring;
c) Protected against tampering and unauthorized access; and
d) Reviewed periodically using a documented process. A record of each review is maintained.

Section 27. Remote access and firewalls

27.1 Remote access security

Remote access is defined as any access from outside the Technology Platform or Technology Platform network including access from other networks on the same site or premises must:

a) Be performed via a secure method, such as a multi-factor authentication process;
b) Have the option to be deactivated;
c) Accept only remote connections allowed by the firewall application and the Technology Platform configuration;
d) Be limited to only those application functions necessary for users to perform their job functions:

i. No unauthorized remote user administration functionality (adding users, changing permissions, etc.) is allowed; and
ii. Unauthorized access to the Operating Platform or any database other than to obtain information using existing functions is prohibited.

27.2 Remote access procedures and providers

A procedure for strictly controlled remote access must be established. The supplier may access the Technology Platform and its associated components remotely for product and user support or update/upgrades, as long as they are permitted by the Contractor or MINCETUR. This remote access must use user accounts reserved for this purpose which are:

a) Continuously monitored by the Registrant;
b) Deactivated when not in use; and
c) Restricted by logical security controls to access only the application(s) and/or database(s) for product and user support or to provide updates/upgrades.

27.3 Remote access activity log

The remote access application must maintain an activity log that is automatically updated presenting all remote access information, including:

a) Identification of the user(s) who performed and/or authorized the remote access;
b) Remote IP addresses, port numbers, protocols, and where possible, MAC addresses;
c) Date and time the connection was made and the duration of the connection; and
d) Activity during the session, including specific areas accessed and changes made.

This activity log is reviewed periodically as required by the Proprietor and/or MINCETUR.

27.4 Firewalls

All communications, including remote access, must pass through at least one approved firewall at the application level. This includes connections to and from any non-platform host used by the Registrant.

a) The firewall must be located at the boundary between two different security domains;
b) A device in the same transmission domain as the Technology Platform host must not have a utility that allows an alternate route to the network to bypass the firewall;
c) Any alternate network paths that exist for the purpose of redundancy must also pass through at least one application-level firewall;
d) Only firewall-related applications can reside on the firewall;
e) Only a limited number of user accounts can be present in the firewall (network or platform administrators only);
f) The firewall must reject all connections except those that have been specifically approved;
g) The firewall must reject all connections from locations that should not reside on the network on which the platform originated (RFC1918 addresses on the public side of an Internet firewall); and
h) The firewall should only allow remote access using encryption that complies with current industry accepted standards such as ISO/IEC 19790, FIPS 140-2 or equivalent.

27.5 Firewall audit logs

Firewalls used to protect the production environment must be able to record audit information in a manner to preserve and secure the information against loss or alteration. This information includes the following:

a) All changes in the firewall configuration;
b) All successful and unsuccessful connection attempts through the firewall; and
c) Source and destination IP addresses, port numbers, protocols, and if possible, MAC addresses.

A configurable parameter "unsuccessful connection attempts" can be used to deny further connection requests when the default limit is exceeded. The Technology Platform administrator must also be notified.

Section 28. Change Management

The Registrant communicates to MINCETUR annually the change management policy for processing the update of the

Technology Platform and its components based on the predisposition for frequent platform upgrades and the selected risk tolerance. For platforms that require frequent upgrades, a risk-based change management program can be used to improve upgrade efficiency. Risk-based change management typically includes a categorization of proposed changes based on regulatory impact and defines the associated certification procedures for each category. The authorized Certification Laboratory evaluates the platform and future modifications in accordance with the change management policy communicated to MINCETUR.

28.1 Criteria for the evaluation of substantial and non-substantial change management

The Contractor must evaluate whether the change is "substantial" or not, taking into account the assessment criteria established in this Technical Standard, as well as the MINCETUR may establish in mandatory Directives.

a) The qualification of a change as "substantial" should be based on the evaluation of the following criteria, among others:

i. The impact that may be generated by the violation of a regulation in force;
ii. The principles of responsible gambling;
iii. The correct functioning of the games in operation;
iv. The authenticity and correct processing of bets;
v. Traceability of the operations performed;
vi. The correct operation of the Technological Platform;
vii. The security of the games and especially in the player's access;
viii. Data recoveries in the event of any occurrence in the Technological Platforms that require great complexity;
ix. The dependencies between the hardware, software and network elements that make up the Technology Platform and the coupling that may exist between its different components;

b) The Registrant, if justified, determines that the change is not substantial, may proceed to make the change, without the need for any communication to the authorized Certification Laboratory. Among the non-substantial changes are the following:

i. Installation or changes to backup software and/or hardware components;
ii. Addition or deletion of users;
iii. Database maintenance that modifies or removes non-critical data from the database;
iv. Scheduled outages or maintenance of any network service provider infrastructure;
v. Scheduled outages or maintenance of any electrical infrastructure (generator, ATS, UPS, etc.), PDU, etc.); or
vi. Installation of operating system security patches;
vii. Background images, color schemes, or similar ancillary updates from the front end to the client.

c) When the Registrant justifiably determines that the change is substantial, prior to deployment, the change to be made must be submitted to an authorized Certification Laboratory for technical evaluation. Among the changes that qualify as substantial, we have the following:

i. Changes in firewall rules;
ii. Database maintenance;
iii. Changes in the physical location of the primary regulated backup data, which implies a critical change that affects the operation of the Technology Platform;
iv. Any change or addition of a physical hardware component, which implies a critical change that affects the operation of the Technology Platform;
v. Changes in the non-gaming logic components of the Technology Platform that are not benign in nature.
vi. Implementation of a new game feature or a change in any logic that affects wagering or game logic;
vii. A change that affects required regulatory reporting or data used for financial reconciliation;
viii. a change affecting the handling or storage of personally identifiable information; or
ix. A change to incorporate updated regulatory requirements.

d) All changes made to the Technology Platform must be registered and may be subject to subsequent analysis and audit by MINCETUR. In the event that MINCETUR considers some of the changes made without its authorization to be substantial, it may require the withdrawal of the changes without prejudice to the initiation of the corresponding sanctioning process.

28.2 Change due to extraordinary emergency

The Contractor may make changes considered substantial provided that they qualify as an extraordinary emergency.

a) The Holder has up to two (2) days after the change to communicate such change in a reasoned manner to MINCETUR, through the available means. The report must accredit the exceptional circumstances of urgency and the risk, whether potential or not, involved for the security of the Technology Platform.
b) In the case of qualifying the change as substantial, the Holder has a term of ten (10) days to initiate the certification process of the change made.

28.3 Program change control procedure

The program change control procedure must be adequate to ensure that only authorized program versions are implemented in the production environment. These change controls should include:

a) An appropriate software version control or mechanism for all components, source code and binary controls;
b) Maintain records of all new installations and/or modifications to the Technology Platform, including:

i. The date of installation or modification;
ii. Details of the reason or nature of the installation or change, new software, server repair, significant configuration modifications;
iii. The component(s) to be changed, including the Critical Asset Register unique identification number, version information and, if the component being changed is hardware, the physical location of this component;
iv. The identity of the user(s) performing the installation or modification;
v. The identity of the user(s) responsible for authorizing the installation or modification; and
vi. Reasoned qualification of the change as substantial or non-substantial;

c) A strategy to cover the potential of a failed installation or field problem with one or more changes implemented under the change management process:

i. When an external party, such as an app store, is a stakeholder in the release process, this strategy covers the management of launches through the external part. This strategy can take into account the severity of the problem;

ii. Otherwise, this strategy should cover rollback to the last implementation (rollback or rollback plan), including full backup of previous software versions and a rehearsal of the rollback plan prior to implementation of the rollback environment;

d) A policy that includes procedures for emergency changes;

e) Procedures for testing and migration of changes, including identification of authorized personnel for signature prior to release;

f) Segregation of duties within the release process; and

g) Procedures to ensure that technical and user documentation is updated as a result of change.

28.4 Platform development life cycle

The acquisition and development of new software must use specific processes established by the Contractor, Platform Contractor and/or MINCETUR.

a) The production environment must be logically and physically separated from the development and test environments. When cloud platforms are used, there can be no direct connection between the production environment and any other environment.

b) The delegation of responsibilities between the Holder and/or the supplier is established when applicable.

c) A documented method for developing the software in a secure manner must be established:

i. Following industry standards and/or best practices for coding; and

ii. Incorporate information security throughout the entire life cycle.

d) The documented test methodology should include provisions for:

i. Verify that the test software is not deployed in the production environment; and

ii. Prevent the use of current and confidential personally identifiable information or other primary production data during testing.

e) All documentation related to the development of the application and software must be available and maintained for the duration of its life cycle.

28.5 Upgrade patches

The Licensee must have patch policies, either developed and supported by the Technology Platform Licensee or by an external service provider. All patches should be tested where possible in a development and testing environment configured identically to the target production environment, patch testing should be managed for risk, either by isolation or by removing the untested component from the network or by applying the patch and then testing it.

Section 29. Technical Safety Tests

29.1 Periodic Safety Testing

Technical security tests must be performed annually in the production environment to ensure that there are no vulnerabilities that jeopardize the security and operation of the Technology Platforms.

a) These tests must consist of a security assessment method by means of a third-party attack simulation using a recognized methodology, and the vulnerability analysis consists of the passive identification and quantification of the potential risks of the platform.

b) Unauthorized access attempts must be performed at the highest possible access level and must be completed with and without available authentication credentials (white box/black box tests). These allow evaluations of operating platforms and hardware configurations to be made, including, but not limited to:

i. UDP/TCP port scanning;

ii. Stack identification and TCP sequence prediction to identify operating platforms and services;

iii. Appropriation of public service announcement;

iv. Web scanning using HTTP and HTTPS vulnerability scanner; and

v. Router scanning using Border Gateway Protocol (BGP) routing protocol, Border Gateway Multicast Protocol (BGMP) routing multicast protocol and Simple Network Management Protocol (SNMP).

29.2 Vulnerability assessment

The purpose of the vulnerability assessment is to identify vulnerabilities, which can be exploited later during penetration testing by making basic queries regarding the services running on the platforms in question. The vulnerability assessment should include at least the following activities:

a) External vulnerability assessment - The target are network devices and servers that are accessible by third parties (either an individual and a company), by means of a public IP address (publicly exposed), related to the Technology Platform from which it is possible to access personal identity information and other confidential information.

b) Internal vulnerability assessment - The target is the inbound servers (in the DMZ, or in the LAN if there is no DMZ) related to the Technology Platform from which it is possible to access personal identity information and other confidential information. Testing of each security domain in the internal network must be performed separately.

29.3 Penetration testing

The purpose of the penetration testing is to take advantage of any vulnerabilities discovered during the vulnerability assessment in any publicly exposed application or application host platform that processes, transmits and/or stores personal identity information and other sensitive information. Penetration testing includes the following activities at a minimum:

a) Network Layer Penetration Testing - This test mimics the actions of an actual attacker taking advantage of weaknesses in network security and examines platforms for any deficiencies that can be used by an external attacker to disrupt the confidentiality, availability and/or integrity of the network.

b) Application Level Penetration Testing - This test uses utilities to identify deficiencies in applications with authenticated and unauthenticated scans, analysis of the results to remove false positives, and manual testing to confirm the results of the utilities and to identify the impact of deficiencies.

29.4 Review of firewall rules

Firewall rules are periodically reviewed to verify the operational condition of the firewall and the effectiveness of its security configuration and rule sets, and are performed on all perimeter firewalls and internal firewalls.

29.5 Quarterly Vulnerability Scans

Internal and external network vulnerability scans are run at least quarterly and after any significant changes to the Registrant or network infrastructure.

a) Testing procedures should verify that four internal and quarterly scans were performed within the last twelve (12) months and that further scans were performed until all "medium risk" vulnerabilities (CVSS 4.0 or higher) were resolved and/or accepted through a formal risk acceptance program. Internal scans must be performed from an authenticated scanning perspective. External scans may be performed from a non-authenticated perspective.

b) Quarterly scans may be performed by the authorized Certification Laboratory or through a qualified employee of the Registrant.

c) Verification of the scans must be submitted to MINCETUR on a quarterly basis and must include a remediation plan and any risk mitigation plans for those vulnerabilities that cannot be resolved.

SECTION C

Section 30. Audit for Service Providers

This section establishes procedures and practices for the evaluation of particular service providers, which are reviewed in an operational audit as part of the evaluation of the Technology Platform, which includes, among others, the evaluation of information security services, cloud services, service payments (financial institutions, payment processors, etc.), live gaming services and any other services that may be offered directly by the Registrant or that involve the use of external service providers.

Section 31. Information Security Services

31.1 Information Security Management System (ISMS) platform audits

The Registrant or a third party information security service provider used to provide management, support, security or disaster recovery services for the Platform undergoes an audit of the Platform. The Information Security Management Platform (hereinafter ISMS) is reviewed against common information security principles regarding confidentiality, integrity and availability, as covered in this section. It is permitted to leverage the results of previous audits performed by appropriately accredited vendors and qualified persons, within the current audit period (e.g., within the last year), against standards such as ISO/IEC 27001, the NIST Cybersecurity Framework (CSF), or equivalent.

31.2 Information Security Policy

An information security policy is applied to describe the ISMS approach to managing information security and its implementation. The information security policy should:

a) Have a provision that requires review at planned intervals and when changes occur in the Technology Platform or in the Registrant's processes that alter the risk profile of the platform;

b) Be approved by management and communicated to all employees of the Registrant and relevant employees of external service providers; and

c) Delineate the security roles and responsibilities of the Registrant's employees and employees of external service providers relevant to the operation, service and maintenance of the Technology Platform and/or its components;

31.3 Access Control Policy

An access control policy is established and documented within the ISMS and periodically reviewed based on business and security requirements for physical and logical access to the Technology Platform and/or its components.

a) A formal registration and cancellation procedure is established to grant and revoke access to the Technology Platform and/or its components.

b) The assignment of access privileges is restricted and controlled based on business requirements and the principle of least privilege.

c) Employees only have access to services or facilities that they have been specifically authorized to use.

d) Employees receive appropriate security awareness training and periodic updates on organizational policies and procedures as necessary for their job function.

e) Management reviews user access rights at regular intervals using a formal process.

f) Employees' access rights to the Technology Platform and/or its components are removed upon termination of their employment, contract or agreement, or are adjusted upon change.

31.4 Assignment of Security Responsibility

Security responsibilities should be documented and effectively implemented within the ISMS.

a) A security forum composed of management is formally established to monitor and review the ISMS to ensure its continued suitability, adequacy and effectiveness, maintain formal minutes of meetings, and convene periodically as required by MINCETUR.

b) The Holder shall be responsible for developing and implementing security strategies and action plans, and shall:

i. Review all processes related to security aspects, including, but not limited to, protection of information, communications, physical infrastructure and gaming processes;

ii. Reporting to the general management and to the IT;

iii. Have the competencies and be sufficiently trained and have access to all necessary resources to enable proper assessment, management and risk reduction.

c) The Registrant is responsible for recommending security policies and changes.

31.5 Information Security Management System (ISMS) Occurrence Management

A process for reporting information security occurrences and management response is documented and implemented within the ISMS in accordance with the information security policy. The occurrence management process shall:

a) Include a definition of what constitutes an information security occurrence;

b) Document how information security occurrences are reported through the appropriate management channels;

c) Addressing management responsibilities and procedures to ensure a rapid, effective and efficient response information security occurrences, including:

i. Procedures for handling different types of information security occurrences;
ii. Procedures for the analysis and identification of the cause of the occurrence;
iii. Communication with those affected by the occurrence;
iv. Report the occurrence to the appropriate authority;
v. Collection of forensic evidence; and
vi. Controlled recovery of information security occurrences.

Section 32. Cloud Services

32.1 Cloud Service Provider Audits

A Registrant using a cloud service provider to store, transmit or process personally identifiable information and other sensitive information is subject to a specific audit as required by MINCETUR. The operations of the cloud service provider are reviewed against common information security principles in connection with the provision and use of cloud services, as covered in this section. It is acceptable to leverage the results of previous audits conducted by appropriately accredited vendors and qualified persons, within the current audit period (e.g., within the last year), against standards such as ISO/IEC 27017 and ISO/IEC 27018 or equivalent. Such recourse is noted in the audit report.

32.2 Cloud Service Provider Relationship

The security in the cloud is a shared responsibility between the cloud service provider and the Holder, being the only responsible before MINCETUR the Holder.

a) If Personally Identifiable Information and other Sensitive Information is stored, processed or transmitted in a cloud environment, the applicable requirements apply to that environment and generally involve validation of the cloud service provider's infrastructure and the Registrant's use of that environment.
b) The allocation of responsibility between the cloud service provider and the Registrant for administering security controls does not relieve a Registrant of the responsibility to ensure that Personally Identifiable Information and other confidential information is adequately protected in accordance with applicable requirements.
c) Clear policies and procedures are agreed between the cloud service provider and the Registrant for all security requirements, and responsibilities for operation, administration and reporting are clearly defined and understood for each applicable requirement.

Section 33. Payment Services

33.1 Payment Service Provider Audit

The Registrant or an external payment service provider used to conduct transactions with financial institutions is subject to a specific audit. The operations of the payment service provider are reviewed against common information security principles in relation to the provision and use of payment services, as covered in this section. It is acceptable to leverage the results of previous audits conducted by appropriately accredited providers and qualified persons, within the current audit period (within the last year), against the payment card industry data security standards (PCI-DSS) or equivalent. Such a resource is noted in the audit report.

33.2 Payment Guarantee

The Payment Service Provider protects the payment types used on the Technology Platform against fraudulent use.

a) The collection of personally identifiable information and other confidential information directly related to financial transactions is limited only to the information strictly necessary for the transaction.
b) Processes should be in place to verify the payment service provider's protection of personally identifiable information or other confidential information directly related to each financial transaction.
c) Any communication channel between the Holder and the payment service provider transmitting payment details must be encrypted and protected against interception.
d) All financial transactions are reconciled daily between the Cardholder and the payment service provider. There will be procedures in place for:

i. Calculate the amounts paid to or received from a player, taking into account all payments used by the player and Holder; and
ii. If possible and if the means of payment allows it, the identity match between the owner of the means of payment and the holder of the gaming account must be ensured.

Section 34. Live Gaming Services

34.1 Auditing of Live Gaming Service Providers

The live gaming service provider is required to comply with applicable aspects of the appropriate policy documents and/or procedures as determined by the Registrant, including the controls within this section.

a) The live gaming environment used to conduct live or similar games must be in a secure location. The Registrant, at MINCETUR's request, must provide remote access(s) to the live gaming environment and its transmissions.
b) The live gaming environment must undergo a live gaming environment audit by an authorized Certification Laboratory within ninety (90) days after the start of operations in Peru, and as required by MINCETUR.

34.2 Live Gaming Environment Security

The live gaming environment is defined and has appropriate physical security controls. Secure areas, gaming media, tables and gaming equipment must be protected by appropriate entry controls and security procedures to ensure that only authorized staff members have access in accordance with the following guidelines:

a) In the event that live gaming occurs in a MINCETUR authorized casino gaming room, where the gaming area is open to the public, the live gaming environment is controlled by the same rules and controls as the authorized casino gaming room, including, but not necessarily restricted to:

i. To have perimeter security platforms in those areas where live games take place; and
ii. Having access controls to such areas, to ensure that only authorized staff members have access, and controls in all areas near live gaming equipment, to ensure that live gaming is conducted in the correct manner.

b) In the event that live games occur in a casino gaming room authorized by MINCETUR, during public opening hours, but the gaming area is not open to the public, please note that:

i. The areas where live gaming occurs and all areas near live gaming equipment and related access must be at least protected by boundary barriers and alerted and supervised by security personnel; and

ii. Live game equipment is subject to access controls.

c) In the event that live gaming occurs in a private gaming studio or licensed casino gaming floor area during public closing hours or in a licensed casino gaming floor area that is not open to the public and is not supervised by security personnel:

i. The areas where live gaming occurs and the entire area near the live gaming equipment and related accesses must be protected by physical barriers and related accesses protected through perimeter access security platforms; and

ii. Access points, such as delivery and loading areas and other points where unauthorized persons may enter the areas where live games occur, should be controlled and, if possible, isolated from operational areas to prevent unauthorized access.

34.3 Surveillance and Recording

The live gaming service provider is required to install, maintain and operate a surveillance platform that has the capability to monitor and record continuous unobstructed views of all live game play.

a) A continuous recording of all games played is made so that:

i. The information necessary to properly reconstruct each game, in accordance with the applicable withdrawal requirements set forth in the section entitled "Last Game Information Required" that are not displayed on the Technology Platform, is identifiable and distinguishable;

ii. The date and time of each game can be determined with an accuracy of one second in relation to the clock used by the platform; and

iii. The sequence of games can be determined between

ye
s.

b) Procedures are established to ensure that the recording:

i. Covers the defined live game environment in sufficient detail to confirm whether game rules and procedures were followed and to identify discrepancies;

ii. It is captured in such a way as to prevent interference or elimination;

iii. May be reviewed by the Registrant and/or MINCETUR in case of a complaint/dispute from the player; and

iv. It is maintained for at least ninety (90) days or as required by MINCETUR.

v. At MINCETUR's request, the Contractor must provide remote access to the surveillance system and security cameras.

34.4 Simulcast Control Servers

The live gaming service provider uses simulcast monitoring servers to record all game activity and results. The live gaming service provider may use its own surveillance camera and split the stream into The simulcast control server may be live to the simulcast control server, or there may be a separate video network involved. The simulcast control servers should:

a) Provide the player with real-time audio/visual access to the live game being played, including:

i. Any information found in the "Game Information and Rules of the Game" and "Information to be displayed" sections of the Technical Standards I and II that is not displayed by the Technology Platform and there must be a mechanism to provide such information;

ii. The actions of the game assistant and, when applicable, of other players;

iii. Date and time at the game site; and

iv. Game identification/table number and location.

b) Provide each player with the equivalent of a quality video/audio stream.

i. This equivalence is measured and verified whenever communications are initiated, including reconnection due to signal interruptions or restart when the signal is cut off.

ii. A minimum signal connection requirement is established, required and disclosed to the player.

c) Prevent anyone from accessing the outcome of the live game before finalizing a wager.

d) Record game results prior to posting on the Technology Platform. Be equipped with a mechanism for an authorized employee to override game results, if necessary.

34.5 Live gaming equipment

The live gaming service provider must provide a secure location for the location, operation and use of live gaming equipment, including simulcast control servers, game servers and communications equipment. Security policies and procedures must be in place and periodically reviewed to ensure that risks are identified, mitigated and underwritten by contingency plans. It must also comply with the following requirements:

a) Live gaming equipment is installed according to a defined plan and records of all live gaming equipment installed are maintained.

b) Live gaming equipment should be located or protected to reduce the risks of:

i. Environmental threats and hazards;

ii. Opportunities for unauthorized access;

iii. Power failures; and

iv. Other outages caused by support utility failures.

c) Access to the live gaming equipment by the gaming attendant is controlled by a login procedure or other secure process to ensure that only authorized gaming attendants are allowed access. It is not possible to modify live gaming equipment configuration settings without an authorized secure process.

d) The gaming wizard initiates a user session, where it supports live gaming equipment, by logging into your user account using your secure username and password or an alternate means for the gaming wizard to provide identifying information.

i. All available options presented to the game wizard are linked to your user account.

ii. If the live gaming team does not receive information from the gaming attendant within five minutes, the session will

The user is disconnected or locked out, requiring the game wizard to reset their login to continue.

e) To ensure its continued availability and integrity, equipment designated for live gaming must be properly maintained, inspected and repaired at regular intervals by designated personnel to ensure that it is free of defects or mechanisms that could interfere with its operation.

f) Before disposal or reuse, live gaming equipment containing storage media should be checked to ensure that any licensed software and other confidential information has been securely removed or overwritten (i.e., not just deleted).

34.6 Live Gaming Consumer Goods

Consumer goods (gaming media, such as cards, dice, etc.) used by live gaming services must comply with the minimum standards determined by MINCETUR, as well as with the following requirements:

a) Procedures are implemented to track the inventory of consumables from receipt, through storage, installation, use, removal and destruction. All consumables should have an associated audit trail showing which designated personnel had access to the consumables at any time for any operation;

b) Periodic random inspections of consumer goods in use are carried out from disbursement to retirement; and

c) Used consumer goods are destroyed in a manner that prevents their accidental reuse in live games and puts them permanently out of use.

34.7 Player Physicals

The following controls apply to physical player chips used in live games. For example, in a live poker game involving both in-person players and players playing through a Technology Platform, physical player chips may be placed on the table to indicate the player's wager to the other players.

a) All cards must have identical physical characteristics, except for specific differences in the denomination.

b) Chips of all possible denominations (according to the denomination of the game) are shown so that the lack of chips of smaller denominations does not force players to bet more.

c) Each chip is designed so that the specific denomination of each chip can be determined when placed in a stack of chips of various denominations.

d) The tokens used are unique for each denomination they represent, and the denomination must be clearly visible on any token.

34.8 Live Game Procedures

The following procedures apply to live gaming service providers. These procedures are reviewed periodically to ensure that risks are identified, mitigated and underwritten by contingency plans.

a) Procedures should be in place to allow for an adequate response to any security issues within live gaming services.

b) Procedures must be in place to prevent any person from tampering with or interfering with the operation of any live gaming or live gaming equipment.

c) Separate procedures should be in place for each The game and new games must have their procedures defined before being offered to players.

d) The following procedures apply for live gaming service provider personnel, including gaming attendants:

i. Procedures should be in place to conduct periodic background checks of personnel;

ii. Staff should receive adequate training to provide live game play fairly in accordance with documented procedures and game rules. Evidence of training and periodic refresher training is maintained;

iii. Staff must be trained and are regularly reminded of any physical behavior that is prohibited or mandatory (including hand signals, talking, card handling, etc.);

iv. Policies and procedures related to rotations, shift patterns and assignment should be documented, including how attendants are assigned to tables/games (without prior knowledge of the tables/games they serve and with their time in the game set at a level to discourage harmful relationships from developing) and changes in game attendants during exceptional circumstances;

v. A method to reasonably detect players who reject tables/games and consistently re-request another within the same game type until they reach their preferred table/game;

vi. Documentation retention should be strong, allowing personnel records to be audited and investigations to be conducted where staff members are directly involved or where their presence at a particular place and/or time is crucial to understanding a chain of events;

vii. Procedures for hiring and termination of personnel are documented;

viii. A supervisory employee is always present when live games are being played;

ix. Personnel records are maintained for each table/game;

e) Procedures are established to inform in-person players that they are being filmed as part of a live broadcast;

f) Procedures related to anomalous events that may occur during live games must be documented and understood by personnel, including, but not limited to, the following:

i. Malfunction of the specialized device or physical randomization device, including incorrect detection of results;

ii. Letters dropped;

iii. Wrong distribution;

iv. Re-turns;

v. Suspended games; and

vi. Table/game closure.

g) There should be consistent procedures for shuffling cards, including verification of card count, frequency of shuffling, and instances of reshuffling. The deck of cards is recorded.

h) There must be a defined procedure for the accounting of the player's physical chips.

i) Procedures are established to demonstrate that a single staff member cannot perform all tasks related to game management and that there is a segregation of responsibilities before the game, during the game and after the game.

j) Procedures should be in place to deal with player disconnection or any interruption of video, voice or data transmission during a live game.

k) Procedures are established to guarantee bets placed in live games:

i. When bets are placed by verbal instruction, the content of the bet is communicated and confirmed by the player before the bet is confirmed;

ii. When a gaming assistant receives wagers indicated by the player, a clear indication or notification is provided if the wager has been accepted or rejected (in whole or in part; and

iii. The winning player is notified of the prize won, including the prizes awarded, after the completion of the game and his account balance is updated immediately or once he exits the game.

l) Variations in the operation of card shufflers and dealers, roulette wheels, spinners, dice shakers or other live gaming equipment are incorporated into the game procedures to maintain randomness. This equipment has a level of randomness consistent with that seen in gaming venues to ensure fairness and integrity.

m) Procedures should be in place to ensure that card dealers and similar specialized devices and physical randomization devices are tamper-proof once loaded to prevent interference before and during play.

n) In order to ensure and maintain their integrity, all specialized devices and physical randomness are periodically inspected and tested for reliability. In addition:

i. All consumer goods or live gaming equipment that are subjected to this hardware are checked for defects prior to processing to avoid disruption of play; and

ii. Records should be kept of all tests.

o) There will be procedures in place to inform the player when the manual operation mode of the specialized device is activated, and tracking is enabled to allow for additional review;

p) Policies and procedures are established to identify and replace specialized devices and physical randomization devices that exhibit an unacceptable level of errors; and

q) Procedures should be in place to maintain game records and classify game events into statistics that can be analyzed for trends related to game performance, personnel and/or locations in the live game environment, including supervisors, shifts, procedural violations, as well as other occurrences, irregularities and errors.

TECHNICAL STANDARDS IV

ECONOMIC AND TECHNICAL DATA TO BE TRANSMITTED BY THE TECHNOLOGICAL PLATFORMS TO THE MINCETUR'S DATA CENTER

COMMUNICATION PROTOCOL.

The communication protocol between the Technology Platform and the MINCETUR Data Center is SFTP (Secure File Transfer Protocol) or other secure protocol.

MINCETUR provides the Holder with the credentials in order to establish a secure access for the delivery of one plain text file per day, containing all the information.

The structure of the file names is as follows:

REPX	REGDGJCMT	FEC	VXX	.TXT

WHERE:

1. REPX: Economic or technical data report X = E:
   Economic data;
   X = T: Technical data;
2. REGDGJCMT: Registration code granted by MINCETUR to the Holder.
3. FEC: Date in YYYYYMMDD format.
4. VXX: Version of the file. Each version must contain all the information.
   XX: must be replaced by the updates that can be submitted, as indicated in the following example
   - V01.- Original file;
   - V02.- Corrected file.
5. .TXT: File extension.

a) Structure of the consolidated economic data to be transmitted:

GENERAL STRUCTURE OF ECONOMIC DATA:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	...	30	31	32	...	106	107	108	...	120	121	122	...	106	...	276
1	1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	D	D	...	S	1	2	...	19	D	D	...	S	1	2	...	19	...	1
C A B E	T I P O	REGDGJCMT														Fecha_Inicio				Datos económicos				Fecha_Fin				Datos económicos				FLG3	FLG4
CABECERA																DATOS																	

Longitud en caracteres: 276

HEADER

Content	Abbreviation	Character length	Example	Observation
It is worth mentioning	C	1	E	Where: E = Economic data
Type	T	1	1	Where: 1 = Overall consolidated total of the Technology Platform 2 = Total consolidation of the Technology Platform with respect to transactions carried out directly on the Technology Platform by means of gaming media (PC, cell phones, Tablet, etc.). 3 = Consolidated total of the operations carried out by each sports betting room.
Code registry code granted by MINCETUR	REGDGJCMT	14	21000000100001	Registration code granted by MINCETUR to the Registrant

DATA

Content	Abbreviation	Character length	Example	Observation
Date	FECI	14	20220824000000	With format YYYYMMDDHH24MISS Example: Start date of operations on August 24, 2022 corresponds to 00:00:00 hours.
Bets	API	19	0000000092327621.24	It is mandatory to fill with zeros to the left of the whole number to comply with the length of 19 characters. Likewise, it is mandatory to place the decimal point and two characters for decimals, in case of not having decimals, you must complete with zeros until you reach two decimals.
Returns	DEI	19	0000000002327121.18	It is mandatory to fill with zeros to the left of the whole number to comply with the length of 19 characters. Likewise, it is mandatory to place the decimal point and two characters for decimals, in case of not having decimals, you must complete with zeros until you reach two decimals.
Awards	PGI	19	0000000032317621.22	It is mandatory to fill with zeros to the left of the whole number to comply with the length of 19 characters. Also, it is mandatory to place the decimal point and two characters for decimals, in case of not having decimals, you must complete with zeros until you reach two decimals.
Bonus	BNI	19	0000000002327121.26	It is mandatory to fill with zeros to the left of the whole number to comply with the length of 19 characters. Also, it is mandatory to place the decimal point and two characters for decimals, in case of not having decimals, you must complete with zeros until you reach two decimals.
Date	FECF	14	20220825235959	With format YYYYMMDDHH24MISS Example: End of operations date of August 24, 2022 corresponds to 23:59:59 hours.
Bets	APF	19	0000009992327621.24	It is mandatory to fill with zeros to the left of the whole number to comply with the length of 19 characters. Likewise, it is mandatory to place the decimal point and two characters for decimals, in case of not having decimals, you must complete with zeros until you reach two decimals.
Returns	DEF	19	0000000000027121.03	It is mandatory to fill with zeros to the left of the whole number to comply with the length of 19 characters. Likewise, it is mandatory to place the decimal point and two characters for decimals, in case of not having decimals, you must complete with zeros until you reach two decimals.

Content	Abbreviation	Character length	Example	Observation
Awards	PGF	19	0000009932317621.22	It is mandatory to fill with zeros to the left of the whole number to comply with the length of 19 characters. Likewise, it is mandatory to place the decimal point and two characters for decimals, in case of not having decimals, you must complete with zeros until you reach two decimals.
Bonus	BNF	19	0000000992327121.26	It is mandatory to fill with zeros to the left of the whole number to comply with the length of 19 characters. Likewise, it is mandatory to place the decimal point and two characters for decimals, in case of not having decimals, you must complete with zeros until you reach two decimals.
Reservation1	RSV1	19	0000000000000000.00	
Booking2	RSV2	19	0000000000000000.00	
Reserve3	RSV3	19	0000000000000000.00	
Reserve4	RSV4	19	0000000000000000.00	
FLG1	FLG1	1	0	
FLG2	FLG2	1	0	
FLG3	FLG3	1	0	
FLG4	FLG4	1	0	

Where:

a) Cabe = E (Economic data)
b) Type:

1 = Total overall consolidation of the Technology Platform.
2 = Total consolidation of the Technology Platform with respect to transactions carried out directly on the Technology Platform by means of gaming media (PC, cell phones, Tablet, etc.).
3 = total consolidation of the operations carried out by each sports betting room;

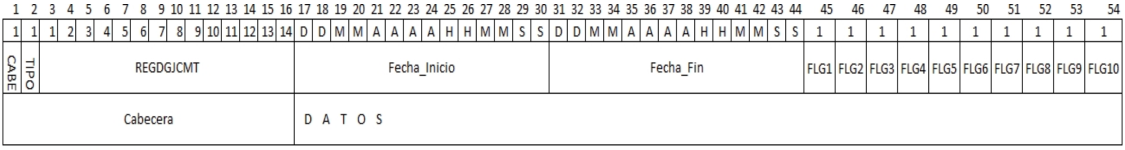
c) REGDGJCMT: Registration code granted by MINCETUR to the holder of a Technology Platform;
d) FECI: Date and time of start of operations for the day, in the format YYYYYMMDDHH24MISS.
e) API: Consolidated start of operations of the day, related to the Bets made by the players.
f) DEI: Consolidated start of operations of the day, with respect to returns.
g) PGI: Consolidated start of operations for the day, related to player awards.
h) BNI: Consolidated start of operations of the day, related to bonuses delivered.
i) FECF: Date and time of end of operations for the day, in the format YYYYYMMDDHH24MISS.
j) APF: Consolidated end of day operations, related to the Bets made by the players.
k) DEF: Consolidated end of day operations, with respect to returns.
l) PGF: Consolidated end of day operations, related to players' awards.
m) BNF: Consolidated end of day operations, related to bonuses paid.
n) RSV1, 2, 3 and 4: The DGJCMT issues the standard for implementation.
o) FLG1, 2, 3 and 4: The DGJCMT issues the standard for implementation.

Note:
The information must be sent in plain text. Pipelines (|) must be used to delimit the fields of each record. To separate the integer from the decimal number, the dot (.) is used. Likewise, line breaks (enter) are used to separate records. Thousand, million and space separators are not considered.

MINCETUR for reasons of changes or improvements in technology may modify the structure or communication protocol by means of mandatory rules.

b) Structure of the consolidated technical data to be

transmitted: GENERAL STRUCTURE OF TECHNICAL DATA:



1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54
1	1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	D	D	M	M	A	A	A	A	H	H	M	M	S	S	D	D	M	M	A	A	A	A	H	H	M	M	S	S	1	1	1	1	1	1	1	1	1	1
CABE	TIPO	REGDGJCMT														Fecha_Inicio														Fecha_Fin														FLG1	FLG2	FLG3	FLG4	FLG5	FLG6	FLG7	FLG8	FLG9	FLG10
Cabecera																D A T O S																																					

Longitud en caracteres: 54

HEADER

Content	Abbreviation	Character length	Example	Observation
It is worth mentioning	C	1	T	Where: T = Technical data
Type	T	1	1	Where: 1 = Technological Platform presents critical failures that temporarily stop its operation. 2 = Loss of communication between the Technological Platform and the remote sports betting gaming room.
Registration code granted by MINCETUR	REGDGJCMT	14	21000000100001	Registration code granted by MINCETUR to the Registrant

DATA

Content	Abbreviation	Character length	Example	Observation
START DATE	FEC_START	14	20230124000010	With format YYYYMMDDHH24MISS Example: Technological Platform presents critical failures on January 24, 2023 at 00:00:10 hours.
DATE END	FEC_FIN	14	20230124000110	With format YYYYMMDDHH24MISS Example: Technology Platform recovers from critical failures on January 24, 2023 at 00:01:10 hours.
FLG1	FLG1	1	0	
FLG2	FLG2	1	0	
FLG3	FLG3	1	0	
FLG4	FLG4	1	0	
FLG5	FLG5	1	0	
FLG6	FLG6	1	0	
FLG7	FLG7	1	0	
FLG8	FLG8	1	0	
FLG9	FLG9	1	0	
FLG10	FLG10	1	0	

Where:

a) CABE =T (Technical Data)
b) Type:

1 = The Technological Platform presents critical failures that temporarily stop its operation.
2 = Loss of communication between the Technological Platform and the remote sports betting gaming room.

c) REGDGJCMT: Registration code granted by MINCETUR to the Holder;
d) FEC_START: Date and time of start of the event in format YYYYYMMDDHH24MISS.
e) FEC_FIN: Date and time of the end of the event in YYYYYMMDDHH24MISS format.
f) FLG1, 2, 3, 4, 4, 5, 6, 7, 8, 9, 10: MINCETUR issues regulations for its implementation.

Note:

The information must be sent in plain text. Pipelines (|) must be used to delimit the fields of each record. To separate the integer from the decimal number, the dot (.) is used. Likewise, line breaks (enter) are used to separate records. Thousand, million and space separators are not considered.

MINCETUR for reasons of changes or improvements in technology may modify the structure or communication protocol by means of mandatory rules.

2224342-1