RESOLUTION OF 6 OCTOBER 2014, FROM THE DIRECTORATE GENERAL FOR THE REGULATION OF GAMBLING, APPROVING THE REGULATION WHICH ELABORATES ON THE TECHNICAL SPECIFICATIONS FOR GAMBLING, TRACEABILITY AND SECURITY THAT MUST BE MET BY THE NON-RESERVED TECHNICAL GAMBLING SYSTEMS LICENSED UNDER THE GAMBLING ACT 13/2011 OF 27 MAY.

The Gambling Act 13/2011 of 27 May establishes the national and legislative framework for gambling activities in its different forms for the purposes of ensuring the protection of public order, combating fraud, preventing addictive behaviour, protecting the rights of minors and safeguarding the rights of gambling participants.

The technical requirements of the Gambling Act 13/2011 were implemented by Royal Decree 1613/2011 of 14 November, which, when interpreted in accordance with the Tenth additional provision of the Establishment of the National Markets and Competition Commission Act 3/2013 of 4 June, assigns, in its First final provision, the elaboration of particular technical features for the marketing of gambling activities covered by the Gambling Act to the Directorate General for the Regulation of Gambling.

The technical specifications that must be met by the technical gambling systems licensed under the Gambling Act 13/2011 of 27 May were developed by the Directorate General for the Regulation of Gambling in its Resolution of 16 November 2011.

On the basis of accumulated experience after more than one year since the opening up of the market, it now proves necessary to revise the Resolution of 16 November in its form and content.

By virtue thereof, and following the favourable report from the Office for Legal Counsel to the State Secretariat for Finance under the aegis of the Ministry of Finance and Public Administrations, it is hereby agreed:

One.

To approve the Regulation elaborating on the technical specification that must be met by technical gambling systems licensed in Spain and their control mechanisms, which is contained Appendix I of this Resolution.

The technical specifications stipulated in said regulation shall not apply to gambling activities conducted through text messages, landline or mobile telephone services or audiovisual communication methods where such specifications are incompatible with the type and features of the channel for participating in the gambling activity.

Two.

This Resolution shall enter into force on the day following its publication in the Official State Gazette of Spain.

Three.

Technical systems licensed prior to the publication date of this Resolution must be adapted to comply with said Resolution within a period of six months following its entry into force.

A one-year transitional period is established, from the date of publication of this Resolution, for compliance with the technical requirements concerning the format and length of passwords as established under section "2.1.12 User authentication and password policy". If, during the period between six months and one year subsequent to the publication of this Resolution, the user has to

renew his password due to its loss or expiration, the new password must adhere to the requirements established herein.

Four.

To repeal the regulation elaborating on the technical specifications that must be met by technical gambling systems, approved by the Directorate General for the Regulation of Gambling through its Resolution of 16 November 2011, and replace it with the present Regulation.

Madrid, 6 October 2014.– Director-General for the Regulation of Gambling, Carlos Hernández Rivera.

APPENDIX I

Regulation elaborating on the technical specifications for gambling, traceability and security that must be met by the non-reserved technical gambling systems licensed under the Gambling Act 13/2011 of 27 May.

Contents

3.14 Move repetition.
3.15 Virtual players.
3.16 Metamorphosis games.
3.17 Absent participant.
3.18 Hosted multiplayer games.
3.19 Live-broadcast games.
3.20 Jackpots, progressive jackpots and additional prizes
3.21 Gambling through pre-recorded communication channels.

4. Security of Information Systems.
4.1 Critical components.
4.2 Security management of the technical gambling system.
4.3 Risk management.
4.4 Security Policy.
4.5 Organisation of the Information Security.
4.6 Security of communications with participants.
4.7 Staff and third-party security.
4.8 Physical and environmental security.
4.9 Management of Communications and Operations.
4.10 Access Control.
4.11 System purchase, development and maintenance.
4.12 Management of security incidents.
4.13 Change management.
4.14 Management of service availability.
4.15 Plan for preventing information loss
4.16 Business continuity management.
4.17 Penetration testing and vulnerability analysis.

5. Internal Control System and inspection.
5.1 Internal Control System.
5.2 On-site and telematic inspection.

1. *General provisions*

1.1 Purpose.

The purpose of this Regulation is to elaborate on the technical specifications that must be met by the non-reserved technical gambling systems of those operators licensed under the Gambling Act 13/2011 of 27 May and the control mechanisms of said systems.

The technical infrastructure of the operators shall ensure the supervision by the Directorate General for the Regulation of Gambling of the performed gambling operations, the gathering of records created during their realisation, as well as the creation of any other information that may be considered relevant and making it available to the Directorate General for the Regulation of Gambling.

Therefore, this Regulation establishes the specifications for storing records of gambling operations and their traceability in accordance with the procedure and format established by the Directorate General for the Regulation of Gambling. It also describes the physical and logical security requirements of the information systems employed for gambling, as well as the security requirements for the organisation and management of such systems.

1.2 Definitions.

For the purposes of this Regulation, the following terms shall have the meaning as defined in this section.

1. Technical Gambling Systems: A technical gambling system means the set of equipment, systems, terminals, devices and software materials, as well as the procedures necessary for managing its proper operation, used by the operator for organising, operating and carrying out the gambling activity. The technical gambling system supports all necessary procedures for the

organisation, operation and realisation of the gambling activity, along with the detection and recording of the relevant transactions between the participants and operator.

The fundamental elements of the technical gambling system are the Central Gambling Unit and the internal control system. The technical gambling system must provide the information required for its supervision in the Spanish language. If it is not available in Spanish, the Directorate General for the Regulation of Gambling may require its translation either on a continuous or occasional basis.

2. Central Gambling Unit: The Central Gambling Unit is the set of technical elements that are necessary for processing and managing the operations performed by gambling participants. The Central Gambling Unit is composed of the Gambling Platform and the Game Software.

3. Gambling Platform: The gambling platform is the hardware and software infrastructure that comprises the main interface between the participant and the gambling operator and that provides the participant with the necessary tools for opening and closing his account, editing and saving his profile information, making gambling-account deposits and withdrawals and viewing details, or a summary, of movements on said account.

The gambling platform includes any website showing relevant information to the participant on the gambling offered by the operator, as well as any client software that the participant must download in order to be able to interact with the platform.

The gambling platform allows the operator to manage the gambling accounts of participants and the financial transactions for gambling, notify the gambling results, activate or deactivate registrations and accounts as well as set up all configurable parameters.

The gambling platform is composed of the following components:

● Databases that collect the personal details of gambling participants, all data on transactions performed by the participants and information concerning the results of the sporting events or tournaments, coefficients, etc.

● Payment gateways that allow financial transactions between the participant and the gambling operator and that contain the logic necessary for transferring funds, through the used payment method, from the participant to the operator and vice versa.

The gambling platform must comply with all technical requirements stipulated in this Regulation.

4. Game software: Game software means every software module or component, accessible from the gambling platform, which allows the management of each gambling activity, and the authorisation and implementation of the rules of such activities.

5. Random Number Generator: The random number generator, known by the Spanish initials GNA, is the hardware or software component that generates, through procedures guaranteeing its randomness, the numerical output used by the operator for determining the results of each game in which it is used.

Through a process called scaling, the raw output obtained by the random number generator is converted into a value within the range of values permitted in each game (52 card values, n bingo numbers). These numbers are converted into the symbols used by the game (cards, balls, etc.) through a conversion or mapping process.

6. Internal Control System: The Internal Control System, or SCI, is the set of components dedicated to recording the operations conducted in carrying out the gambling activities for the purpose of ensuring that the Directorate General for the Regulation of Gambling can continually supervise the gambling activities of the operator.

The Internal Control System is composed of the data capturer and the secure database or storage system of gambling operations.

7. Data capturer: The data capturer is the component in the operator's internal control system which is designed to capture and record the monitoring and control data stipulated by the Directorate General for the Regulation of Gambling, along with its conversion and storage in the device known as the storage system of gambling operations.

8. The secure database or storage system of gambling operations. The secure database or storage system of gambling operations (hereinafter, storage system) is the device located in Spain in which the data capturer records the monitoring and control data and which is accessible to the Directorate General for the Regulation of Gambling at any time. The information extracted by the data capturer from the gambling system must be stored in compliance with the format and structure stipulated by the Directorate General for the Regulation of Gambling.

9. User registration: User registration means the unique registration permitting the participant to access the gambling activities of a specific operator. It is composed of, but not limited to, data allowing identification of the participant and permitting financial transactions between said participant and the gambling operator.

10. Gambling account: A gambling account means an account opened by the participant and linked to his user registration, to which the participant adds monetary funds for the purposes of paying for his participation in the gambling activities and which is credited with the prizes or winnings obtained from the activity.

2. *User registration, gambling account and payment methods.*

2.1 User registration and restriction on participation.

Requirements in relation to the identification of gambling participants and the monitoring of individual prohibitions to participation are stipulated in articles 26 and 27 of the Royal Decree 1613/2011, and further elaborated upon in the relevant Resolution of 12 July from the Directorate General for the Regulation of Gambling.

This regulation expands on the minimum content of the user registration and the internal controls to be implemented by the operator.

2.1.1 Minimum content of the user registration.

Participants shall be identified through a user registration that must contain at least the following data:

- Identification details:
  - The tax identification number (NIF) or foreigner identification number (NIE) for residents. In both cases, the number must be stored in a standardised format.
  - An equivalent document for non-residents: identification document, social security card, passport, driver's licence.
  - Given name and surname(s).
- Personal details:
  - Date of birth.
  - Sex.
  - Address.
  - For non-residents, country of residence.
  - Nationality.
  - Email.
  - Telephone number.
- Tax residency details:
  - Tax residency code of the participant, in accordance with self-assessment form 763 for Gambling tax approved by Order EHA/1881/2011 of 5 July.
  - Non-resident participants must supply a copy of the document used for identifying themselves.

2.1.2 Storage of a copy of all supplied documents.

The operator shall implement the necessary technical procedures for storing a digital copy of the documents provided by the participants.

2.1.3 Gambling contract

The operator shall keep a record of the acceptance of the gambling contract and any amendments to it.

2.1.4 Verification services offered by the Directorate General for the Regulation of Gambling.

The Directorate General for the Regulation of Gambling offers operators an online service for verifying the identity details and date of birth of those participants resident in Spain, which is based on the NIF/NIE of the participant.

The operator shall keep a record of all queries made to the identity verification system and record the date and exact time of the query. The data must be stored together with user registration data for the period of the user's registration and the six years subsequent to the cancellation or termination of registration.

The Directorate General for the Regulation of Gambling offers operators an online service for verifying the registration of participants in the General Register of Gambling Access Bans:

● A service for checking, through the use of the NIF/NIE, the possible registration of a participant in the General Register of Gambling Access Bans for those participants resident in Spain. Operators must use this service to the check for such registration during the process of user registration.

● A consultation service for any changes (registrations/removals) in relation to the registration in the General Register of Gambling Access Bans of those participants whom the operator had previously verified. Operators must use this service every hour in order to check any changes in the registration of its participants in the General Register of Gambling Access Bans.

The operator shall keep a record of all queries made to the general register of gambling access prohibitions and record the date and exact time of the query. The data must be stored together with user registration data for the period of the user's registration and the six years subsequent to the cancellation or termination of registration.

2.1.5 User registration activation and restriction on participation.

The operator shall have a documented procedure for the registration and activation of the user that shall include the identity requirements and the restriction on participation stipulated in articles 26 and 27 of Royal Decree

1613/2011 of 14 November, elaborating on the technical requirements of gambling activities under the Gambling Act 13/2011 of 27 May.
The operator is responsible for the veracity of the data that appears in its user registrations and for the correct identification of the participants in any gambling that it organises or promotes. The operator must furthermore possess a verification service for identity details and dates of birth to ascertain the veracity of registrations. This service may be provided by third parties who supply professional identity verification services.
Operators must record and store all steps, queries and requests made for verifying the data supplied by applicants, as well as those documents received or used for this purpose. The data must be stored together with user registration data for the period of the user's registration and the six years subsequent to the cancellation or termination of registration.

2.1.6 Periodic review of user registrations.
The operator shall implement a technical procedure for the periodic review of user registrations under the terms stipulated in article 26.3 of Royal Decree 1613/2011 of 14 November, elaborating on the technical requirements of gambling activities under the Gambling Act 13/2011 of 27 May.

2.1.7 Cancellation of user registration.
The operator shall store the data of cancelled user registrations. The record shall include the time and reasons for the cancellation.

2.1.8 Suspension due to inactivity.
The operator shall keep a record of user registrations suspended due to inactivity, which shall include the suspension date.

2.1.9 Precautionary suspension of user registration.
The operator may suspend on a precautionary basis, until the facts have been verified, a participant who, in the opinion of the operator, has behaved in a

collusive or fraudulent manner or who has allowed his user registration to be used by third parties.

2.1.9.1 Fraud and money-laundering prevention measures.

The operator must have procedures in place for detecting fraud and money laundering. Procedures shall include the timely reporting of suspicious activities to the relevant public bodies for subsequent investigation.

In live betting games, the operator must have measures in place reducing the risk of some players being able to gain advantage over other players by betting with information on a particular result or following an event that fundamentally alters the odds of the bet.

2.1.9.2 Recording and reporting of precautionary suspension of user registration.

The operator shall keep a record of suspended users. The register shall include the date and reason for the suspension.

The DGOJ shall implement a telematic procedure through its electronic office which allows operators to report every month on locked or suspended accounts.

2.1.10 Single active-user registration.

The operator shall adopt the necessary procedures and mechanisms for ensuring a single active user registration per participant as required by article 26.2 of Royal Decree 1613/2011 of 14 November, elaborating on the technical requirements of gambling activities under the Gambling Act 13/2011 of 27 May.

2.1.11 Identification for access.

Once the participant has completed the registration process, he/she shall be allocated a unique user identifier. Access to the user registration and the gambling account must be reserved exclusively for the participant who is holder of the user registration.

2.1.12 User authentication and password policy.

Access to the user registration must involve security mechanisms for authenticating the user on the platform.

The user may be authenticated through the use of passwords. The password policy must entail at least the following minimum requirements:

● An initial user password must be established either by default or by the participant.

● During the process of creating a user password, the participant must be informed of the good practices in relation to choosing secure passwords.

● The minimum length of passwords shall be 8 characters or digits and must include elements from at least three of the following categories: numbers, lower-case letters, upper-case letters and other symbols.

● The password may not contain any of the following details: the username, pseudonym, given name, surname(s) or date of birth of the participant.

● The user must be reminded, on at least a yearly basis, to change his password, although such changes are not compulsory.

● The identification mechanism by means of the username and password must be locked if, during the same day, 5 failed attempts at access are made. The operator may establish a limit of fewer attempts to this requirement.

The operator's system must be designed so as to require the authentication of the participant prior to each commencement of a user session and, in the case of passwords, the entering of the password. The system shall not use cookies or any other mechanisms for avoiding the authentication of the user or the entering of the password.

The operator may provide other methods of user authentication provided that such methods offer a greater level of security than that of the password.

The system shall store a record of all access attempts, whether successful or otherwise, for its later auditing.

The operator shall have a documented security procedure for user access, which details:

· The manner in which the records on unauthorised user access is protected.

· The existence, or lack, of an indirect method, or a method with the assistance of the operator's staff, for accessing the user registration upon the correct answering of questions prior to granting or renewing access.
· The processing of user identifiers or lost passwords.
· The operator shall have a procedure for detecting accounts that are inactive for a reasonably extended period, and shall require a greater-than-normal authentication level or additional verifications through the customer service centre prior to allowing the participant to resume gambling and, in particular, withdrawing funds. The time period of inactivity, before which an additional level of authentication or verification as established by the operator is required, may not be longer than six months.

· Furthermore, the operator shall have a procedure for detecting, insofar as reasonable, unauthorised access to accounts of participants, phishing attempts or access to their personal details.
· The operator shall also have a procedure for detecting sudden changes in the behaviour of a participant and, in particular, in the amounts deposited or withdrawn. Accordingly, the operator shall initiate any action necessary for preventing the access to a gambling account by a third party.

2.1.13 Information to the participant regarding the last connection.
Once the user has been authenticated, the system will show the date and time of the user's previous access.

2.1.14 Record of session configurations for slot machine gambling.

In relation to slot machines, operators must record and store data on the user's configurations for each one of the user's slot machine game sessions, pursuant to article 14 of the Order HAP/1370/2014 of 25 July, which enacts the basic regulation for slot machine gambling.

2.2 Gambling account and deposits from participants.

2.2.1 Functionality of the gambling account.

Where the operator manages funds deposited by the participants, the operator must use a gambling account for keeping accounting records of the transactions.

Each user registration shall be linked to one or more gambling accounts. In the case of accounts linked to the same user registration, at least one such account shall permit the deposit and withdrawal of funds. The transfer of funds between different gambling accounts linked to the same user registration shall be immediate and free of charge for the participant. Each gambling account shall allow the payment for participating in one, several or all gambling activities offered on the platform.

The gambling account shall show all transactions that entail a change in the participant's balance, such as deposits from the participant, charges for gambling and any additional services provided by the operator, payments on bonuses offered by the operator and prizes obtained by the participant.

The gambling account shall be expressed in euros.

Corrections, cancellations or adjustments shall be recorded under separate entries. Under no circumstances may the original transaction be deleted.

Any bets once placed and subsequently cancelled by the operator must be recorded along with a clear statement on the reason for the cancellation.

The account entries in the gambling account shall clearly identify the nature of the transaction and the moment it was carried out.

2.2.2 Control procedure for deposits from participants.

The obligations of the operator in relation to the funds of participants are stipulated in article 39 of Royal Decree 1614/2011 of 14 November, elaborating on the licensing, authorisation and registration of gambling activities under the Gambling Act 13/2011 of 27 May. Such obligations must be supplemented by a

procedure that can guarantee their proper implementation and includes at least the following controls:

● There shall be a record book that is completed at least weekly, in which the operator checks and notes the balance of the funds deposited by the participants into the gambling accounts, the balance of each Spanish current account referred to in article 39 of Royal Decree 1614/2011, the time and date of the verification and the signature of the person appointed by the operator.

● If the balance of the funds deposited by the participants is below that of the current accounts, immediate measures shall be taken to increase the balance in the current accounts and the checking and noting in the record book will take place again on the following work day.

2.2.3 Record.

The participant shall be given the up-to-date balance of the gambling account and a record of all wagers or moves made over the course of at least the last thirty days

The participant may consult in real time a summary of the movements on his/her gambling account, covering at least the calendar year, which includes: the initial balance, total deposited, total withdrawn, total charges for participating in the gambling and for any additional services offered by the operator, total payments for any payments accepted by the participant and for prizes won, and the current balance.

The system shall be designed to allow real-time issuance, following application from the participant, of a document including the information described in the previous paragraph and containing the operator and participant's identification details. The operator shall have a procedure allowing those users without an active gambling account with the operator at the moment of the query to obtain such information through the operator's user service channels. With regard to the application of the participant, the operator must, subsequent to making the necessary identity verifications, provide the user with the requested document within ten days.

2.2.4 Currency of the gambling account.

The currency unit of the gambling account shall be the euro in accordance with article 35.2 of Royal Decree 1614/2011 of 14 November, elaborating on the licensing, authorisation and registration of gambling activities under the Gambling Act 13/2011 of 27 May.

The operator may use other units as bonus points, points to gain entry into tournaments, etc. The platform shall record the balance and the movements made in each of the units.

2.2.5 Restriction on transfers between participants

The operator shall implement technical procedures required to prevent the transfers between gambling accounts associated with different user registrations.

2.2.6 Promotional offers.

If the conditions of a promotional offer stipulates a specific amount, of points for example, to accumulate, the participant must be able to look up the points already accumulated or points remaining for fulfilling the conditions.

2.2.7 Accounts associated with user registrations that are not active.

Operations on the platform must be, completely or partially, restricted for user registrations that are not active. The operator must have a documented procedure of technical controls and reviews in order to ensure that gambling accounts associated with non-active user records do not make unauthorised movements.

2.2.8 Deposit limits.

The operator shall keep a record of the changes to the deposit limits according to user registration. The record shall include the date and reason for the change. It must be recorded whether the change was requested by the player or established by the operator.

Furthermore, the operator must retain the tests, passed by the player, on problem gambling prevention and on responsible gambling, which are necessary for applying for an increase of deposit amounts or the removal of any limit established on the player's deposits, as well as the historical analysis of the participant's actions in the event of a second or later application from the participant to raise the limits.

2.2.9 Positive balance.

Without prejudice to any other limitations to participation, where there is not a sufficient balance available in the gambling account at the time the player wishes to participate in a game or bet, said participation must be rejected.

Consequently, no gambling account may show a negative balance as a result of allowing gambling where there was not a sufficient balance.

2.3 Payment and collection methods.

2.3.1 Record of payment and collection transactions.

The operator must store or be in the position to obtain a detailed statement of every deposit or withdrawal, in addition to all the information associated with each transaction, whether by its own means or that of a third party.

Where additional pricing services are employed, the operator must store the information relating to the participation price and the identifier of the participated game or competition. The operator must also be in the position to obtain the telephone number and the bank account used in order to bill the player for participating.

2.3.2 Withdrawal of funds.

The operator shall establish a procedure for arranging the transfer of funds through the relevant payment method within a period of 24 hours. This procedure must stipulate that, in exceptional cases of failure to comply with the time frame, the Directorate General for the Regulation of Gambling must be notified of such in advance.

2.3.3 Monitoring procedure for payment and collection transactions.

The operator shall implement a procedure for cross-checking payment and collection transactions with the entries on gambling accounts or gambling software, which shall include at least:

● Verification that gambling accounts linked with non-active user registrations are not making unauthorised movements.

● Verification that deposit and withdrawal amounts match the transactions carried out through the payment methods.

● Verification that participants do not make deposits exceeding the limits established for that participant.

● Verification that withdrawals are arranged within 24 hours, unless there are exceptional reasons that have been notified in advance to the Directorate General for the Regulation of Gambling.

This procedure shall be performed on at least a monthly basis.

2.4 Personal data protection.

2.4.1 Data Protection.

Operators shall implement appropriate technical procedures for maintaining the privacy of participant details in accordance with the Organic Law 15/1999 of 13 December on Personal Data Protection and its supplementary regulations.

Also, in relation to files and processes, operators must incorporate the security measures stipulated under current regulations on data protection and comply with the duty on secrecy imposed by said regulations.

2.4.2 Privacy policy.

The operator shall publish its privacy policy on the gambling platform.

In order to complete the user registration process, the participant must agree to the operator's privacy policy. The platform shall record the participant's acceptance and the content of the privacy policy or a link to its text. Any

subsequent changes to the privacy policy must to be notified to the user and shall also require his/her acceptance.
The operator shall have a technical and operational plan for guaranteeing the data privacy of users.

3. Gambling

3.1 Basic regulations of the gambling activity.

The operator shall offer gambling and its forms in accordance with its licences and the basic regulations of each such gambling activity.
Operator gambling systems must incorporate procedures necessary for fulfilling the requirements stipulated in every game's basic regulations and in the relevant ministerial order and also, in particular, the established requirements relating to:

- Particular rules of the game.
- Claims by participants.
- Duties of informing participants.
- Promotion of gambling activities.
- Channels and means of participation.
- Objective of the gambling activity.
- Gambling participation and restrictions on participating.
- Realisation of the gambling activity, determination and allocation of prizes.
- Establishment of bets or moves as well as cancellation and postponement scenarios.
- Payment of prizes.

The operator shall establish a procedure, to be carried out at least on a monthly basis, which shall verify that the operator's gambling on offer is suited to the held licences. It shall also verify that the options and variant of each type of game comply with the current regulations and that the authorised software versions are being used.

The operator shall keep a record of active games at all times. The record shall indicate the game, option or variant, where appropriate, commercial name and the authorised version.

3.2 Redirection to the ".es" domain name.

The operator shall implement procedures and mechanisms to ensure that all connections from Spain or through a Spanish user registration to a domain owned or controlled by the gambling operator, its parent company or subsidiaries, are redirected to a website with the ".es" domain name.

Accordingly, the operator must establish measures allowing it, insofar as possible, to detect and prevent connections through network technologies that are designed to hide the player's IP address.

The operator must have a procedure allowing for the cross-check of the gambler's IP location with his country of residence and, if appropriate, the payment methods used in order to check for any fraudulent activity by the gambler.

3.3 Return percentage to the participant.

For each gambling activity, form or version, the operator shall determine the value or range of values expected for the return percentage.

The operator shall implement a procedure that shall help ensure the proper functioning of the expected return to the participant. It shall verify, at least on a monthly basis, that the return percentage to the participant obtained in any one of the gambling activities, options or variants, coincides with the expected value or ranges.

If any serious deviations are detected, the operator must deactivate the affected gambling activities, options or variants, until the problem is discovered and resolved. If improper functioning is confirmed, the operator shall notify the Directorate General for the Regulation of Gambling and state the cause, time period, the gamblers and amounts concerned as well as the adopted measures.

In those gambling activities where the return percentage may depend on parameters that are configurable on the technical system, such as prize tables, the operator shall keep a record of all changes to said parameters.

3.4 Prize tables.

Prize tables, in those gambling activities that have them, shall be public and available to participants. They shall include all possible winning combinations and a description of the prize for each combination.

Information on the prize scheme must clearly indicate whether the prizes are measured in units of account, monetary units or in any other established unit.

Information on the prize scheme shall reflect any change in the value of the prize that may occur during the course of the gambling. For these purposes, it will be sufficient that the operator arranges and shows a box presenting said changes to the value of prizes in a prominent position on the graphic interface of the gambling activity.

If there are jackpots or multiplying effects to the prizes shown on the screens, it must be specified whether or not the jackpot or multiplying effect affects the prize scheme.

The operator shall keep a record of prize tables for each game so that changes may be audited.

Prize tables may not be changed during the gambling activity unless such a case is stipulated in the particular rules and the participant has been adequately informed.

3.5 Random number generator (GNA).

3.5.1 Functioning of the GNA.

At a minimum, the Random Number Generator must comply with the following requirements:

- The generated randomised data must be statistically independent.
- The randomised data must be distributed evenly within the established range.

- The randomised data must remain within the established range.
- The generated randomised data must be unpredictable (its prediction must not be computable without knowing the algorithm and the seed).
- The series of generated data must not be reproducible.
- It must not be possible to synchronise different applications of the GNA which would allow the output of one to predict the output of the other.
- The seeding/reseeding techniques must not allow any prediction of the output.
- The mechanisms for generation must have successfully passed the different statistical tests that prove its random nature.

The technical system may share a GNA or its application for one or more games provided that the random behaviour of the system is not compromised.

3.5.2 Scaling methods.

Scaling methods must comply with the requirements placed on GNAs.

Scaling methods must be linear and must not introduce any bias, pattern, or predictability. It must also be possible to subject such methods to recognised statistical tests.

3.5.3 GNA Hardware.

In the event that GNA hardware is used, it must comply with the same requirements, adapted to the technical nature of the hardware and, in relation to where it is located, it must be guaranteed that no one who operates it can have any influence on the output. In the cases where GNA hardware is operated by staff, the operator must have a procedure in place minimising the hypothetical risks that could affect the output.

3.5.4 Faults in the GNA.

The operator must implement a monitoring system for the GNA, thereby allowing detection of its faults, as well as mechanisms disabling the game upon occurrence of a fault in the GNA.

3.5.5 Reseeding of the GNA.

The operator must have a procedure for reseeding the GNA.

3.6 Game logic.

3.6.1 Logic independent of the user terminal

All functions and logic that is essential for the implementation of the game's rules and the determination of the result must be created by the Central Gambling Unit and be independent of the user terminal.

3.6.2 Application of the GNA to gambling activities.

The GNA's value range must be concise and not distort the return-to-player percentage.

The conversion method for the symbols or results of the gambling activity must not be subject to any influence or control from any factor other than the numerical values derived from the GNA.

Chance events must be governed exclusively by the random number generator and there must not be any correlation between some turns and others. The game must not exclude any chance event unless such a circumstance is provided for in the rules of the gambling activity.

The gambling activity must not manipulate chance events, whether manually or automatically, nor manipulate them for maintaining a minimum return-to-player percentage.

Where the rules of the gambling activity require a sequence of chance events (for example, cards in a deck), the chance events shall not be rearranged during the course of the game unless such a circumstance is provided for in said rules.

3.6.3 Game logic controls.

The game must be designed in such a way so as to minimise the risk of manipulation. Technical, organisational and procedural measures preventing behaviour that may breach the rules of the game shall be adopted.

The operator shall have a documented procedure that details the measures applied to its system for ensuring that:

- Gambling progresses in accordance with the rules of the gambling activity.
- Gambling data is recorded on the system.
- The receipts or identification documents of a bet or participation are protected from any possible alteration.
- The system controls the time bets or stakes are made available. Closure of the bet or stake promotion must be in accordance with the provisions of gambling regulations and, in all circumstances, shall be prior to the final action which triggers the result of the game.
- The system monitors the established prize fund.
- The procedure for deciding winners is functioning correctly, and it does not introduce winners who do not fulfil the reward conditions, nor does it overlook those who do fulfil such conditions.
- The system will actually award the prizes to participants on the list of winners.
- All types of operations occurring during the game, including those for exception handling, system parameter changes, cancellations, manual actions, must be recorded on the system along with the relevant audit trail.

Any data modification, alteration or deletion must leave an audit trail, especially when the action has been done manually.

3.7 User terminals and physical terminals of an incidental nature.

3.7.1 Terminals.

Terminals are the set of software and hardware components that interact directly with the participant.

User terminals are those components provided by the participant. They may be hardware components, such as a personal computer, mobile phone or smartphone, or they may be software components such as the operating system or web browser.

Physical terminals of an incidental nature are terminals under the control of the operator which are intended to directly interact with the participant. Such terminals include those for self-service by the participant (kiosks or others), those intended for operation by the operator's staff, as well as those that are a combination of both.

3.7.1.1 Terminal identification.

The platform must be capable of identifying the different types and versions of terminals. A record of such identification shall be kept. The platform must record if the participant is using a specific solution provided for mobile devices, except in cases of duly justified technical reasons.

If the terminal is located in physical betting premises, casino or other authorised establishment, the platform must identify the establishment.

3.7.1.2 Terminal functionality.

The terminal shall only deal with the interaction with participants and the offered gambling activities.

The game logic or any other randomised component must be implemented by the Central Gambling Unit and be independent of the terminal.

Transactions conducted from the terminal must be simultaneously confirmed by the Central Gambling Unit before they may be considered formalised and obtain accreditation for the bets or deposits made.

All transactions carried out through the terminal shall be recorded in the central gambling unit and ascribed to a person who must have provided prior authentication, whether participant, operator, technicians or staff authorised by said operator. The records shall allow the transactions made from each terminal to be identified.

3.7.2 User terminals.

The technical requirements applicable to user terminals are set out below.

3.7.2.1 Installation of components on the user terminal.

If the installation of a component is required for using the gambling system, the express consent of the participant prior to installation must be acquired.

3.7.2.2 Disadvantage due to connection quality.

The operator is obliged to introduce all possible measures to their technical systems aimed at reducing the risk whereby certain customers are disadvantaged in relation to others due to technical factors affecting the speed of the connection.

The participant must be informed of those cases where the response time may have a significant effect on the odds of winning.

3.7.2.3 Information on connection quality.

The system shall inform the participant regarding the loss of connectivity with the gambling system as soon as such loss is detected.

The game software must not be affected by the poor functioning of the devices of the end participants, with the exception of the operation of procedures established for concluding turns or incomplete games.

3.7.2.4 Reduced functionality for certain user terminals.

User terminals with a smaller graphic interface than others (such as, mobile devices compared to personal computers) are allowed to offer some content that is not as fully visible as it is on larger terminals. The platform may offer different functionalities on different types of terminals on the grounds of strictly technical reasons resulting from the terminal's characteristics.

The participant must be informed of the information or functionality limitations of the terminal and client application being used. In such cases, there must be an express acceptance of such by the participant.

The operator shall alleviate any risks resulting from the lack of information or functionality on a particular terminal by offering the same information through other means.

All information that must appear on the interface must also appear on the terminal's interface except in cases of technical difficulties that are duly justified. In cases where it is not possible to include all information or links on the gambling interface, such information or links shall be offered via a link, menu or other application of that terminal.

3.7.2.5 Minimum resources of the terminal.

The platform shall not process any gambling activities from the terminal if it does not have the minimum resources that would allow its use without suffering technical problems or disadvantages.

3.7.3 Physical terminals of an incidental nature.

The technical requirements applying to physical terminals of an incidental nature are set out below.

3.7.3.1 Processing of participant details.

To guarantee the security and confidentiality of a participant's information, necessary measures must be adopted to ensure a participant's data is not accessible to any other participant subsequently using the same terminal. The terminal must not permanently store a participant's data. In cases where some of a participant's data is stored provisionally, the data shall be deleted at the end of the user's session.

3.7.3.2 Physical design.

The terminal shall be designed so as to minimise the possibility of it being tampered with by a third party which would place the participant using the terminal at risk. Accordingly, the following shall be taken into account: logical attacks such as through software tampering; physical attacks such as through unauthorised access of chips or ports; attacks through connections; and, combined attacks.

3.7.3.3 Terminal integrity.

The terminal must also enter a local record or log, which stores an audit trail for any modification, deletion or reinstallation of an installed software component, as well as any access and attempted access, whether locally or remotely. These records shall be kept on file for at least 90 days. The general requirement of six-year storage is not applicable. The technical system shall, on a daily basis at least, check that the terminal's software components are the approved components.

As a step prior to any installation of software components, the terminal shall use a system to verify that any software component to be installed is authentic and has not been modified.

The terminal shall be reasonably designed to detect any erroneous or insecure operation and, where appropriate, it must warn the participant and restrict its operation.

While a participant is using a terminal, the operator may remotely access the terminal over normal connections only for carrying out the gambling activity with the Central Gambling Unit, the monitoring of quality, security and performance, and planned periodic tasks such as the download of content. The operator may also access the terminal in order to resolve problems or technical incidents, provided that the participant is notified. Prior to allowing any access of this kind, the terminal must authenticate the operator's system and establish a secure connection.

3.7.3.4 Mobile terminals.

In the case of mobile physical terminals of an incidental nature, the terminal shall include mechanisms allowing the operator to monitor the location of the terminal.

3.8 User session.

A user session is the period of time during which a user remains connected to the operator's website, counting from the moment of authentication of the user on the system until disconnection of said user.

3.8.1 Disconnection due to inactivity.

The time of inactivity leading to disconnection shall be no more than 20 minutes, after which the platform must disconnect the user.

When the operator performs communications in one direction where the participant is expected to behave passively, for example in the broadcast of a live sporting event, the user may be considered active despite the lack of action on the part of said user.

If technically possible, the participant shall be informed that the session has ended.

3.8.2 Record of user sessions.

The platform shall keep a record of user sessions, detailing the start and end times of the session, authentication methods employed by the user and reason for disconnection or inactivity.

If the terminal belongs to the user, the platform shall allow identification, if technically possible, of the type of device (computer, smartphone or other), the application/version used (browser or actual application), and the IP address where appropriate.

If the terminal belongs to an operator, it shall allow identification of the type and version of the terminal as well as the actual terminal if technically possible.

3.9 Graphic interface.

3.9.1 Gambling details.

The name of the game being played by the participant must be clearly visible on all related screens.

Instructions for the gambling activity must be easily accessible. The graphic interface must include all the information necessary for carrying out the gambling activity. The function of all action buttons shown on the screen must be clear.

The outcome of each turn must be shown instantly to the participant if technically possible and be kept on screen for a reasonable period.

3.9.2 Participant details.

The screen must show both the current balance of the participant at least in euros and the bets wagered in unit and total amounts.

3.9.3 Prizes.

The interface must clearly indicate whether the prizes are shown in euros or credits. The prizes must not be switched between different units which could confuse the participant.

If random prizes associated with a turn or bet are offered, the participant must be made aware of the maximum amount obtainable from the turn or bet that is about to be made.

The participant must be informed when the amount of the random prize is determined on the basis of the amount placed for the turn or bet. When the text or graphics announce a top prize, such a prize must be obtainable through a single game.

3.9.4 Card games.

Card games must fulfil the following conditions:

- Card faces must clearly show the value of the cards.
- Card faces must clearly show the suit/colour of the cards.
- Jokers must be distinguishable from the other cards.
- The use of more than one deck in the game must be clearly shown.
- The player must be clearly informed of the frequency of possible shuffling of cards during the game; such shuffling must be shown at the time it is performed.

3.9.5 Simulation of real-life features.

Gambling activities that simulate real-life features (roulette, raffle drums, etc.) must behave in way that is as similar as possible to the behaviour of said physical features. The probability of an event occurring in a simulation, which

affects the outcome of the gambling activity, must be equal to that of the real-life event.

3.9.6 Third-party graphic interface.

Third-party graphic interfaces are those interfaces not offered by the operator as part of its platform or where the operator includes a link for downloading the interface and next to the link it is clearly stated that the interface is not the responsibility of the operator.

Participants who decide to use a third-party user interface must be informed by the operator that they may not gain complete functionality and information.

3.10 Integration with providers and into gambling networks of other operators.

The operator shall be responsible for gambling operations conducted through third parties or providers. The technical systems of third parties or providers will be considered as part of the operator's technical system for these purposes. Such systems must comply with the specifications stipulated in this Regulation.

The operator must ensure that any integration with the systems of other operators is performed in compliance with the specifications stipulated in this Regulation.

3.11 Disabling a gambling activity or a user session.

The platform must allow under exceptional circumstances the possibility to disable a game in its totality, or particular user sessions, and record the actions and their reasons for subsequent review.

3.12 Incomplete game.

An incomplete game is where the result has still not occurred or, if it has occurred, it has not proven possible to inform the participant of said result.

In the event of an incomplete game, the particular rules of the game shall decide the platform's action, which may be to wait for a participant, cancel the game or continue as if the game were complete.

- If an incomplete game is due to a user's terminal losing connection, the platform will show the incomplete game when the participant reconnects.
- The operator must have a documented procedure for managing the downtime of one, several or all components, which includes associated technical measures. The components must run a self-diagnostic, a critical file check and an inter-component communication check.
- Following recovery, the technical gambling system must handle the on-going games affected by the interruption.

The technical system shall keep a record of service interruptions, with details on its time, duration and affected services for later review.

3.13 Automatic gambling.

If the system offers gambling-strategy advice or options for automatic gambling, such advice or options must be true and ensure that the gambling activity abides by the compulsory return percentage.

It must be ensured that the participant retains control of the gambling activity when he opts for the automatic-gambling mode. The participant may control the maximum amount of automatic plays or the highest betting amount and the number of automatic bets. The participant may deactivate the automatic-gambling mode at any time.

When the automatic-gambling mode is activated, the information shown on the screen (duration, graphics or others) shall be the same and have the same characteristics as when the game is not in automatic mode. The interface shall also show the number of automatic turns played or remaining.

The automatic repetition of play may not place a participant at a disadvantage, and neither the sequence of automatic games nor any strategy recommended to the participant must be misleading.

In gambling activities where more than one participant is involved, all participants must be informed of and accept a participant who has opted for the automatic-playing mode.

3.14 Move repetition.

The platform must provide the participant with the option to repeat a move, which will be shown as a visual reconstruction or an understandable description that must perform all moves having a consequence on the gambling activity's progress. The option to repeat the move must supply all information necessary for replicating the last ten games played during the user session in progress.

3.15 Virtual players.

3.15.1 Virtual players provided by the operator.

The operator may use artificial intelligence through virtual players, otherwise known as robots, provided that the relevant gambling regulation explicitly permits such use.

In gambling activities where more than one participant is involved, all participants must be informed of and accept the participation of a virtual player.

Virtual or automatic players must be clearly identified on the interface.

The virtual player must not have any technical advantage over the participant, nor have access to information that is not available to said participants.

3.15.2 Virtual players used by participants

The operator may supply artificial intelligence to participants through the use of virtual players or robots provided that the relevant gambling regulation permits such use.

The operator shall inform participants on whether or not they may use virtual players or robots. Where such use is permitted and a gambling activity involves more than one participant, the operator must ensure that all participants know which participants are virtual players or robots. Where such use is not permitted and a gambling activity involves more than one participant, the operator must attempt to prevent the use of virtual players by participants and in the event of detecting such use all participants must be immediately notified of this fact. Participants must have a mechanism for reporting the existence of a possible virtual player.

The operator shall have procedures for detecting the use of artificial intelligence methods by a participant.

3.16 Metamorphosis games.

Metamorphosis or evolution games must:

- Inform the participant of the rules applicable at every moment or stage of the game.
- Indicate the approaching metamorphosis to the participant by providing sufficient information. For example, if the participant is collecting items, the interface must show the number of items to be collected for the metamorphosis or those remaining to be collected before said metamorphosis.
- The probability of a metamorphosis must not vary on the basis of the prizes obtained by the participant in previous games. Any exception to this point must be authorised in advance by the Directorate General for the Regulation of Gambling.
- The information and the game must not be misleading or ambiguous.

3.17 Absent participant.

During a gambling activity involving more than one participant, the platform must allow any user to place his status as "absent" or on "pause". Such statuses may be used if the participant needs to stop playing for a brief period that must not exceed twenty minutes. The participant cannot take any new turns while his status is "absent". If he takes a turn, his status automatically returns to active. The "absent" status shall remain in the event that any actions taken do not affect the gambling activity (e.g. consulting a help page).

3.18 Hosted multiplayer games.

In games where a participant acts as host, the participant may decide on who to accept as a participant or whether a participant must first receive an invitation. The host may not exclude participants from a game if they have been previously accepted to join the game.

3.19 Live-broadcast games.

Live-broadcast games are those games using an actual croupier or an actual game table as a game device, and said game involves a broadcast and online-betting system.

The participants may view a broadcast online which allows them to follow the game and know the outcome.

There must be procedures for actions on resolving incidents that may occur during real-time gambling operations.

Automatic devices used for recognition and registration must be equipped with an option of manual operability which allows correction of any erroneous result. The participant must be informed that the manual option has been activated. Every time the manual operability option is activated, it must leave evidence of such for a subsequent review.

There must be procedures for dealing with game interruptions caused by lapses in the flow of data, video and voice.

3.20 Jackpots, progressive jackpots and additional prizes.

The operator may set up jackpots, progressive jackpots or additional prizes provided that they are permitted under the basic regulations of the relevant gambling activities.

Where the participant is contributing to any jackpot, the platform shall clearly inform him of such as well as the method to compete for said jackpot. All participants contributing to the jackpot must have the opportunity to compete for said jackpot while gambling. The conditions of the jackpot and the requirements for winning it must be communicated to the participant.

The conditions of the jackpot must take into account any completion or interruption of the gambling activity, whether foreseeable or otherwise, as well as any technical interruptions to the system.

The operator's system shall maintain an account linked to the management of jackpots, thereby allowing control of the jackpots and identifying at the very least:

- The creation of each jackpot.

- The time periods during which each jackpot has been active.
- The configurable features that are active at any time for the jackpot.
- The games or machines involved in or contributing to the jackpot at any one time.
- The jackpot's balance at all times, and the contributions to it from every type of game or machine.
- The prizes awarded on the basis of the jackpot, describing the winner, amount and time of award.
- The record of manual actions affecting the jackpot's balance.
- The transfer or redirection of funds to another jackpot.
- The close of a jackpot or the moment it was cancelled.

The operator must have a procedure providing control over the jackpots and ensuring that the jackpot is created, managed and awarded in accordance with the rules of the game.

In particular, the operator must check on at least a monthly basis:

- The proper functioning of the jackpots as well as their balances and movements.
- That once the jackpot has been created and available for winning, the conditions do not change until the jackpot has been won by one or more participants and the amount has been paid out.
- That the procedure for deciding winners is functioning correctly. The procedure must not introduce winners who do not fulfil the reward conditions, nor must it not award those who do fulfil such conditions.
- That the system awards prizes to participants on the list of winners.
- If applicable, special attention will be placed on systems redirecting a jackpot through which part of the accumulated jackpot is redirected to another fund and may be won later. The system redirecting a jackpot may not be used as a means to postpone indefinitely the awarding of a prize.

Where a jackpot stops functioning properly, the participants must be informed of such through messages on their terminal such as "jackpot closed" or other such messages. It shall not be possible to win an accumulated jackpot that has been closed beforehand.

3.21 Gambling through pre-recorded communication channels.

Pre-recorded gambling covers those gambling activities whose randomness, or other element, leading to its outcome has been obtained prior to the commencement of interaction between the participants and the game during the round.

The operator shall adopt the necessary technical, security and organisational measures for preventing that neither the operator, nor its staff, nor participants obtain any advantage resulting from prior knowledge, whether partial or otherwise, of the elements that may determine the result.

4. Security of Information Systems

The purpose of the security requirements on technical gambling systems is to protect the user registrations and associated gambling accounts of users as well as to guarantee that the gambling activity is carried out correctly.

4.1 Critical components.

Critical components are those parts that must have enhanced security since they have a significant role in the realisation of the gambling activity.

Critical components are:

- In relation to the user registration, gambling account and processing of payment methods: components of the technical gambling system that store, handle and transmit sensitive information of customers, such as personal, authentication or financial details, as well as those components that store the occasional status of games, bets and their outcomes.
- In relation to the random number generator: components of the technical gambling system which transmit or process randomised numbers upon which the outcome of gambling activities are based and the integration of the outcomes from the random number generator into the game logic.
- Connections with the Directorate General for the Regulation of Gambling.

- With regard to the internal control system: the data capturer and the storage system.
- Points of access and communications to and from the above-mentioned critical components.
- Communication networks that transmit sensitive information of the participants.

4.2 Security management of the technical gambling system.

The operator must implement a management system for security, which will protect, in particular, the critical components referred to in the above provision.

The security procedures must be aimed at implementing specific security measures on the basis of a risk assessment. The operator must schedule periodic reviews and perform reviews arising from significant changes.

4.3 Risk management.

The management of risks shall identify elements to be protected, and then conduct a periodic identification, quantification and prioritisation of the risks faced by the technical gambling system. The management of risks must be expressed in an action plan.

4.4 Security Policy.

Operators must have in place security procedures of which all its employees and, if appropriate, external collaborating bodies are informed.

4.5 Organisation of the Information Security.

Operators must establish a management framework for information security which states the roles and responsibilities of its staff.

4.6 Security of communications with participants.

Authentication mechanisms allowing the gambling system to identify the participant and vice versa must be adopted.

The operator must establish systems and mechanisms that guarantee the confidentiality of participants' communications with the technical gambling system and especially with the Central Gambling Unit and its replication. In relation to the transmission of personal or financial details (i.e. user registration and gambling account respectively), such communications shall be encrypted.
The operator shall adopt all necessary measures for guaranteeing the completeness and non-rejection of communications where personal or financial details are transmitted, and where gambling transactions are involved.

4.7 Staff and third-party security.

The security plan for the operator's staff shall include training activities, recruitment management, employment changes and terminations, with particular attention on the authorisation of access to information and critical components.
Where the operator requires services from third parties that may involve access, processing, communication or handling of information, or even access to facilities, products or services related to gambling, said third parties must fulfil all security requirements that are applicable to the operator's staff.

4.8 Physical and environmental security.

With regard to the physical security of components of the technical gambling system and their replication, the security plans of operators must include the following:

- Perimeter security for those areas containing critical components and sensitive information: enclosures, access cards, etc.
- Physical access control to facilities that store equipment for both employees and outsourced staff. Such control includes physical items, authorisation procedures, access records and surveillance services.
- Protection of critical equipment from environmental risks: water, fire, risks caused by any person, etc.

- Protection of critical equipment from electricity cuts and other interruptions caused by faults in ancillary facilities. The cabling of the electrical mains must be protected from damage.
- Access control to the communications cables in the event that unencrypted critical information is transmitted through them.
- Maintenance of the facilities and equipment.
- Devices containing information must be securely erased or destroyed prior to their reuse or disposal.
- Equipment containing information may not be transferred outside of secure facilities without correct authorisation.

4.9 Management of Communications and Operations.

The secure and proper functioning of the technical gambling system and communications, must be guaranteed:

- Critical components must be monitored in order to prevent the possible use of versions different to the authorised versions.
- The integrity and confidentiality of communications between the components of the technical gambling system shall be guaranteed.
- Tasks shall be divided among the different areas of responsibility in order to minimise the possibility of unauthorised access and potential damage.
- Tasks related to development, tests and production shall be separated.
- Services provided by third parties must include security controls and metrics in the contracts and such services must be audited and monitored on a periodic basis.
- Measures shall be adopted to protect the system from malicious code.
- Backup files must be created on an appropriate regular basis and be securely stored as per the plan for backup files.
- Security measures for the communications network shall be adopted.
- Security measures preventing the manipulation of removable media, as well as measures for the secure deleting or destruction of such media, shall be adopted and expressed in a documented procedure.

- Internal clocks of all components, especially critical components, must be synchronised with a reliable time source. The reliable time source may be different for each component. The operator shall establish controls and measures to prevent manipulation of time stamps or their subsequent alteration, especially in the audit trails.
- An audit trail for the activities of all users, information security exceptions and incidents covering a minimum period of 2 years must be created and kept.
    - The audit trails shall be protected from any alteration and unauthorised access.
    - The activities of the System Administrator and System Operator must be recorded.
    - The audit trails shall be periodically analysed. Actions based on detected incidents shall be taken.

4.10 Access Control.

Any access by the operator's staff and participants must fulfil the following requirements:

- There must be a documented policy on access to information which is periodically reviewed.
- Authorised access must be ensured, while unauthorised access prevented, through controls on user logins, management of access privileges, periodic review of such privileges and a policy on the management of passwords.
- Users must follow good practices in the use of passwords and adequately protect documentation and media at their workstations.
- Users shall have access only to those services that they have been authorised to use.
- There shall be no generic usernames and users shall have access through the use of their own unique username.
- The system must authenticate each and every access, whether by the system's staff, maintenance staff, etc., or by other systems and components (for example, the payment gateway). Access by the inspection staff of the

Directorate General for the Regulation of Gambling or other staff acting on its behalf must also be authenticated.

- The networks shall be separated on the basis of the area and accountability of the task or role.
- Access to operational systems shall require a secure authentication mechanism.
- The use of programs allowing the bypass of access and security controls shall be restricted and controlled.
- User sessions shall have a maximum time limit of connection and also a period of inactivity leading to disconnection.
- IT staff shall have restricted access to the real data of applications. Sensitive real data shall be located in isolated environments.
- Risks associated with mobile devices shall be managed.
- Where teleworking is possible, the associated risk must be verified that it is being managed within the framework of the security plan.

4.11 System purchase, development and maintenance.

Any decisions taken on the purchase, development and maintenance of information systems must be analysed for their impact on security.

4.12 Management of security incidents.

The operator must have a documented procedure for the management of any security incidents.

All security incidents must be recorded. The facts, consequences and the adopted measures shall be clearly and concisely documented.

4.13 Change management.

Reports of authorisation and certification shall include a list of critical components in accordance with article 8.5 of Royal Decree 1613/2011 of 14 November, elaborating on the technical requirements of gambling activities under the Gambling Act 13/2011 of 27 May. The Directorate General for the Regulation of Gambling may classify other components as critical.

From the moment of commencing its activity, the operator must have in place a documented procedure for the management of changes, which monitors any changes to equipment and components of the technical gambling system in use.

a) There shall be formal process for the internal approval of all changes, which must involve the request for the change and its approval by the relevant managers.

b) In the case of changes to critical components, it must be assessed whether such changes are of a significant nature.

c) Change requests and the decisions taken in this regard must be recorded and they may be subject to a subsequent audit.

d) In relation to all software versions used in the technical system over the last four years, the operator must store copies of the binary files of the software elements. The Directorate General for the Regulation of Gambling may establish an obligation to include a fingerprint of the binary files that are the subject of the storage procedure.

4.14 Management of service availability.

The operator must have a plan for the management of service availability. Within the plan, the operator must take into account each of the following services:

- Registration of the participant, gambling accounts, including the possibility of depositing and withdrawing funds.
- Gambling services.

The plan shall state the maximum accumulated time per month each service may be unavailable as well as its maximum recovery time. The operator shall adapt its infrastructure and processes and it shall implement the measures necessary for fulfilling the objectives set out in its plan for the management of service availability.

4.15 Plan for preventing information loss

The operator must have a plan guaranteeing that there is no loss of data or transactions affecting, or likely to affect, the realisation of gambling activities, rights of participants or the public interest. The plan must also state the risk assumed by the operator.

The operator shall adapt its infrastructure and processes and it shall implement the measures necessary for fulfilling the objectives set out in its plan containing the following minimum requirements.

- Copies of the information shall be stored in a location suitably far from the data being safeguarded.
- The copy of information shall be protected from unauthorised access through security measures that are analogous to those protecting the information being safeguarded.

The operator shall have a documented action procedure for cases of information loss which includes the mechanisms for dealing with claims from users, the resumption of gambling or interrupted bets and any other consequential circumstances.

In the event of a loss of information, the operator must immediately inform the Directorate General for the Regulation of Gambling and state the actions taken along with an estimate on the consequences of the loss.

4.16 Business continuity management.

The operator must have a plan on the continuance of business in order to maintain gambling activities operational in the occurrence of emergency situations. The plan must include technical, staff and organisational measures necessary for guaranteeing the continuance of the service and a substitute for the Central Gambling Unit that will allow normal business to be carried out.

The business continuity plan shall define one or more recovery scenarios and state, for each scenario, the recovered services and the maximum amount of time required for said services to become operational again. Within the plan, the operator must take into account the following scenarios:

- The access of participants to their user registrations and gambling accounts, with the possibility of checking the balance and movements on their

gambling accounts. The maximum amount of time for providing these services again shall be one week.

- The possibility of participants withdrawing funds. The maximum amount of time for providing these services again shall be one week.
- The continuation of incomplete gambling activities or pending bets and the paying out of validly won prizes. The maximum amount of time for providing these services again shall be one month.
- The complete re-establishment of all services.

The operator shall adapt its infrastructure and processes, as well as implement the necessary measures, for making possible the objectives set out in its plan on the continuance of business.

In the event of an emergency situation, the operator must immediately notify the Directorate General for the Regulation of Gambling and carry out an estimate on the impact of the situation and the time required for recovery.

4.17 Penetration testing and vulnerability analysis.

The gambling system must undergo a penetration test and vulnerability analysis on at least an annual basis. Technical systems, or those parts being only for information purposes, on which no bets are made and there is no access to the user registration or gambling account, shall be exempt from the obligation to conduct such tests and analyses.

Technical systems with which the player interacts through telephonic or text messaging services shall also be exempt from this obligation.

The penetration test and vulnerability analysis may be conducted by entities that are not the entities appointed to assess security, or they may even be conducted with the operator's own resources in cases where the operator possesses the appropriate resources.

The penetration test shall entail an assessment method for the security of a network or system by means of simulating a third-party attack. The process includes an active analysis of the system which searches for weaknesses, technical faults or vulnerabilities. The test shall include all public interfaces that store, process or transmit personal, financial or gambling data.

The vulnerability analysis shall entail the identification and passive quantification of the potential risks to the system. The analysis shall include all components that store, process or transmit personal, financial or gambling data.

The results of the test and analysis must be stored, for their subsequent review or inspection, together with the corrective measures that have been applied or scheduled.

Prior to the marketing of gambling, the technical system must have successfully undergone a penetration test and vulnerability analysis. The scope and results must be evaluated by one of the entities appointed for the certification of security during the certification process.

In the event that a very serious security failure is detected in the test or analysis which could place at risk the identity or financial situation of players or allow theft of such information, the operator shall immediately report the failure to the DGOJ along with the action plan that has been set out. The DGOJ may require the affected gambling on offer to be suspended until the failure has been rectified.

In relation to security incidents of a minor nature, the operator shall adopt an improvement plan and the scope of the subsequent test or analysis shall include the verification that the previously detected incidents have been appropriately rectified.

The operator must retain the full report of each conducted test and analysis for at least four years.

5. Internal Control System and inspection

5.1 Internal Control System.

5.1.1 Description.

Gambling activities conducted by the operator shall be monitored and supervised through the internal control system (hereinafter, SCI), which must be implemented by all operators.

The SCI must capture and record all gambling operations and financial transactions of participants located in Spain or with a Spanish user registration, irrespective of their means of participation.

The internal control system must be adapted to the different marketing channels for gambling and channels of interaction with participants so that the capture and recording of all gambling operations may be ensured.

Where different channels of marketing or of participant interaction are simultaneously employed in a single gambling activity, the operator must state the gateways, interfaces or communication channels among all means of participation or interaction of that gambling activity for the purposes of allowing the Directorate General for the Regulation of Gambling to access the performed operations and transactions in their entirety regardless of the means used for said activity.

The operator must establish and maintain a secure connection for access by the Directorate General for the Regulation of Gambling, as well as a service for queries and downloading data that is always available to the Directorate General for the Regulation of Gambling.

The SCI is composed of a data capturer and a storage system of gambling operations (storage system).

5.1.2 Access to the storage system by the Directorate General for the Regulation of Gambling.

The storage system shall always have the following access points open to enable access by the Directorate General for the Regulation of Gambling.

- Access through the SFTP protocol in order to download information.
- SSH access with read-only attributes and sufficient privileges for listing and viewing the content of the entire storage system.

The operator shall provide the following authentication methods to the Directorate General for the Regulation of Gambling.

- For manual access – username and password.
- For automated downloading – the operator shall set up an exchange of a set of keys (SSH key swap) for the same user described in the manual access.

The operator may use several storage systems. Data must be reported only once thereby avoiding redundant information being contained in different storage systems.

5.1.3 Data model for the SCI.

The Directorate General for the Regulation of Gambling shall establish the data model for the SCI by means of a resolution.

The data model for the SCI contains the range of data to be recorded, the frequency of updating such data and the technical requirements of availability and access, under the terms stipulated in article 24 of Royal Decree 1613/2011 of 14 November, elaborating on the technical requirements of gambling activities under the Gambling Act 13/2011 of 27 May.

The data shall be stored in an XML file structure according to the defined scheme for data monitoring (XSD-XML Schema Definition).

5.1.4 Time source of the SCI.

All components of the technical gambling system, including the data capturer and storage system, shall be synchronised with a reliable time source.

5.1.5 Signature, compression and encryption of SCI data.

That data to be recorded in the storage system shall be grouped together in batches. Each batch must be digitally signed, compressed and encrypted by the operator who must use the format and procedure detailed in the monitoring data model.

The operator must supply the Directorate General for the Regulation of Gambling with the public key of the electronic certificate which will be used for digitally signing the batches. The operator must inform the Directorate General for the Regulation of Gambling of any revocation of the electronic certificate.

The operator may use its own certificate or employ a third party who will sign the batches on behalf of the operator.

5.1.6 Efficiency of the data capturer and storage system.

The data capturer must have the capacity to process and record the information of gambling operations.

Except where duly justified, the data capturer must be designed in order to process, format and record the information in the storage system within a maximum time limit of twice that defined for real time in the monitoring data model.

The storage system shall have a capacity, or minimum Internet transfer rate, sufficient for the Directorate General for the Regulation of Gambling to access it:

- For downloading data – it must have a guaranteed minimum transfer rate that would allow the maximum amount of information generated in a day to be downloaded in four hours through the SFTP protocol.
- For uploading data – it requires a minimum transfer rate of 64 kbps.

The storage system must perform equal to or better than what is necessary for guaranteeing the described transfer rates, regardless of any other operations it must carry out.

5.1.7 Security of the SCI.

The SCI in its entirety, including the data capturer and the storage system of gambling operations, are considered critical components. The security requirements stipulated in section 4 therefore apply to the SCI.

Although the data model requires the information in the storage system to be eventually encrypted, such information is not required to be encrypted at all times. The chain of custody for the encryption key must be included in the security design of the SCI.

The data capturer must be able to record transactions at all times and on a continuous basis. In fulfilling this requirement, the operator must devise the

availability, plan for preventing information loss, recovery time after emergency situations and business continuity.

5.1.8 Unavailable SCI and suspension of the gambling on offer.

In the event that the internal control system becomes unavailable, the operator must suspend the gambling on offer

In the case that the storage system is unavailable for 24 hours, the operator may continue the gambling on offer if the capture system remains operable and is capable of recording transactions until the storage system becomes available. The operator shall suspend the gambling on offer where the storage system in unavailable for over 24 hours.

5.1.9 Availability of the SCI.

The data capturer must be able to record transactions at all times and on a continuous basis. The storage system may not have an accumulated downtime greater than 48 hours per month.

5.1.10 Plan for preventing information loss in the SCI.

The SCI is a critical component. Gambling operators must implement a procedure that minimises the risk of losing information for a period greater than 24 hours.

In the event of information loss in the SCI, the operator must have a procedure for newly extracting the lost information which may rectify the loss within one week.

Any loss of information affecting the SCI must be immediately reported to the Directorate General for the Regulation of Gambling, along with an assessment of the loss and a plan for the measures to be applied.

5.1.11 Information quality of the SCI.

The operator must have a documented control procedure for the data quality of the SCI. This procedure must be performed at least monthly and shall include, as a minimum, the following verifications:

- That the data includes all participants registered with the operator.
- That financial data includes all gambling transactions for the period, consisting of deposits and withdrawals, and that the obtained figures match the official figures of the operator.
- That the participants' account balances are adequately described in the information of the internal control system.
- That the monthly and daily files for the period have been created.

The operator shall store documentation of previous verification results. Said documentation shall include the date of verifications, the signature of the supervisor on behalf of the operator, the main financial and registered user figures transmitted in the files of the internal control system, as well as their comparison with the operator's official figures.

The operator must be prepared to rectify incorrect data within one month by means of new extractions.

5.1.12 Continuity of business in the SCI.

Considering that the gambling on offer is suspended upon the SCI becoming unavailable, the operator must have a business continuity procedure which, in the event of an emergency situation, allows the SCI to become operational within one month.

Any emergency situation affecting the SCI must be immediately reported to the Directorate General for the Regulation of Gambling, along with an assessment of the loss and a plan for the measures to be applied.

5.1.13 Storage of SCI information.

The storage system must retain its data for a minimum period of six years.

Gambling operators shall have the duty to allow and provide the Directorate General for the Regulation of Gambling with online access to information related to the previous 12 months of activity recorded on the storage system.

Operators must plan to implement a procedure for recovering information related to a period of no less than six years.

5.1.14 Location of storage system in Spain.

The storage system or systems of the SCI must be located in Spain for the purposes of carrying out verifications and checks on the information. The location and any changes to the location must be reported to the Directorate General for the Regulation of Gambling.

Backup copies of the storage system or replication sites of the principal system may be located outside of Spain.

5.2 On-site and telematic inspection.

The Directorate General for the Regulation of Gambling must have the opportunity to monitor and supervise any elements of the technical gambling platforms of operators.

Therefore, the operator must link the necessary mechanisms for the secure connection to its technical systems, as well as allow and provide access of the systems at all times to the Directorate General for the Regulation of Gambling, regardless of the location of the systems.

The Directorate General for the Regulation of Gambling shall inform the operator of its intention to connect to the technical gambling system and provide a description of the functionalities that it intends to access along with the expected time and duration of said access.

The operator shall provide the Directorate General for the Regulation of Gambling with the means for securely accessing the system. Staff appointed by the operator shall assist the Directorate General for the Regulation of Gambling in adequately accessing and checking other systems and applications. The Directorate General for the Regulation of Gambling may make recordings of the user session and as many checks as is necessary for performing its duties.

Unless otherwise required, the access provided to the Directorate General for the Regulation of Gambling shall be on a read-only basis and shall have the authorisation level needed to access all systems and applications of the technical gambling system without any filter on the accessible data.

Once such access has concluded, the operator must close the secure access.

6. Records and logs of the Technical Gambling System

6.1 Records and traceability.

The operator shall maintain records and logs of all decisions made by the participant, operator, its staff or systems, which may have an impact on game progress, user registration, gambling accounts or payment methods.

With regard to game progress data, the data must be able to reconstruct all moves that may have a consequence on its progress. The Technical Gambling System must store all records and logs pertaining to security of the IT systems. The Directorate General for the Regulation of Gambling must have online access to said records and logs for a period of no less than 12 months. The operator may be exempted from this requirement, on an exceptional and justified basis, following prior request of authorisation from the Directorate General for the Regulation of Gambling. Without prejudice to the foregoing, the records and logs must be stored for at least 6 years.

Operators must plan to implement a procedure for recovering such information.

Records and logs shall be designed in such a way as to prevent deletion or modification.

In the event of the operator having to delete an entry, for example, in order to correct technical errors, such deletion must be approved by the operator and the supporting documentation for the changes must be retained.

6.2 Records according to the marketing channel.

Particular terminals and procedures for participation have specific requirements on the recording of gambling operations. These requirements shall not affect other communications between the operator and participants which are different to those for the realisation of the gambling activity.

These particular terminals and procedures shall apply to the recording of messages sent and received for gambling activities conducted through text messages, landline or mobile telephone services or audio-visual communication methods.