I. GENERAL PROVISIONS

MINISTRY OF ECONOMY AND FINANCE

18055 *Resolution of 16th November 2011, of the Directorate General for Gaming Regulation, approving the provision supplementing the technical specifications that must be complied with by technical gaming systems object of the licences granted under Act 13/2011, of 27th May, of gaming regulation.*

Act 13/2011, of 27th May, of gaming regulation, establishes the regulatory framework of gaming activity, for the different modes, developed at the national level, in order to guarantee public order protection, to fight against fraud, to prevent addictive behaviour, to protect minors' rights and to safeguard game players' rights.

The establishment of the technical requirements of said Act 13/2011 was the object of Royal Decree 1613/2011, of 14th November, which confers in the first final Provision to the National Game Commission the development of certain technical aspects of gaming activity commercialisation object of said Act.

Given the National Game Commission has not been effectively established and in application of the first provisional provision of Act 13/2011, of 27th May, of gaming regulation, this Directorate General for Gaming Regulation of the Ministry of Economy and Finance is in charge of developing and specifying the technical requirements established in said Act 13/2011 and in Royal Decree 1613/2011, of 14th November, to supplement it.

By its virtue, and after the favourable report of the State's Attorney General's Office at the State Secretariat for Finance and Budgets of the Ministry of Economy and Finance, it agrees:

First.

To approve the Provision developing the technical specification to be fulfilled by the technical gaming systems authorised in Spain and their control mechanisms enclosed as Appendix I to this Resolution.

The technical specifications provided in this provision incompatible with the nature and characteristics of the game participation channel shall not be applicable to gaming activities carried out through text messaging, through land line or mobile phone services or through audiovisual communication means.

Second.

The references in this Provision approving this Resolution made to the National Game Commission shall be understood to be made to the Directorate General for Gaming Regulation of the Ministry of Economy and Finance or to the managerial centre to which its powers are attributed until the effective constitution of said regulating Body. References to the President of the National Game Commission shall be understood as made to the Director General for Gaming Regulation.

Third.

This Resolution shall come into force on the day after its publication in the «Official State Gazette».

Madrid, 16th November 2011. -The Director General for Gaming Regulation, Inmaculada Vela Sastre.

cve: BOE-A-2011-18055

APPENDIX I

Provision developing the technical specifications to be complied with by technical gaming systems object of the licences granted under Act 13/2011, of 27th May, of gaming regulation

Table of contents

cve: BOE-A-2011-18055

1. General provisions

1.1 Object.

The purpose of this Provision is to develop the technical specifications that must be complied with by technical gaming systems of operators with a licence granted under Act 13/2011, of 27th May, of gaming regulation and the control mechanisms therefor.

The operators' technical infrastructure shall ensure the supervision by the Spanish National Game Commission (*Comisión Nacional del Juego*; hereinafter, NGC) of the gaming operations carried out, the obtention of records generated during the development of such operations, and the generation and placing at the NGC's disposal of any other information considered relevant.

In this respects, the specifications are established for the storage of gaming operations records and their traceability, in the format and in accordance with the procedure established by the NGC and the general requirements used for the game are detailed for both logical and physical security of Information Systems, and of system management and control thereof.

1.2 Definitions.

For the purposes of this Provision, the terms used therein shall have the meaning established in this section.

1. Technical Gaming System: The Technical Gaming System is the set of equipment, systems, terminals, instruments and software material used by the operator for the organisation, exploitation and development of the gaming activity. The Technical Gaming System supports all the necessary operations for the organisation, exploitation and development of the gaming activity, as well as the detection and registration of the corresponding transactions between the players and the operator.

The basic elements of the Technical Gaming System are the Central Game Unit and the internal control system. The Technical Gaming System shall provide the necessary information for its control in Spanish. In case it is not available in Spanish, the National Game Commission may require a translation, permanently or punctually.

2. Central Game Unit: The Central Game Unit is the set of technical components necessary for the processing and management of the operations carried out by participants in the games.

It is composed of the Game Platform and the Game Software.

3. Game Platform: The Game Platform is the software and hardware infrastructure making up the main interface between the player and the game operator. It offers the player the necessary tools in order to open and close his or her account, record and edit the information in his or her profile, deposit or withdraw funds from his or her gaming account, view details or a summary of the movements in his or her account.

cve: BOE-A-2011-18055

The Game Platform includes any website showing relevant information to players on the games offered by the operator, and also any client software which players must download in order to interact with the platform.

The game platform allows the operator to manage the players' gaming accounts, and also financial gaming transactions, inform on games results, enable or disable players' accounts, and establish all parameters that may be set up.

The Game Platform consists of the following components:

• Databases, which collect personal data from participants in the games, those related to all the transactions carried out by participants, and information on results of sports events, odds, etc.

• Payment transfer methods, which make it possible to carry out financial transactions between participants and game operators, containing the necessary software for the transfer of funds from the means of payment used by the participant to the operator, and from the operator to the participant.

The Game Platform should comply with the technical requirements established in this Provision.

4. Game Software: The game software represents each of the software modules or components which allow to manage each of the games, authorise and implement the rules of each game and which can be accessed from the Game Platform.

5. Random number generator: The random number generator, also known as RNG, is the software or hardware component which, by procedures ensuring randomness, generates the numerical results used by the operator to determine the results of each of the games in which it is used.

Through a process called "scaling", the raw result obtained by the random number generator shall be converted within the range of values admitted by each game (52 card values, n bingo numbers). These numbers, through a translation or mapping process, are converted into the symbols used by the games (cards, balls, etc.).

6. Internal Control System: The Internal Control System or ICS is the set of components meant to register all the operations and transactions performed during the development of games seeking to ensure that the National Game Commission has the possibility to keep permanent control over the operator's gaming activities.

The Internal Control System will be formed by the Capture Device and the secure database or gaming operation store.

7. Capture Device: The Capture Device is the component of the operator's Internal Control System whose function is to capture and record monitoring and control data established by the NGC, their translation and storage in the device called gaming operation store.

8. The secure database or gaming operation store: The secure database or gaming operation store (hereinafter, store) is the device located in Spain containing all the monitoring and control data introduced by the Capture Device to which the NGC shall be provided permanent access. The information extracted from the gaming system by the Capture Device shall be stored, in the format and structure established by the NGC.

9. User registration: The user registration is the single registration allowing the player to have access to all the gaming activities of a specific operator and which collects, among others, the data enabling the identification of participants and the performance of financial transactions between the player and the game operator.

cve: BOE-A-2011-18055

10. Gaming Account: The gaming account is the account opened by the player, linked to his or her user registration, to debit the payments for financial sums assigned by him or her to the payment of participation in gaming activities and to credit the sums of prizes obtained through participation. The gaming account may never have an outstanding balance.

2. User register, gaming account, means of payment

2.1 User registration and limitation to participation.

2.1.1 Participants' identification.

The identification of participants will take place through a user register which shall contain, at least, the following data:

• Identification data:

o For residents, Fiscal Identification Number (NIF) or Alien's Identification Number (NIE).
o For non-residents, an equivalent document: identity document, social security card, passport, driving licence.
o Name and surname(s).

• Personal data:

o Date of birth.
o Sex.
o Address.
o For non-residents, country of residence.
o Nationality.
o E-mail.
o Telephone.

• Tax residence data:

o Tax residence code, in accordance with the provisions of model 763 for the voluntary payment of the Gaming activities tax, approved in Order EHA/1881/2011, of 5th July.
o For non-residents the player must submit a copy of the document used for identification.

2.1.2 Keeping of a copy of the documents submitted.

The operator shall establish the necessary technical procedures in order to keep an electronic copy of the documents submitted by each player.

2.1.3 Game agreement.

The operator shall keep the record of the game agreement acceptance and any subsequent modifications.

2.1.4 Verification services provided by the National Game Commission.

The National Game Commission shall provide operators with an online identity data verification service (name and date of birth) for players residing in Spain: the verification service is based on the player's NIF/NIE.

The National Game Commission shall provide operators with two online services for the verification of player inscriptions in the General Game Access Interdiction Register (*Registro General de Interdicciones de Acceso al Juego*, hereinafter RGIAJ):

• A service for the verification of the player inscription in the General Game Access Interdiction Register for players residing in Spain based on the NIF/NIE. Operators must use this service to check the inscription in the user registration process.

cve: BOE-A-2011-18055

• A service containing information on modifications (additions/eliminations) in the RGIAJ corresponding to players that the operator has previously checked. Such information service shall be called upon by the operator every hour, in order to check any modification occurred in the RGIAJ corresponding to players in its registers.

2.1.5 Periodic review of user registers.

The operator shall establish the necessary technical procedures enabling the periodic review of user registers in the terms established in article 26.3 of Royal Decree 1613/2011, of 14th November, supplementing the Gaming regulation Act 13/2011, of 27th May, as regards the technical requirements of gaming activities.

2.1.6 Cancellation of the user register.

The operator shall keep the data on cancelled user registers. The register should include the moment of cancellation and the reason.

2.1.7 User register activation and limitation to participation.

The operator shall have a documented procedure for user registration and activation including the identification and limitation to participation requirements established in articles 26 and 27 of Royal Decree 1613/2011, of 14th November, supplementing the Gaming regulation Act 13/2011, of 27th May, as regards the technical requirements of gaming activities.

The operator must have an identity data verification service (name and date of birth) enabling to determine the registration veracity. This service may be provided by third parties providing professional identity verification services.

2.1.8 Suspension for inactivity.

The operator shall keep a register of the user registers suspended for inactivity including the suspension date.

2.1.9 Interim suspension of the user register.

The operator shall keep a register of the user registers suspended for the reasons established in article 33.2 of Royal Decree 1614/2011, of 14th November, supplementing the Gaming regulation Act 13/2011, of 27th May, as regards game licences, authorisations and registers. The register shall include the date and reason for suspension.

2.1.10 Single active user register.

The operator shall establish the necessary procedures and mechanisms to guarantee the requirement of single active user register per player established in article 26.2 of Royal Decree 1613/2011, of 14th November, supplementing the Gaming regulation Act 13/2011, of 27th May, as regards the technical requirements of gaming activities.

2.1.11 Access identification.

Once the registration process has been completed, each player shall be given a single user identifier. Access to the user register and the game account must be exclusively reserved to the players themselves.

cve: BOE-A-2011-18055

2.1.12 User authentication and password policy.

Access to the user register shall include security procedures for user authentication in the platform.

User authentication may be carried out through passwords. The password policy shall include at least the following minimum requirements:

• Either by default or by the player himself or herself, an initial user password must be established.
• During the password definition process, the player shall be informed on good practice for the choice of secure passwords.
• The minimum length of the password shall be 4 alphanumeric characters.
• If the password is created by the user and its length is below 6 characters, from which one shall be a letter and one shall be a digit, the user shall receive a message recommending good practices in the choice of secure passwords. The user will have to reconfirm the password choice.
• The passwords shall not contain any of the following data: the user name, the pseudonym, the name or surname(s) or the date of birth of the player.
• The user shall be sent a message reminding of the possibility to change password at least once a year, although such change shall not be obligatory.
• The identification procedure through user name and password shall be blocked if there are more than 5 failed access attempts within the same day. The operator may set a lower limit concerning this requirement.

The operator may offer other user authentication methods, provided they offer a higher security level than that offered by passwords.

The system shall keep a record of all access attempts, whether successful or not, for subsequent auditing.

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

· The way in which user register is protected from unauthorized access.
· Whether there exists an indirect procedure, or one assisted by operator's staff, to access the user register, requiring a correct answer to questions before access is granted or renewed.
· The procedure in case of loss of user identification or passwords.

2.2 Participants' deposits.

2.2.1 Procedure for the control of deposits account.

The operator obligations as regards the participants' funds are established in article 39 of Royal Decree 1614/2011, of 14th November, supplementing the Gaming regulation Act 13/2011, of 27th May, as regards game licences, authorisations and registers.

2.2.2 Game account. Association to user register.

Each user register shall have one or several associated gaming accounts. Out of the accounts associated to the same user register, at least one of the gaming accounts will allow the deposit and the withdrawal of funds. Fund transfers between the various gaming accounts associated to the same user register shall be instantaneous, and at no cost to the player. Each gaming account shall allow the payment for the participation in one, several or all the games offered in the platform.

2.2.3 History.

The player shall be able to consult in real time the balance of the gaming account and a record of all participations or games occurred at least during the last thirty days.

cve: BOE-A-2011-18055

2.2.4 Units in the gaming account.

In accordance with the provisions of article 35.2 of Royal Decree 1614/2011, of 14th November, supplementing the Gaming regulation Act 13/2011, of 27th May, as regards game licences, authorisations and registers, the currency unit in the gaming account shall be the euro.

The operator may use other units, such as bonus points, or points for the payment of access to tournaments, or others. The platform shall keep a record of the balance and movements expressed in each of the units.

2.2.5 No transfers between players permitted.

The operator shall establish the necessary technical procedures to prevent transfers between gaming accounts associated to different user registers.

2.2.6 Promotional offers.

If the conditions of promotional offers include an amount to be accumulated (e.g. points), the player must be able to see the points he or she has accumulated, or those remaining for the conditions to be complied with.

2.2.7 Accounts associated to user registers in a non-active status.

User registers whose is status is other than “active” shall have partly or totally restricted access to operations in the platform. The operator shall have a documented procedure for technical controls and reviews ensuring that gaming accounts associated to user registers in a non-active status are not allowed to carry out non-permitted operations.

2.2.8 Outstanding balance.

No gaming account may have an outstanding balance. If there is not sufficient balance available in the gaming account, game participation shall be refused and fund withdrawals shall not be permitted.

Without affecting what is established in the preceding paragraph, the operator shall have a documented procedure in order to correct possible errors that may cause from time to time outstanding balances as a result of operator’s errors. Such procedure shall include a record of any such situations, identifying the cause and their correction.

2.3 Means of payment and collection.

2.3.1 Withdrawal of funds.

The operator shall establish a procedure to order the corresponding means of payment the transfer of funds in a maximum period of 24 hours. This procedure must ensure that, in the exceptional case the referred period is not complied with, this shall be notified to the National Game Commission.

2.3.2 Limits to deposits.

The operator shall keep a record of any amendment to the limits to deposits detailed by user register. The register shall include the date and reason for modification.

2.4 Personal data protection.

2.4.1 Data protection.

Operators shall establish the suitable technical procedures for the protection of the privacy of their users’ data, pursuant to Act 15/1999, of December 13th, for the Protection of Personal Data, and any supplementary regulations.

cve: BOE-A-2011-18055

Operators shall also implement on records and procedures the security measures provided by the laws in force regarding data protection, and comply with the duty of secrecy as provided by such laws.

2.4.2 Privacy policy.

The operator shall publish its privacy policy in the game platform.

In order to complete the user registration process, the player must accept the operator's privacy policy. The platform shall keep a record of such acceptance and of the policy contents, or a link to the text of such policy. Any subsequent amendment to the privacy policy shall require notification to users and acceptance by users.

The operator shall have a technical and operation scheme to ensure the protection of the users' data.

3. *Game*

3.1 Basic rules of the game

Operators must implement in their gaming system such procedures as are necessary to comply with the requirements set forth in the basic rules of each game, established in the corresponding Ministerial Order, and particularly the requirements set forth regarding:

- particular rules of the game;
- participants' complaints;
- obligations of information to participants;
- promotion of games;
- channels and means for participation;
- game goal;
- participation in the game and participation limits;
- game development, determination and award of prizes;
- formalization of bets or moves and cases for annulment and postponement;
- payment of prizes.

3.2 Redirection to ".es" domain

The operator shall establish such procedures and mechanisms as are necessary to guarantee that all the connections made from Spain or with a Spanish user registration are directed to a website with a domain name under ".es".

3.3 Return to participant percentage

In such games where it is possible, the operators shall determine the theoretical return to participant percentage. The theoretical return to participant percentages shall be public and accessible to participants, and shall be included, at least, in the particular rules of the game.

In the case of a theoretical return to participant percentage, information must always be provided regarding the minimum or the expected range, as well as an explanation of its meaning for each game or family of games. A participant following an optimal gaming strategy must obtain a return to participant percentage higher than the one of which the participant was informed. The operator must guarantee that he/she also obtains a return to participant percentage higher than or equal to a participant following an average gaming strategy.

The operator must demonstrate the return to participant percentage for each game to the National Game Commission.

The operator shall keep a record of the changes to return to participant percentage for each game for reviewing purposes.

The return to participant percentage cannot be changed during the course of the game, except for such cases where this is provided for in the particular rules and the participant is adequately informed.

3.4 Prize charts

Prize charts, for such games where they exist, shall be public and accessible to participants, and shall include all the possible winning combinations and a description of the corresponding prize for each combination.

The information of the prize program must clearly indicate whether the prizes are quantified in units of account, currency units or any other set unit.

The information of the prize program shall reflect any changes to the prize value that may occur during the course of the game. For these purposes, it shall suffice that the operator has available and

shows a box in a prominent place of the game graphic interface showing said changes to the prize value.

When there are jackpots or prize multipliers shown on the screens, whether the jackpot or multiplier affects the prize program or not must be specified.

The operator shall keep a record of the prize charts for each game so that those changes can be audited.

The prize charts cannot be changed during the game, except for such cases where this is provided for in the particular rules and the participant is adequately informed.

3.5 Random number generator (RNG)

3.5.1 RNG functioning

The Random Number Generator must meet at least the following requirements:

- Randomly generated data must be statistically independent.
- Random data must be uniformly distributed within the set range.
- Random data must remain within the set range.
- Randomly generated data must be unpredictable (their prediction must be computationally impractical without knowing the algorithm and the seed).
- The series of generated data must not be reproducible.
- Different instances of a RNG must not be synchronized between them so that the results of one would allow predicting the results of another.
- Seeding/reseeding techniques must not allow making predictions on the results.
- Generation mechanisms must have successfully passed different statistic tests that demonstrate their random nature.

The technical system may share a RNG or an instance thereof for one or several games if this does not affect the random behavior of the system.

3.5.2 Escalation methods

Escalation methods must meet the requirements set forth for RNGs.

Escalation methods must be linear, must not introduce any bias, pattern or predictability, and must be able to be subjected to recognized statistical tests.

3.5.3 RNG hardware

In the event that RNG hardware is used, it must meet the same requirements adapted to the hardware technical features and, if it exists, it must demonstrate that the staff operating it cannot influence the results. In the event that RNG hardware operated by staff is used, the operator must have a procedure in place to minimize the hypothetical risks that might affect the result generation.

3.5.4 RNG failures

The operator must implement a RNG monitoring system enabling it to detect its failures, as well as mechanisms that disable the game when there is a failure in the RNG.

3.5.5 RNG reseeding

The operator must have a RNG reseeding procedure in place.

3.6 Game logic

3.6.1 Logic independent from the user's terminal

All the functions and logic that are critical to implement the rules of the game and determine the result must be generated by the Central Game Unit independently from the user's terminal.

3.6.2 RNG application to games

The RNG value range must be accurate and must not distort the return to participant percentage.

The method to translate the game symbols or results must not be subject to influence or controlled by any factor other than the numerical values derived from the RNG.

Random events must be exclusively governed by the random number generator and there must

not be any correlation between some moves and others.

The game must not discard any random event, except for such cases where this is contemplated in the rules of the game.

The game must not manipulate random events manually or automatically, not even to keep a minimum return to participant percentage.

When the rules of the game require that a sequence of random events is drawn (for example, the cards from a pack), the random events shall not be re-sequenced during the course of the game, except for such cases where this is contemplated in the rules of the game.

3.6.3 Game logic controls

The game must be designed so as to minimize the risk of manipulation. Technical, organizational and procedural measures to avoid behaviors that mean deviations from the rules of the game shall be adopted.

The operator shall have a documented procedure describing the measures applied to its system to guarantee that:

- The game runs in accordance with the rules of the game.
- The game data are recorded in the system.
- The receipts or attesting documents for a bet or participation are protected against their potential manipulation.
- The system controls the time for trading bets or participation. The moment when trading is closed must be as set forth in the rules governing the game and in any case must be prior to the end of the event that triggers the result of the game.
- The system controls the established prize pool.
- The procedure to determine winners functions adequately and does not allow the introduction of winners that do not qualify as winners or the failure to determine as winners those who do qualify.
- The system shall effectively grant the prizes to the participants appearing in the winner list.

Any modification, alteration or deletion of data must leave audit trails, especially when there is manual intervention.

3.7 User terminals

3.7.1 Terminal identification

The platform must be able to identify the different types and versions of user terminals and a record thereof shall be kept.

If the terminal is installed in physical gaming rooms, casinos or other premises where they are authorized, then the platform must identify the premises. Except for duly justified technical reasons, the platform must record whether a participant is using a specific solution provided for mobile devices.

3.7.2 Component installation in the participant’s equipment

If the use of the gaming system requires the installation of any component in the participant’s equipment, the express consent by the participant must be required prior to such installation.

3.7.3 Disadvantage due to connection quality

The operator is required to introduce in its technical systems all the possible means to try to reduce the risk that certain customers are at a disadvantage against others due to technical factors that may affect the connection speed.

The participant must be informed in such cases where the response time may have a significant impact on the probability of winning.

3.7.4 Information on the connection quality

The system shall inform the participant of the non-availability of communication with the gaming system as soon as it detects it.

The game software must not be affected by the poor functioning of the end participants’ devices, except for the set-up of the procedures planned for ending incomplete rounds or games.

3.7.5 Reduced functionality for certain terminals

Terminals with a graphic interface that is more reduced than others (for example, mobile devices compared to personal computers) may offer some contents that cannot be completely viewed as in other terminals. The platform may offer, for strictly technical reasons arising from the terminal characteristics, different functionalities for the different types of terminals.

Participants must be informed of the limitations of information or functionality of the terminal and client application that they are using, and must expressly accept it.

The operator shall mitigate the risks arising from lack of information or functionality in any given terminal by offering the same information through other means.

Except for duly justified technical constraints, all the information items that must appear in the interface must also appear in a terminal's interface. Whenever it is not possible to include all the information items or links in the game interface, they shall be offered from a link, from a menu or from another application of the same terminal.

3.7.6 Minimum terminal resources

The platform shall not process the games of the terminal if it does not have all the minimum resources to allow playing without technical problems and without disadvantages.

3.8 Game session

3.8.1 Disconnection due to inactivity

The time for disconnection due to the user's inactivity shall be a maximum of 20 minutes; once this time has lapsed, the platform must disconnect the user.

When the operator makes communications of a basically unidirectional nature where the expected user's behavior is passive, for example in a live sports event broadcast, it may be understood that the user is still active although he/she does not perform any action.

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

3.8.2 Record of game sessions

The platform shall keep a record of user sessions detailing the times for logging in and out, the authentication mechanism used by the user and the reason for disconnection or inactivity.

If the terminal belongs to the user, the platform shall allow to identify, if it is technically possible, the type of device (computer, smartphone or others), the used application/version (browser or particular application), and the IP address, if any.

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

3.9 Graphic interface

3.9.1 Game data

The name of the game that the participant is playing must be clearly visible on all the associated screens.

The game instructions must be easily accessible. The graphic interface must include all the information necessary for the game development. The functions of all the action buttons represented on the screen must be clear.

The result of each move must be shown, if it is technically possible, instantly to the participant and must be kept for a reasonable time span.

3.9.2 Participant's data

The screen must show the current balance of the participant at least in Euros and the bets made, both single and total bets.

3.9.3 Prizes

The interface must clearly indicate whether the prizes are shown in Euros or in credits. Different representations that may confuse the participant must not be alternated.

If there are random prizes associated to a move or a bet, then participants must know the maximum amount obtainable from the bet or move that they are going to make.

The participant must be informed when the amount for the random prize is determined based on the amount for the move or bet. When the text or the graphic elements advertise a maximum prize, such prize must be obtainable by means of a single game.

3.9.4 Card games

Card games must comply with the following:

- The card faces must clearly show their value.
- The card faces must clearly show their suit.
- Jokers or wildcards must be distinguishable from the other cards.
- The use of more than one deck in the game must be clearly shown.
- If the cards are shuffled during the game, its frequency must be clearly indicated and the moment when it is done must be shown.

3.9.5 Simulation of elements from real life

Games simulating elements from real life (roulettes, drums or others) must behave in a manner as similar as possible to the behavior of such physical elements. The probability that any event in the simulation takes place and affects the game result must be equivalent to that of the physical device in real life.

3.9.6 Third parties' graphic interface

A third party's graphic interface means an interface not offered by the operator as part of its platform or when the operator includes a link to download it and next to the link it is clearly specified that the operator is not liable for it.

The operator must inform participants deciding to use a third party's user interface that the functionality and information that they will receive may not be complete.

3.10 Integration into game networks with other operators

The operator must guarantee that any integration with another operator's systems is made so that the specifications contained in this Regulation are complied with.

3.11 Deactivation of a game or a game session

The platform must allow that in exceptional circumstances a whole game or specific users' sessions are deactivated, keeping a record of any actions and the reasons originating them for a subsequent review.

3.12 Incomplete game

An incomplete game means a game whose result has not yet occurred or, if it has occurred, the participant has not been informed of this fact.

In the face of an incomplete game the particular rules of the game shall determine the action by the platform, which may wait for the participant, annul the game or proceed with the game until it is completed.

- If the incomplete game is due to a connection loss by the user's terminal, then the platform shall show the incomplete game when the participant is connected again.
- The operator must have a documented procedure for managing the unavailability events of one, several or all the components, including the associated technical measures. The components must carry out a self-diagnosis, a check of the critical files and a check of the communications between the different components.
- After recovering, the technical gaming system must treat the ongoing games affected by the interruption.

The technical system shall keep a record of the service interruptions, with their start, duration and affected services for a subsequent review.

3.13 Automatic game

If the system offers advice on game strategies or automatic game functionalities, then such recommendations or functionalities must be truthful and ensure that the compulsory return percentage is achieved.

It must be guaranteed that the participant maintains the game control when the automatic game function is provided. The participant shall be able to control the maximum amount for the automatic game or the maximum bet and the number of automatic bets. The participant shall be able to

deactivate the automatic game function at any time.

When the automatic game function is being used, the information items shown on the screen (duration, graphic elements or others) shall be the same and shall have the same characteristics as when the game is not automatic. The interface shall additionally show the number of occurred or remaining automatic moves.

The automatic reproduction function cannot put a participant at a disadvantage, and the sequence of automatic rounds and any strategy recommended to the participant must not be misleading.

In the case of games where more than one participant take part simultaneously, all the participants must be informed and accept a participant that has set the automatic game function.

3.14 Replay

The platform must provide the participant with a “replay” option showing it as a graphic reconstruction or an intelligible description, which must reproduce every game incident that may have an impact on its development. The replay option must provide all the information necessary to reconstruct the last ten rounds in the ongoing session.

3.15 Virtual players

3.15.1 Virtual players provided by the operator

The operator may use artificial intelligence through virtual players, also called robots, if specifically allowed by the corresponding game rules.

In the case of games where more than one participant take part simultaneously, all the participants must be informed of and accept the presence of a virtual player.

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

The virtual player must not have any technical advantage over the participants and may not have access to any information that is not available to them.

3.15.2 Virtual players used by participants

The operator may provide participants with artificial intelligence through the use of virtual players or robots if so allowed by the corresponding game rules.

The operator shall inform whether or not it allows the use of virtual players or robots by participants. In the event that it allows them and more than one participant take part simultaneously, the operator must ensure that the rest of the participants know who is a virtual player or robot. In the event that it does not allow them and more than one participant take part simultaneously, the operator must try to avoid that participants use virtual players and, as soon as it detects its use, it must inform the participants of this. Participants must have a mechanism to report the existence of a potential virtual player.

The operator shall have a procedure in place to detect if a participant is using artificial intelligence techniques.

3.16 Metamorphic games

Metamorphic or evolution games must:

- Inform of the applicable rules for each moment or stage of the game.
- Show the participant sufficient information to indicate the nearness of the next metamorphosis. For example, if the participant is collecting items, the interface must show the number of items that the participant has collected, those necessary for the metamorphosis or those remaining to achieve it.
- The probability of a metamorphosis must not be varied depending on the prizes obtained by the participant in previous rounds. Any exception to this must be previously authorized by the National Game Commission.
- The information and the game must not be misleading or ambiguous.

3.17 Participant in “away” status

During a game where more than one participant take part simultaneously the platform must allow a user to set an “away” or “pause” status that can be used if the participant needs to stop playing for a brief period of time that may not be over twenty minutes. During the “away” status the participant does not make new moves. If he/she makes any move, his/her status stops automatically being “away”. If the actions do not affect the game (e.g. consulting help), the “away” status shall be maintained.

3.18 Multi-participant games with host

In games where a participant is the host, the host can decide whether he/she accepts any participant or only through invitation. The host may not exclude participants from the table once they have been previously accepted thereat.

3.19 “Live” game

There must exist action procedures to solve any events that may occur during the live game operations.

The automatic recognition and registration devices used must be equipped with a manual functioning mode enabling to correct an erroneous result. The participant must be informed that the manual mode is active. Every time that the manual functioning mode is activated, a trail enabling its subsequent review must be left.

There must exist procedures to treat interruptions in the game caused by the discontinuity in the flow of data, video and voice.

3.20 Jackpots, progressive jackpots and additional prizes

Provided that the basic rules of the corresponding games allow it, the operator may create jackpots, rollover jackpots, progressive jackpots or additional prizes.

The platform shall clearly inform the participant when he/she is contributing funds to the jackpot and the manner in which a participant may go for such jackpots. All participants contributing to the jackpot must have chances to win it throughout the development of the game. The description of the jackpot conditions and the requirements to win it must be communicated to the participant.

Jackpot conditions must consider any conclusion or interruption, expected or not, of the game, as well as technical interruptions in the system.

The operator must have a procedure in place to allow for jackpot control and guarantee that:

- The jackpot is created, managed and awarded in accordance with the rules of the game.
- Once the jackpot is formed and opened, jackpot conditions are not modified until the jackpot has been won by one or more participants and its sum has been cashed.
- The procedure to determine winners functions adequately. The procedure does not allow the introduction of winners that do not qualify as winners or the failure to determine as winners those who do qualify.
- The system grants the prizes to the participants appearing in the winner list.
- If they exist, special attention must be paid to the jackpot redirection systems where part of the rollover jackpot is redirected to another pot to be won subsequently. The jackpot redirecting system may not be used to indefinitely postpone the award of a prize.

Procedures involved in the determination of winners must leave trails that allow for a subsequent review of the entire decision-making process.

The amount of the jackpot must appear updated in all the terminals of the participants taking part in it.

The jackpot non-operation capacity must be clearly indicated to the participants by displaying messages such as “Closed Jackpot” or similar ones in their terminals. It shall not be possible to win a rollover jackpot which had been previously closed.

4. Security of the information systems

The established security requirements for the technical gaming system are aimed at protecting the users' registers and their associated gaming accounts, as well as guaranteeing that the game is correctly developed.

4.1 Critical components

Critical components are elements whose security must be reinforced because their impact on the game development is important.

Critical components are:

- in the user registration, game account and payment methods processing: the components from the technical gaming system that store, manipulate or transfer sensitive information from customers, such as personal data, authentication or economic details, and those components that store the specific estate of the games, bets and their results;
- in the random number generator: components from the technical gaming system that transfer or process random numbers that shall be the object of the result of the games and the integration of the results of the random number generator into the logic of the game;
- the connections with the National Game Commission;

- the internal control system: the capture device and the store;
- access points and communications from and to the critical components above;
- communication networks transferring sensitive information from participants.

4.2 Technical gaming system security management

The operator must implement a security management system protecting especially the critical components listed under the previous heading.

Security procedures must be aimed at implementing specific security measures based on a risk evaluation. The operator must plan periodic reviews and carry out the reviews arising from significant changes.

4.3 Risk management

The risk management shall identify the elements to be protected, to subsequently perform a periodic identification, quantification and prioritization of the risks to which the technical gaming system is subject. The risk management must be stated in a plan of measures.

4.4 Security policy

Operators must have a security procedure, which shall be communicated to all their members of staff and external collaborating institutions, if any.

4.5 Information security organization

Operators must establish a management framework for the information security stating the duties and responsibilities of their members of staff.

4.6 Security in communications with participants

Authentication mechanisms allowing the gaming system to identify the participant must be adopted and, in turn, these shall allow the participant to identify the gaming system.

Communications must be encoded in the case of transfer of personal (user's registration) or economic (game account) data.

Regarding communications, the operator shall adopt such measures as are necessary to guarantee the integrity and the non-repudiation in the cases of personal or economic data transfer and in game participation transactions.

4.7 Human resources and third parties' safety

The operator's plan for staff safety shall include training actions, contracting management, changes and termination of contracts, paying special attention to information access permits and critical components.

Should the operator need the services of third parties which may mean information access, processing, communication or treatment, or access to game-related facilities, products or services, then such third parties must comply with all the safety requirements required to the rest of the staff.

4.8 Physical and environmental safety

Operators' safety plans must include, regarding the physical safety of the components of the technical gaming system and their replica, the following:

- Perimeter safety for the areas containing critical components and sensitive information: walls, access cards, etc.
- Physical access control to the facilities where the equipments are placed, both for employees and external staff, and including physical elements, authorization procedures, access records and surveillance services.
- Protection of critical equipment against environmental risks: water, fire, caused by persons, etc.
- Protection of critical equipment against electric supply cut-offs and other interruptions caused by failures in support facilities. The electric supply cabling must be protected against damage.
- Control of access to communication cabling if it transports not encrypted critical information.
- Maintenance of facilities and equipments.
- Devices containing information must be safely deleted or destroyed prior to being reused or retired.
- Equipments containing information must not be moved out of the safe facilities without the corresponding authorization.

4.9 Communication and operation management

The secure and correct operation of the technical gaming system must be guaranteed, as well as communications:

- Critical components must be monitored to avoid the use of versions other than the approved.
- Communication between the components of the technical gaming systems shall guarantee integrity and confidentiality.
- Tasks must be segregated among the different responsibility areas in order to minimize the chances of unauthorized access and potential damage.
- The tasks of development, tests and production shall be separated.
- Services provided by third parties must include security controls and metrics in the contracts, and must be periodically audited and monitored.
- Protection measures against malicious code shall be taken.
- Regular back-up copies must be done with the appropriate frequencies and must be kept according to what the back-up copies plan provides.
- Safety measures for the communication network must be taken.
- Safety measures for manipulating portable media must be taken, as well as for safely deleting or destroying them, and they must be stated in a documented procedure.
- The clocks of all the components, especially critical components, shall be synchronized with a reliable time source. The reliable time source cannot be the same for every component. The operator shall establish measures and controls so as to avoid the manipulation of time marks or their subsequent alteration, especially in audit records.
- An audit record of the activities of all users, exceptions and security events of information must be created and stored for at least 2 years.
  - Audit records shall be protected against alterations and improper access.
  - Activities done by the System Administrator and the System operator must be recorded.
  - A periodical analysis of the audit records shall be performed. Actions shall be taken in accordance with the incidents detected.

4.10 Access control

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

- There must be a documented information access policy in place, which shall be periodically reviewed.
- Authorized access must be guaranteed and unauthorized access must be prevented through controls upon user registration, management of access privileges, periodic revision of access privileges and password management policy.
- Users must follow good practice in the use of passwords and must appropriately protect the documentation and supports in their place of work.
- Users shall only have access to the services that they are authorized to use.
- There shall be no generic users and all users shall access with their exclusive user name.
- The system must authenticate all access, either by the staff, by maintenance workers or others, or from other systems and components (for instance, the payment gateway). The National Game Commission inspection staff or any other staff acting in their name must also be authenticated.
- Networks shall be segregated depending on the area and responsibility of the task or duty.
- Access to operating systems shall require a secure authentication mechanism.
- Sessions shall have a maximum connection time and a disconnection time due to inactivity.
- Computing support staff shall have restricted access to the actual data of the applications. Sensitive actual data shall be located in isolated environments.
- Risks related to mobile devices shall be managed.
- Where telecommuting exists, it shall be checked that the associated risk is managed in the framework of the security plan.

4.11 Purchase, development and maintenance of systems

Impact on security must be analyzed when making decisions regarding the purchase, development and maintenance of computing systems.

4.12 Management of security incidents

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

All security incidents must be recorded, clearly and precisely documenting the facts, impacts and measures taken.

4.13 Change management

Under the provisions of section 8.5 of Royal Decree 1613/2011 of November 14, implementing Act 13/2011 of May 27, regulating gaming regarding technical requirements for gaming activities. Approval and certification reports shall include a list of the critical components. The implementation of any substantial modification that affects a critical component shall require the prior authorization from the National Game Commission after the corresponding report for its approval has been submitted. The National Game Commission may classify other additional components as critical.
The operator must have a documented change management procedure in place to control changes in equipments and components of the technical gaming system in the production environment.
The operator shall follow a formal process for internal approval of all changes, which must include the change request and its approval by the corresponding managers. Change requests and the decisions taken shall be recorded and may be subject to a later audit.
Substantial changes to critical components must be previously authorized by the National Game Commission. The change requests must be accompanied by the corresponding application for the approval of the new components. In the face of extraordinary emergency situations, duly evidenced and communicated to the National Game Commission, that affect security, the operator may introduce substantial changes in critical components and may request the authorization subsequently. In order to obtain approval the operator shall submit at the National Game Commission, together with the certification report, a report evidencing the exceptional circumstances.

4.14 Service availability management

The operator must have a service availability management plan in place.
The operator shall consider in the plan each of the following services:

- participant registration, gaming accounts, including the possibility to make deposits and withdraw funds;
- game services.

The plan shall indicate the maximum accumulated unavailability time per month, as well as the maximum recovery time for each service. The operator shall adapt its infrastructure and process, and shall implement such measures as are necessary to meet the goals set in its availability management plan.

4.15 Information loss prevention plan

The operator must have a plan in place guaranteeing that no data or transactions are lost that may or might affect the development of the games, participants' rights or the public interest, and indicating the risk borne by the operator.
The operator shall adapt its infrastructure and process, and shall implement such measures as are necessary to meet the goals set in its plan, the following minimums being set:

- Copies of the information shall be kept in a place conveniently far away from the data intended to be safeguarded.
- The copy of the information shall be protected from unauthorized access with security measures that are equivalent to those for the information to be safeguarded.

The operator must have a documented procedure of action in case of loss of information, which shall include mechanisms to answer users' complaints, continue with the interrupted games or bets and any other situations that may result.

In the event of data loss, the operator shall immediately inform the National Game Commission, stating the actions taken and an estimate of the impact of the loss.

4.16 Business continuity management

The operator shall have a business continuity management plan in place to maintain the game operations in case of disaster, including such technical, human and organizational measures as are necessary to guarantee the continuity of the service and a replica of the Central Game Unit allowing the normal development of the activity.

The business continuity plan shall determine one or several recovery scenarios, stating the recovered services for each of them and the maximum time in which they would be in operation. The operator shall consider within the plan the following scenarios:

- Participants' access to their user registers and gaming accounts with the possibility to consult the balance and movements of their associated gaming accounts. The maximum amount of time to provide again these services shall be one week.
- Participants' possibility to withdraw their funds. The maximum amount of time to provide again these services shall be one week.
- Continuation of uncompleted games or pending bets, and payment of prizes validly obtained. The maximum amount of time to provide again these services shall be one month.
- Complete re-establishment of all services.

The operator shall adapt its infrastructure and process, and shall implement such measures as are necessary to make feasible the goals set in its business continuity plan.

In the event of disaster, the operator must immediately inform the National Game Commission, making an estimate of the impact and the estimated recovery time.

4.17 Penetration test and vulnerability analysis

The gaming system must pass a penetration test and a vulnerability analysis at least with a bi-annual periodicity. The penetration test shall consist of an evaluation method for the security of a network or system by simulating an attack made by a third party. The process includes an active analysis of the system searching weaknesses, technical failures or vulnerabilities. The test shall include all the public interfaces safekeeping, processing or transferring personal, economic or gaming data.

The vulnerability analysis shall consist of the identification and the passive quantification of the potential risks of the system. The analysis shall include all the public interfaces safekeeping, processing or transferring personal, economic or gaming data.

The results of the tests and analyses must be kept together with the corrective measures taken or planned for a later review or inspection.

5. Internal Control and Inspection System

5.1 Internal Control System.

5.1.1 Description.

The monitorization and supervision of the gaming activities run by the operator shall take place by means of the internal control system (hereinafter, ICS), which must be implemented by operators. The ICS shall include all participants located in Spain or with a Spanish user registry, whichever the means of participation. The operator shall establish and maintain a safe communications line for access by the National Game Commission, and a data consultation and download service that is permanently available to the National Game Commission.

The ICS consists of the capture device and the game operations store (CAJA).

5.1.2 Access to the CAJA by the National Game Commission.

The CAJA shall maintain the following accesses permanently open for access by the National Game Commission:

- Access through SFTP protocol for information download.
- Access through SSH with read-only attributes and sufficient permits to list and view the contents of the entire CAJA.

The operator shall provide the following authentication methods to the National Game Commission:

- For manual access, user and password.

For automated download, the operator shall configure SSH keyswap for the same user described in manual access.

The operator may use several CAJAs. The data must be reported just once, in order to prevent several CAJAs from containing redundant information.

5.1.3 ICS Data model.

The ICS Data Model contains the scope of the data that shall be registered, the period of updating of such data and the technical requirements for availability and access, as provided in Article 24 of Royal Decree 1613/2011 of November 14, supplementing Law 13/2011, of May 27, of gaming regulation, regarding the technical requirements for gaming activities.

The data shall be stored in a file structure, in an XML-structured format, following the definition of the monitorization data schema (XSD-XML Schema Definition).

5.1.4 ICS Time Source.

All the Technical Gaming System elements, including the capture device and the CAJA, shall be synchronized with a single, reliable time source.

5.1.5 ICS Data Signature, compression, encryption and time stamping.

The data to be stored in the CAJA shall be grouped into batches. Each batch shall be signed, compressed and encrypted by the operator, using the format and procedure described in the Monitoring Data Model.

The operator shall provide the NGC with the public part of the digital certificate used to sign the batches. The operator shall inform the National Game Commission if the certificate used is revoked. The operator may use its own certificate, or order a third party to sign the batches in its name.

5.1.6 Performance of the CAJA and the capture device.

The capture device shall have enough capacity to process and register the information on the transactions.

Unless exceptional circumstances occur, for which due justification must exist, the capture device shall be designed for information to be processed, formatted and registered in the CAJA in a maximum of twice the defined time for real time in the Monitoring Data Model.

The CAJA shall have enough communication capacity or flow on the Internet for the National Game Commission to be able to access to it:

- For data download, the minimum guaranteed flow shall allow the maximum download of information created in four hours in one day, through the defined SFTP protocol.
- For data upload, a minimum of 64 kbps are required.

The performance of the CAJA as a system shall be equal to or higher than that necessary in order to guarantee the aforementioned communication flows, regardless of other operations it may have to perform.

5.1.7 ICS Security.

The ICS as a whole, both the capture device and the Gaming Operations Store, are considered critical components. The security requirements listed in section 4 are applicable to the ICS.

Although the data model requires that the information should be ultimately stored in the CAJA in an encrypted mode, it is not required that it should be encrypted at all times. The chain of custody of the encrypting code must be included in the ICS security design.

The capture device shall be able to register transactions at all times and in a permanent way. The operator shall design the availability, the back-up copy plan, the disaster recovery time and the business continuity, all in accordance with this requirement.

5.1.8 Non-availability of the ICS and suspension of the game offer.

The operator shall suspend the game offer in cases where the internal control system is not available. Capture device CAJA capture device. Where the non-availability of the CAJA is shorter than 24 hours, the operator may continue its game offer if the capture device is still available, provided it is able to continue registering transactions until the CAJA becomes available again. The operator shall suspend the game offer in those cases where the CAJA is not available for a period longer than 24 hours.

5.1.9 ICS Availability.

The capture device shall be able to register transactions at all times and in a permanent way. The CAJA may not have more than 48 hours of accumulated failure time per month.

5.1.10 ICS Back-up Copy Plan.

The ICS is a critical component. Gaming operators shall implement a procedure minimizing the risk of loss of information up to a maximum of 24 hours.

In case of loss of information in the ICS, the operator shall have a planned procedure in order to extract the lost information, which makes it possible to repair the loss within a maximum period of one week.

Any loss of information affecting the ICS shall be reported to the National Game Commission immediately, with an assessment of the loss and the measures to be adopted.

The operator shall have a documented procedure in order to control the quality of the data in the ICS, and shall be prepared in order to replace incorrect data, through new extractions, within the maximum period of one week.

5.1.11 ICS Business Continuity.

Given that non-availability of the ICS entails the suspension of the game offer, the operator shall have a business continuity procedure, which in the event of disaster makes it possible to keep the ICS operative for a period of less than one month.

Any disaster affecting the ICS must be reported to the National Game Commission immediately, with an assessment of the loss and the measures plan to be adopted.

5.1.12 Preservation of the ICS information.

The data in the CAJA shall be preserved for a minimum period of six years.

Gaming operators shall give and allow the National Game Commission online access to the last 12 months of activity registered in the CAJA.

Operators shall have a planned procedure for the recovery of the information corresponding to a minimum period of six years.

5.1.13 Location of the CAJA in Spain.

The ICS CAJA or CAJAs shall be located in Spain, so that the operations of verification and control of information may be carried out. The location, and any modification thereof, shall be reported to the National Game Commission.

5.2 Physical and online supervision.

The National Game Commission shall have the possibility to monitor and supervise any of the elements of the operators' technical gaming platforms.

For such purpose, the operator shall implement the mechanisms needed for secure communication with its technical systems, and shall also facilitate at all time access to such systems, regardless of their location, to the National Game Commission.

The National Game Commission shall inform the operator of its desire to connect itself to the technical gaming system, providing a description of the functions it desires to access and the estimated time and duration of such access.

The operator shall provide the National Game Commission with the means to safely access the system. The staff designated by the operator shall cooperate with the National Game Commission for the adequate access to, and consultation of, other systems and applications. The National Game Commission may make session recordings, and collect any evidence required in order to carry out its functions.

Unless otherwise required, it shall be understood that the access provided to the National Game Commission is a read-only access, and the authorization level is only that required in order to access all systems and applications of the technical gaming system, with no filter in the data it may have access to.

Once the access ends, the operator shall close the secure access.

6. Registries and logs of the Technical Gaming System

6.1 Registration and traceability.

The operator shall keep registries and logs of all decisions by participants, by the operator

itself, its staff or its systems, which have a consequence upon the development of the game, the user register, the gaming accounts or the means of payment.

Regarding the data on the development of the games, the data shall be enough to reconstruct all the events of the game which might have an influence upon its development. The Technical Gaming System must also keep registries and logs regarding the safety of information systems. All said registries and logs shall be accessible on-line to the National Game Commission for a minimum period of 12 months. This notwithstanding, registries and logs must be stored for at least 6 years.

Operators shall have a planned procedure for the recovery of this information.

6.2 Registration according to the communication channel.

Certain participation procedures and terminals have specific registration requirements for gaming operations. These requirements shall not affect other communications between the operator and the participant other than those proper to the development of the game itself.

These specific procedures and terminals shall apply to the registration of messages sent and received for gaming activities by means of text messaging, through land or mobile telephone services, or through audiovisual media.