

Decision No. 79841/ΕΞ2020/20 (Government Gazette 3266/Β/05-08-2020): Enactment of the Technical Specifications (TS) Regulation on Organising and Conducting Online Gaming Services/Games of Chance.

THE MINISTER OF FINANCE

Having regard to:

The provisions of:

- a) Articles 25 to 54 of Law 4002/2011 on Amending the state pension legislation - Reforms for development and financial consolidation - Issues within the remit of the Ministries of Finance, Culture & Tourism and Labour & Social Security (Government Gazette 180/A), and in particular the provisions of Article 29(3) as well as those of Articles 189 to 203 of Law 4635/2019 on Investing in Greece and other provisions (Government Gazette 167/A);
- b) Law 4624/2019 on the Hellenic Data Protection Authority, measures for implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, and transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, and other provisions (Government Gazette 137/A);
- c) Articles 13, 18, 19 and 41 of Law 4622/2019 on the Executive State: organisation, operation and transparency of the Government, governmental agencies and central public administration (Government Gazette 133/A);
- d) Law 4557/2018 (Government Gazette 139/A) on the Prevention and suppression of money laundering and terrorist financing (incorporation of Directive 2015/849/EU) and other provisions;
- e) Law 3861/2010 (Government Gazette 112/A) on Improved transparency via the mandatory posting of laws and acts of governmental, administrative and local government bodies on the Internet [the "Diavgeia" (Clarity) Programme] and other provisions; and of Law 3469/2006 (Government Gazette 131/A) on the National Printing House, Government Gazette and other provisions;
- f) Articles 16 to 23 (incl.) of Law 3229/2004 on the Supervision of private insurance, supervision and control of games of chance, application of the International Accounting Standards and other provisions (Government Gazette 38/A) and in supplement the provisions of Law 3051/2002 (Government Gazette 220/A) on Constitutionally established independent authorities, amendment and supplementation of the public sector recruitment system and related regulations;
- g) Articles 58 to 60 of Law 2961/2001 on the Ratification of the Code on taxation of inheritance, gifts inter vivos, parental donations and lottery gains (Government Gazette 266/A);
- h) Presidential Decree No. 83/2019 (Government Gazette 121/A) on the 'Appointment of a Deputy Prime Minister, Ministers, Deputy Ministers and State Secretaries';

- i) Presidential Decree No. 81/2018 on the Transposition of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (consolidated version) (OJ L 241, 17.9.2015, p. 1) and other provisions into Greek law (Government Gazette 151/A);
 - j) Article 34 of the Presidential Decree No. 142/2017 on the 'Organisational structure of the Ministry of Finance' (Government Gazette 181/A);
 - k) Article 90 of the Presidential Decree No. 63/2005 on the 'Codification of laws on Government and government agencies (Government Gazette 98/A) as currently in force;
 - l) the Joint Ministerial Decision No. 70330οικ./30.6.2015 of the Minister of Finance, Infrastructure, Maritime Affairs and Tourism and the Minister of Justice, Transparency and Human Rights, on the adaptation of the Greek legal order in line with Directive 2013/11/EU as in force (Government Gazette 1421/B);
 - m) the Joint Decision No. 56660/1679/22.12.2011 (Government Gazette 2910/B) of the Ministers of Finance and Culture & Tourism confirming the commencement of the Hellenic Gaming Commission (HGC) operations (Government Gazette 2910/B);
 - n) the Decision No. 2/63389/0004/21.07.2016 of the Minister of Finance on the Appointment of the Chair and two members, and the renewal of the term in office of members of the Hellenic Gaming Commission (Government Gazette 397/Special Officials and Management Positions of Public Sector and Wider Public Sector Bodies Issue) read in conjunction with similar decisions No. 2/3935/0004/24.7.2018 (Government Gazette 428/Special Officials and Management Positions of Public Sector and Wider Public Sector Bodies Issue), οικ. 9433 Ministry of Foreign Affairs 2019/12.2.2019 (Government Gazette 64/Special Officials and Management Positions of Public Sector and Wider Public Sector Bodies Issue) and 3557 Ministry of Foreign Affairs 2020/14.1.2020 (Government Gazette 20/Special Officials and Management Positions of Public Sector and Wider Public Sector Bodies Issue);
2. HGC Decision No. 452/2/16.12.2019, Recommendation to the Minister of Finance on the enactment of the Technical Specifications (TS) Regulation on organising and conducting online gaming services pursuant to Article 29(3) of Law 4002/2011 (Government Gazette 180/A);
3. The draft ministerial decision on the enactment of the Technical Specifications (TS) Regulation on organising and conducting online gaming services, which was notified to the Commission on 31.12.2019, pursuant to the provisions of the presidential decree 81/2018 (Government Gazette 151/A), with reference code number 2019/657/GR and end date of the standstill period on 1 April 2020;
4. HGC Decision No. 482/2/24.04.2020, Recommendation to the Minister of Finance on the enactment of the Technical Specifications (TS) Regulation on organising and conducting of gaming services pursuant to Article 29(3) of Law 4002/2011 (Government Gazette 180/A), amending the notified draft referred to in point 3, following evaluation of notes and comments submitted; for the said modifications no new notification to the Commission is required, pursuant to the provisions of the Presidential Decree No. 81/2018 (Government Gazette 151/A);
5. The need to establish the Technical Specifications (TS) Regulation on Organising and Conducting Online Gaming Services;

6. The fact that this decision does not entail any expenditure for the State budget or the HGC budget, we hereby decide to:

1. Enact the Technical Specifications (TS) Regulation on Organising and Conducting Online Gaming Services, as follows:

TECHNICAL SPECIFICATIONS REGULATION ON ORGANISING AND CONDUCTING ONLINE GAMING SERVICES

Chapter 1.

Definitions and Scope

Article 1.

Definitions

For the purpose of this decision, words and phrases herewith shall have the following meaning:

Online Gaming Licence or Licence shall mean the administrative permit issued by the HGC to allow games to be organised/conducted. Licences shall take either of the following two forms: a) Type 1 Licence for Online Betting and b) Type 2 Licence for Other Online Games;

Excluded Player shall mean a Player who cannot take part in Games of Chance on his/her own initiative or at the request of his or her legal guardian submitted to persons who organise and/or run such Games or court decision or reasoned decision of the Licence Holder;

Seed Pool shall mean the amount of wagers gradually collected by withholding part of the Wagers and/or commission of the Licence Holder (Operator) which is used to improve the payout and to organise jackpots;

Classified Access shall mean the level of access the Licence Holder has designated for Users as shown in the relevant document submitted to the HGC;

Classified Users shall mean the users who have Classified Access to the CIS;

Online Bet or Bet pursuant to Article 25(c) of the Law means the Game of Chance played online which requires Players to predict the development in and/or final outcome of all manner of events, including virtual events, whose result is generated using a Random Number Generator;

Running shall mean conducting a game referred to in Article 25(s) of the Law. Where the provisions of this Decision refer to the concept of 'Conducting', they shall also cover the concept of 'Organisation' and vice versa;

Organisation shall mean organising a game referred to in Article 25(t) of the Law. Where the provisions of this Decision refer to 'Organising', it shall also mean 'Conducting' and vice versa;

HGC or Authority shall mean the Hellenic Gaming Commission;

Studio shall mean the premises where the hardware and infrastructure for conducting Other Online Games played with a live dealer, whose outcome is not generated by an RNG, is installed, and which is located within the EU or EEA;

Intermediate Control System shall mean the IT system which ensures the integrity, authenticity and continuous availability of data collected by the Data Capture System, the Data Sealing System and the Safe;

Sensitive data shall mean data which, if obtained by a third party, may be used to affect the game outcome or Player accounts.

Player Online Account shall mean the account referred to in Article 25(o) of the Law;

Website shall mean the website via which the Licence Holder runs Games of Chance, belongs to the Licence Holder and whose domain name must end in .gr.;

Regulation shall mean the Gaming Regulation referred to in Article 29 of the Law on organising and conducting of online gaming services/games of chance;

Suitability shall mean the finding made by the HGC or the Licence Holder concerning the qualifications and conditions for the issuing of a SL and/or Suitability Card pursuant to the provisions of the Gaming (Suitability of Persons) Regulations;

Licence Holder or Holder shall mean the legal person who provides services to organise and conduct Games of Chance who has been granted an Online Games of Chance Licence pursuant to the provisions of this Law and the Regulations. Each Holder may hold both types of Licence;

Central Information System (CIS) shall mean all hardware and software needed for the Licence Holder to organise, operate, conduct, monitor, record, check and centrally manage the Games of Chance;

Client Software shall mean the software uploaded to and/or installed on a Player device.

Other Online Games, pursuant to Article 25(v) of the Law, shall mean casino games of chance, poker and its variants, provided online and played either live or using a Random Number Generator;

Law shall mean Law 4002/2011 (Government Gazette 180/A);

Game Guide or Guide shall mean the info-material posted by the Licence Holder on its website in Greek which includes, for each Game or group of Games, all information needed for Players to Participate, the terms, conditions and rules for Playing the Games, and the odds/winnings pay table, if applicable;

Instructions shall mean circulars issued by the HGC with instructions on how to implement the provisions of the Gaming Regulations. These instructions are binding in the Authority's dealings with citizens;

Certification Body shall mean the certification body which operates a specialised Test Lab and has been recognised by the HGC in accordance with the Gaming (Suitability of Persons) Regulations, or a certification body accredited in accordance with the applicable European and/or international standards, by a company running a national accreditation system or by accreditation bodies in other countries, with which the company running the national accreditation system has signed a mutual recognition agreement;

Multi-stage Game shall mean a game with one or more intermediate steps that require the Player input in order to proceed. Poker and Blackjack are two typical examples of multi-stage games.

Player shall mean the natural person who legitimately participates in Games of Chance organised and conducted by the Licence Holder;

Player Activity shall mean all transactions and other information held in the Holder's IT System about each individual Player which is linked to the Player Online Account held by the Licence Holder;

Player Session shall mean the time period from the moment the Player logs into his/her Online Account to the moment he/she logs out of it;

Period shall mean the minimum number of values required so that there exists a sequence of values that will be forever repeated. For example, if a RNG were to produce the following sequence of values ad infinitum (1,3,1,3,1,3 ...), the period of that sequence of values would be considered to be 2, since every time a 1 is produced, it is succeeded by a 3, which is succeeded by a 1, and so on and so forth;

Certification shall mean the approval granted by the HGC to install and start using Technical Means and Materials after the Certification Body has ensured its compliance with the Technical Specifications or has certified that it corresponds to equivalent technical and functional characteristics of the Technical Means and Materials with the same specifications;

Gaming Platform shall mean all hardware and software which drives the feature common to all games offered. It is accessible both to the Player and the Licence Holder (Operator) and is part of the CIS;

The Gaming Platform provides the Player with the means to participate in the Game. In addition to playing the Game, the Gaming platform also offers the Player functions such as: setting up and managing a Player Account, depositing and withdrawing funds from it, setting up and managing limits and self-exclusions, managing reporting requests, managing promotional measures and loyalty programmes, etc.

The Gaming Platform provides the Licence Holder (Operator) with the means needed to manage and adjust Game settings.

In addition to managing the Game, the Gaming Platform also offers the Licence Holder functions such as: managing Player Accounts, generating gaming reports and financial transaction reports, inputting and managing betting events and the results/outcomes of such, etc.

Supervision and Control IT System (SCITS) shall mean the IT system referred to in Article 30 of the Law.

Increment Rate shall mean the portion of the Progressive Jackpot contributions which are incrementing the Progressive Jackpot (compared to funding the startup value).

Percentage Return to Player (%RTP) is the expected rate of wagers that a specific game will return to the Player in the long run. The %RTP can be calculated either through a theoretical or simulated approach. The method used for calculation depends on the game type.

Progressive jackpot shall mean an increasing prize based on a function of all credits wagered or won. This includes prizes awarded based on criteria other than obtaining winning outcomes in the game, such as 'Mystery Jackpots'. However, this does not include non-configurable, increasing prizes resulting from bonus features, which are part of the game payable (theoretical %RTP);

Protocol shall mean all rules agreed by both communicating parties to promote the exchange of information between them;

Participation shall mean entering a Player's particulars/options in any Games of Chance and confirming that entry after paying the wager;

Contributions shall mean the financial method by which progressive jackpot pools are funded.

Player Device shall mean the device that converts communications from the Gaming Platform into a human interpretable form, and converts human decisions into a form of communication understood by the Gaming Platform. Examples of Player devices include personal computers, mobile phones, tablets, etc.

Player System shall mean the system comprising the Player Device, Client Software and all other items comprising the entire piece which communicates to the Gaming Platform. This includes personal computer cache, cookies, etc.

Artwork shall mean any graphical and auditory information which is sent to the Player device for presentation to the player.

Technical Means and Materials shall mean the certified (where necessary) medium/hardware/electronic/mechanical or electromechanical equipment and computer program (all manner of software or computer system) used directly or indirectly to organise and conduct games;

Games of Chance or Games shall mean the Online Bet referred to in Article 25(c) of the Law and Other Online Games referred to in Article 25(v) of the Law which may be organised and conducted legally in the territory of Greece by the Licence Holder via its website and which have received the required Certifications.

Responsible Gambling shall mean all provisions of the Gaming Regulations and HGC Instructions that aim to ensure that all activities in the field of games of chance are performed pursuant to the provisions in force, in a socially responsible manner, in order to minimise consequences for the Players due to their participation in games of chance.

Mapping shall mean the process by which a scaled number is given a symbol or value which is usable and applicable to the current Game (e.g., the scaled number 51 may be mapped to an Ace of Spades).

Link utilisation shall mean the percentage time a communications link is engaged in transmitting data.

Timestamp shall mean a record of the current value of the Gaming Platform date and time this is added to message at the time the message is created.

Digital Certificate shall mean the electronic file used to verify ownership of a public key. The certificate includes information about the key, owner details and a digital signature of the entity that has certified the contents of the file. If the signature is valid, then the software using the certificate trusts the issuer and can use the key to securely communicate with the certification entity.

Advanced Encryption Standard (AES) shall mean the data encryption standard.

Batching The data should be placed in the Safe in the form of data packets (batches). A batch is comprised of individual records.

Chaining In order to ensure the maximum possible degree of security in storing and maintaining data in the secure data storing server, techniques for linking consecutive batches are used (chaining) before they are permanently stored in it.

Domain Name System shall mean the global distributed online database which (among other things) regulates naming on the internet.

Electronic Identification, Authentication and trust Services (eIDAS) shall mean the EU Regulation on online identification and trust services for electronic transactions in the domestic market.

ISO 27001 is the standard that defines the prerequisites for an Information Security Management System, aimed to ensure that the company has determined and implements sufficient and appropriate controls relating to confidentiality, integrity and availability of information in order to adequately protect 'stakeholder' information and data.

RSA2048 is an asymmetric key cryptographic algorithm.

Startup value is the initial jackpot value (it excludes values from overflow meters).

Safe shall mean a safe data storing server, which receives the operator's data at predefined frequency. The safe storing server is certified and ensures the appropriate, secure and seamless storage of data about the game, not allowing changes of data stored in it, both by the Operator as well as by the Authority.

XML Advanced Electronic Signatures (XAdES) is an internationally popular standard used for digital signature of XML-type files, which incorporates additional security features, such as time-stamping and certificate revocation information.

XML Schema Definition (Xsd) file is the information included in an XML file governed by certain rules and limitations, which are described at the XSD file (data model).

XML (eXtensible Markup Language). XML language is a vastly popular and open standard for the definition and exchange of data. XML has been developed and is maintained by W3C (World Wide Web Consortium).

X.509 is an international standard that defines the function of Public Key Infrastructure/PKI. It specifies the forms of the relevant information disposal (keys, certificates, recall lists) as well as the algorithms for the verification of a certificate's validity.

NOTE: Words or phrases for which no specific definition is provided in this Decision shall have the meaning stipulated in the Regulation.

Article 2

Scope of Application

This Decision sets out the Technical Specifications that information systems and all types of machinery, devices, hardware components software applications or systems and relevant premises associated with the conducting of online games of chance must comply with.

Chapter 2. Gaming Platform Requirements

Article 3

Player Online Account

3.1 General Requirements

The CIS shall provide and maintain a unique Player Online Account for each Player so that he/she can participate in Games. This account shall record information, among other things, about the bets placed and the winnings from the Games, the financial transactions associated with them, and the Player's available cash balance.

3.2 Player Identity Verification

The CIS shall implement procedures to verify the Player identity, pursuant to the relevant provisions on the implementation of measures for combating the laundering of money from criminal activities and countering financing terrorist activities by the Persons liable in the games of chance services market. The Player verification information must be kept securely online. The CIS shall keep information about all actions of each Player.

The Player verification process shall at least verify the legal name, physical address, age and nationality of the individual at a minimum, as well as anything else required by the Authority. It shall also confirm that the Player is not in any list of excluded persons held by the Operator and/or the Authority.

The Player verification information shall be kept in a secure manner.

It is permitted to use independent secure systems to verify the Player's age and/or identity in accordance with the regulation on the implementation of measures for combating the laundering of money from criminal activities and countering financing terrorist activities by the Persons liable in the games of chance services market and the Authority's instructions.

The Operator must notify a documented policy on how he/she handles Players engaged in illegal activities, including but not limited to the following:

- a) Maintaining information about any player's activity so that the Operator and Authority have the information needed to take appropriate action in the event of illegal activity being identified.
- b) Suspension of a Player Account where it is discovered that it is associated with illegal activities.
- c) Handling of deposits, wagers and winnings of the Player which are associated with illegal activities.

3.3 Personal Data Protection

During the registration process, the Player must agree to the applicable privacy policy pursuant to the applicable provisions. The privacy policy should state the minimum information that is required to be collected, the purpose of information collection, and the conditions under which information may be disclosed, and in particular:

- a) Any information obtained in respect to Player registration, or account establishment must not breach the personal data protection (privacy) policy.
- b) Any information about the current state of Player Accounts must be kept confidential, except where the release of such information is required by law.

c) All Player Information must be securely erased (i.e. not just deleted) from all storage devices, before the device is decommissioned. If erasure of such information is not possible, the storage device must be destroyed; and

d) A Privacy policy must be posted on the Gaming Platform and readily accessible to the Player.

3.4 Locally Stored Information (Cookies)

All cookies used shall contain no malicious code. Where cookies are used, the Player must be informed of the usage during registration. When cookies are required for game play, the latter cannot occur (as an application) if the Player Device does not accept them.

3.5 Opening of Player Account

3.5.1. Terms and Conditions

During the registration process, the Player must agree to the applicable terms and conditions of service. The terms and conditions, among other things, shall:

a) specify what will happen to bets placed but remaining undecided in incomplete games, where there are no game results.

b) clearly define the rules by which any unrecoverable malfunctions of gaming hardware/software are addressed including if this process results in the voiding of any pays or plays.

c) state that only Players who are legally permitted to participate in Games of Chance, pursuant to the relevant provisions, can participate in them.

d) describe the method to which Players will be notified of updates to the terms and conditions.

e) are easily accessible through a link on the Licence Holder's website.

3.5.2. Establishment of Player Online Account

Once identity verification is complete, the Player is not on any exclusion lists, the player account registration is complete, the player has acknowledged all of the necessary privacy policies and terms and conditions and the Player account can become active.

a) Each active Player Online Account must have a unique identifier in order to enable identification of the appropriate player and account details.

b) A Player must only be permitted to have one active Player Online Account.

c) The Player acquires access to the Player Online Account using a username (or similar identifier) and password and/or fingerprint and/or gesture and/or facial recognition. Note that it is possible to select more than one Player authentication method.

d) Where a Player forgets his/her username and/or password, an authentication process must be implemented to recover the username/password. All procedures for handling lost usernames or passwords must be clearly communicated to the Player in a secure manner.

e) The CIS must allow Players to change their passwords and remind them every six months at least of their obligation to change their passwords.

f) The use of multi-factor authentication processes is permitted to enable Players to change their registration details and/or details of the account used for financial transactions.

g) The CIS must support a mechanism allowing a Player Online Account to be excluded in the case where suspect activities are identified in relation to its security (such as many failed login attempts). The multi-factor authentication process must be implemented in order to activate the Player Online Account if it has been locked.

Article 4

Operation of the Player Online Account

4.1. Player Session

A Player Session is the period of time between the moment the authorized Player logs into the CIS to the moment he/she logs out or is disconnected from the CIS. When a system provides access to multiple Games, Players may play more than one game during a Player Session.

4.2. Player Session Start

- a) In order for a Player to start a Player Session, he/she must use his/her unique username and password.
- b) When a Player logs in to the CIS, the last time they logged in must be displayed.
- c) Each Player Session must have a unique identifier which is allocated/assigned by the CIS so that all Player Sessions are separate from each other.
- d) The CIS must employ mechanisms which identify unauthorised use of the Player Online Account, such as the option to show the date and time of the last log in, the IP address at the last log in, as well as the ability to compare payment instruments in relation to already known deposits.

4.3. Self-imposed Player Session Inactivity

During a peer to peer game, the software must allow for user to set an 'Away from computer' status which could be utilized, for example, if the Player needs to step away for a moment. This functionality must be fully described in the help screens or applicable terms and conditions.

- a) The 'Away from computer' status must disallow all play, and also cause the player's turn to be automatically skipped during any round of play which takes place while this status is active.
- b) If a Player sets an 'Away from computer' status during the middle of a game, he/she will automatically forfeit their play for that round (e.g. for a round of poker, the software shall automatically fold the Player's hand during the next round of wagering) assuming that additional wagers or Player decisions are needed to complete the Game.
- c) If a Player performs any game sensitive action within the game window while in an 'Away' state (i.e. selecting an amount to bet, etc), the state shall be removed and the Player will be enrolled into the next round of play. Non-game sensitive actions, such as accessing the help menu from the Game window do not require this status to be removed.
- d) If no action has been taken by the Player within the time period specified in the help screens and/or the terms and conditions, the Player shall be automatically placed into the 'Away from computer' state.
- e) If the Player has been in 'Away' status, he/she must be automatically removed from the table he/she is currently enrolled in, provided that maximum time limit allowed to be in this status is reached, according to

the terms and conditions on conducting the Game or given that the Player has exceeded maximum time limit to participate in a Game, pursuant to Regulation (whichever occurs first).

4.4. Automatic Detected Player Session Inactivity

The CIS must employ a mechanism which detects session-inactivity and terminate a Player session when applicable.

a) If the Gaming Platform fails to receive a response from the Player Device within thirty (30) minutes, it must implement a user inactivity timeout and terminate the Session., according to applicable terms and conditions on the conducting of the Game.

b) If a Play Session is terminated due to a user inactivity timeout, the Player Device must display to the Player the server session termination (i.e: the user inactivity timeout) upon the player's next attempted action on the Gaming Platform.

c) No further game play is permitted until the Gaming Platform and the Player Device establish a new session.

4.5. Player Session End

A Play Session finishes when:

a) The Player notifies the Gaming Platform that the Session is terminated (e.g. 'logs out').

b) A session inactivity timeout is reached.

c) The Gaming Platform terminates the Player Session.

i) Where the Gaming Platform terminates a Session, a record must be written to an audit file that includes the termination reason, and

ii) the Gaming Platform must attempt to send a Session finished message to the Player Device each time a session is terminated by the Gaming Platform.

4.6. Inactive Accounts

a) A Player Online Account shall be considered to be inactive pursuant to the provisions of the Regulation.

b) The CIS shall employ a mechanism to protect inactive interactive Player Online Accounts that contain funds from unauthorised changes or removal.

c) The Licence Holder must put in place and implement a process to deal with unclaimed funds from inactive accounts, in accordance with the Regulation.

4.7. Player Funds Maintenance

To ensure the safe maintenance of player funds, the CIS shall apply the following principles:

a) Player Online Accounts must be secured against invalid access or update other than by approved methods;

b) All transactions are to be maintained in an audit log;

c) A deposit into a Player Online Account made via a credit card transaction or other methods which can produce a sufficient audit trail must not be available for betting until such time as the funds are received by the Licence Holder from the issuer or the issuer provides an authorization number to the Licence Holder indicating that the funds are authorized. The authorization number shall be maintained in an audit log;

- d) The Licence Holder must take the necessary technical and organisational measures pursuant to the provisions hereof and the Regulation so that where use of payment methods belonging to third parties is confirmed, said use shall be prohibited.
- e) Inactive Player Online Accounts holding monies in the CIS must be protected against illicit access or removal.
- f) All transactions involving monies are to be treated as vital information to be recovered by the CIS in the event of a failure.
- g) Payments into a Player Online Account are to be made (including funds transfer) directly in the name of the Player or made payable to the Player, pursuant to relevant provisions.
- h) Upon Player request, Player Online Account statements must be sent to the registered address (e-mail or mailing) of the player within a period of one (1) month at maximum. Statements must include sufficient information to allow the Player to reconcile the statement against his/her own records.
- i) The CIS must implement a secure process regarding any adjustments to the Player Online Accounts and their audit trails. The aforementioned process shall be subject to strict security control and audit trail.
- j) It shall not be possible to transfer credits between Player Online Accounts.

4.8. Taxation

The CIS supports a mechanism that is capable of identifying all wins that are subject to taxation and providing the necessary information specified by the Tax Authority.

4.9. Transaction Log

The Licence Holder (Operator) must provide a transaction log and/or record of the Player Online Account upon request. The information provided must include sufficient data that allow the Player to cross-check the financial information of his/her Online Account. The information provided must include, at least, the following, in relation to the types of transactions listed below:

a) Financial transactions (time-stamping):

- i. Deposits into the Player Online Account;
- ii. Withdrawals from the Player Online Account, and cancellations of withdrawals that have been requested;
- iii. Promotional or bonus credits added/removed from the Player Online Account (apart from credits won during participations);and
- iv. Non-automatic adjustments or modifications to the Player Online Account (e.g. due to refunds).

b) Betting transactions:

- i. The date and time the wager was placed;
- ii. The date and time the event started or date and time the event is expected to take place, for future events (if known);
- iii. The date and time on which the results were confirmed (this field remains blank until the moment of confirmation);

- iv. Any Player Participation options in Games including the choice of events, the type of wager, the features and any special conditions which apply to each Participation;
- v. The outcome of the wager (this field remains blank until the moment of confirmation);
- vi. The total amount wagered including any promotional/bonus credits (if applicable);
- vii. The total amount won, including any promotional/bonus credits (if applicable);
- viii. Commissions or charges collected (if applicable); and
- ix. The date and time on which the amount won was paid to the Player.

Article 5

Responsible Gaming

5.1. Information

The Licence Holder (Operator) must ensure that a responsible gaming page is accessible via all pages on his/her website and/or from any screen where game play may occur.

5.2. Self-imposed Limits

The Licence Holder must offer Players via the CIS an easy mechanism to impose self-limitations, pursuant to the Regulation. The CIS shall ensure that:

- a) All self-imposed limits are correctly implemented immediately or at the point in time (i.e. next login, next day, etc.) that was clearly indicated to the player.
- b) The Self limitations set by a Player must not override any system imposed limitations or contradict information within the Game rules.
- c) The Player may modify the limits set once the time limit set has elapsed.
- d) Self-limitations must not be compromised by internal status events, such as self-exclusion orders and self-exclusion revocations.

5.3. System Imposed Limits

- a) The CIS must be capable of applying Player limits pursuant to the relevant provisions and/or by the Licence Holder. Players must be notified in advance of any system-imposed limits and their effective dates. Once updated, system-imposed limits must be consistent with what it was notified to the Player.
- b) Upon receiving any system-limitation order, the CIS shall ensure that all specified limits are correctly implemented immediately or at the point in time (i.e. next login, next day, etc.) that was clearly indicated to the Player.
- c) In cases where system-imposed limitation values (e.g. limits on deposits, wager, loss, player session duration) are greater than self-imposed player limit values, the self-imposed limitations must take priority.
- d) System-imposed limitations must not be compromised by internal status events, such as self-exclusion orders and self-exclusion revocations.

5.4. Self-imposed Exclusion

The Licence Holder shall provide Players via the CIS an easy and obvious mechanism to self-exclude from game play, pursuant to the Regulation. The CIS shall ensure that:

- a) The Player must be provided with the option to self-exclude temporarily for a specified period of time or indefinitely.
- b) In the case of temporary self-exclusion:
 - i) No new bets or deposits are accepted from the player, until such time as the temporary self-exclusion has expired, and
 - ii) During the temporary self-exclusion period, the Player is not prevented from withdrawing any or all of his/her account balance through the account management console, provided that the CIS acknowledges that the funds have been cleared and that there is a verified legal payment instrument which belongs to the Player.
- c) In the case of indefinite self-exclusion:
 - i) No new bets or deposits are accepted from the player, until such time as the temporary self-exclusion has been revoked.
 - ii) The Player is paid in full for their account balance provided that the CIS acknowledges that the funds have been cleared and that there is a verified legal payment instrument which belongs to the Player.

5.5. System-imposed Exclusion

Exclusion of Players by the Authority and/or the Licence Holder shall be done in accordance with the Regulation. In such case, the CIS must provide a mechanism which shall:

- a) Provide a Player notification containing exclusion status and general instructions on how for resolution;
- b) No new bets or deposits are to be accepted from the Player, until such time as the exclusion has been revoked;
- c) During exclusion period, the Player must not be prevented from withdrawing any or all of their Online Account balance all or part of the balance, provided that the CIS acknowledges that the funds have been cleared, and that the reason(s) for exclusion would not prohibit a withdraw.

5.6. Player Self-Exclusion Service

This Service performs the following operations:

- a) Player self-exclusion notices.
- b) The Licence Holder must send the Authority, within a period not exceeding 24 hours after receipt of the request, the data of Players who have requested self-exclusion or whose previous request for self-exclusion has been amended or withdrawn.
- c) All Licence Holders shall be informed in real time of any updates about amendments relating to Self-excluded Players.
- d) The Licence Holder warrants to respond as needed to the notices referred to in the preceding point and provide the latest version of the list of self-excluded players.

e) Receipt of the latest version of the register of self-excluded players via the HGC's web service, if applicable.

f) The Licence Holder (Operator) must download the latest version of the Register of Self-Excluded Players.

5.7. Triggering the Cooling-off Period

The CIS must apply a cooling-off period which can be triggered with regard to factors such as:

- a) the length of uninterrupted Player Participation in a Game;
- b) the total amount of wagers on Games in each time period; and
- c) the gaming activity pattern related to an increased risk of Player participation in gambling, contrary to the rules and practices of Responsible Gambling.

Article 6

Complaints/Reports/Player Grievances

6.1. Submission – Handling of Complaints/Reports/Grievances

- a) The CIS must follow a procedure for submitting complaints/reports/grievances which shall allow the Player to monitor their progress.
- b) The Player shall have direct access within the Player interface to all information about who to contact to resolve disputes.
- c) The CIS shall ensure that Players can submit complaints/reports/grievances round the clock every day of the week (24/7).
- d) The complaints/reports/grievances log file and related correspondence shall be kept electronically pursuant to the relevant provisions.

Article 7

Control Program

7.1. Control Program Verification

The CIS must be capable of verifying that all control program components contained on the CIS are authentic copies of approved components of the CIS. The aforementioned process shall be made automatically, upon installation and at least once every 24 hours, and on demand. The Licence Holder must send the Authority the control program for approval.

- a) The authentication mechanism must employ a hashing algorithm which produces a message digest of at least 128 bits.
- b) A system log or report must be retained and be accessible for a period of ninety (90) days, which details the verification results for each control component authentication.
- c) The control program authentication must include all control program components which may affect game outcome or required CIS operations. Control program components include, but are not limited to,

executables, libraries, game or CIS configurations, operating system files, components that control required system reporting, and database elements that affect game outcome or required CIS operations.

d) If any control program component is determined to be invalid, the CIS must prevent the execution of or deactivate the control program component, and must automatically stop any gaming related functions related to that control program component.

e) Each control program component of the CIS must also have a method to be verified via an independent third-party verification procedure. The third-party verification process shall not include any process or security software within the CIS. The test laboratory, prior to system approval, shall approve the integrity check method.

7.2. Data Alteration

The CIS shall not permit the alteration/corruption of any accounting, reporting or significant event data without supervised access controls. In the event any data is changed, the following information shall be documented or logged:

- a) Data element altered/corrupted;
- b) Data element value prior to alteration/corruption;
- c) Data element value after alteration/corruption;
- d) Time and date of alteration/corruption.
- e) Personnel that performed alteration/corruption (user login).

7.3. System Clock

The CIS must maintain an internal clock that reflects the current date and time (in 24 Landscape hour format, comprehensible in the local date/time format) that shall be used to provide for the following:

- a) Time- stamping for significant events;
- b) Reference clock for reporting; and
- c) Time stamping of configuration alterations.

7.3.1. Synchronisation Feature

If multiple clocks are supported, the CIS shall have a facility to synchronize clocks since conflicting information could arise.

Article 8

Client Software

8.1 General Statement

The Client Software is any software downloaded or installed on a Player Device.

8.2 Client Software Requirements

The Client Software and Player Device must:

- a) Not contain the logic used to generate the result of any Game;
- b) Not be capable of conducting gaming activity if disconnected from the CIS, and

c) Not be used to store sensitive data or required CIS information.

8.3 Client-Server Interactions

The following requirements apply to Client Software and the client-server interactions during gaming:

- a) The Client Software must not automatically alter any client-specified firewall rules to open ports that are blocked by either a hardware or software firewall;
- b) The Client Software must not have access to ports, either automatically or by prompting the user to manually access, which are not necessary for the communication between the Player and the server (via the Player Device);
- c) Players must not be able to use the Client Software to transfer data to one another, other than chat functions (e.g.: text, voice, video, etc.) and approved files (e.g.: user profile pictures, photos, etc.), and
- d) If the Client Software includes additional non-game related functionality, this additional functionality must not alter the Game's integrity in any way.

8.4 Software Verification

The CIS must employ a mechanism that ensures any critical components contained in the Client Software present on the Player Device and used in conjunction with the CIS is verified upon initiation of any Player Session. The Licence Holder must notify the Authority of the control program in order to be approved. It is recommended that Client Software be verified at predefined time intervals during an active Player Session. Client Software critical components may include, but are not limited to, game rules, pay table information, elements that control the communications with the CIS or other components that are needed to ensure proper operation of the Client Software. The CIS must have the ability to disable the Client Software upon any unsuccessful verification – certification.

Plug-in means a system of elements for software that add special features to a larger piece of software. The plug-ins are used specifically on browsers to show videos, identify viruses and show new types of files. Adobe Flash Player and QuickTime are well-known examples of plug-ins. Plug-ins are specialised forms of what is called add-ons and include extensions or skins.

8.5 Compatibility Verification

During any installation or initialization and prior to establishing of a Player Session, the Client Software used in conjunction with the CIS must detect any incompatibilities or resource limitations with the Player system which would prevent proper operation of the Client Software. If any incompatibilities or resource limitations are detected, the CIS must:

- a) Notify the Player of any incompatibility and/or resource limitation preventing operation (e.g. browser type, browser version, plug-in version, etc.); and
- b) Prevent Gaming activity while any incompatibility and/or resource limitation exists.

8.6 Content

Client Software used in conjunction with the CIS must not contain any functionality that is considered to be malicious. That includes, but is not limited to, unauthorised file extraction/transfers, unauthorised player system modifications, and malware.

8.7 Communications

Communications between any CIS components, Player systems and Client Software which takes place over public networks must be secure. Personally identifiable information, sensitive Online Account data, wagers, results, financial information, and Player Session information must always be protected over any public network.

Article 9

Gaming Disable/Enable

1.1 General Statement

The following requirements apply to the disabling and re-enabling of gaming participation on the CIS:

- a) The CIS must be able to disable or enable all gambling on command.
- b) The CIS must be able to disable or enable Gaming on demand.
- c) The CIS must be able to disable or enable individual Player Sessions on command.
- d) When any gambling is disabled or enabled on the CIS, an entry must be made in an audit log which includes the reason for any disable or enable.

1.2 Current Game

When a Game of Chance or gaming activity is disabled:

- a) The Game is not to be accessible to a Player once the Player's Game has fully concluded.
- b) The Player should be permitted to conclude the Game in play (i.e. bonus rounds, double-up/gamble and other Game features related to the initial game wager should be fully concluded).
- c) If Wagers have been placed on pending real-life events:
 - i) The terms and conditions must clearly define what happens to the Wagers if the gaming activity is to remain disabled and the corresponding real-life event is completed, and the CIS must be capable of returning all bets to Players or settling all bets, as appropriate;
 - ii) The terms and conditions must clearly define what happens with the Wagers if the gaming activity is to re-enable before the corresponding real-life event is completed, and the CIS must be capable of returning all bets to the Players or leaving all bets active, as appropriate.

Article 10

Incomplete Games

10.1 Incomplete Games

A Game is incomplete when the game outcome remains unresolved or the outcome cannot be properly seen by the Player. Incomplete Games may result from:

- a) Loss of communications between the Gaming Platform and the Player Device;
- b) A Gaming Platform restart;

- c) A Player Device restart or malfunction;
- d) Abnormal termination of the Client Software;
- e) A game-disable command by the Gaming Platform during play.

10.2 Completion of Incomplete Games

The CIS may provide a mechanism for a player to complete an Incomplete Game. An Incomplete Game must be resolved before a Player is permitted to participate in another instance of the same game.

a) If the Player has an incomplete Game, the CIS is to present the incomplete Game for completion upon reconnection or whenever a new Player Session is established.

- i) Where no Player input is required to complete the Game, the Game must display the final outcome as determined by the CIS and game rules, and the Player Online Account must be updated accordingly.

- ii) For multi-stage games (single-player, multi-stage games), where Player input is required to complete the Game, the CIS must return the Player to the game state immediately prior to the interruption and allow the player to complete the Game.

Note: The addition of an optional bonus or feature such as double-up or gamble would not turn a Game into a multi-stage Game.

- iii) For multi-Player games, the Game must display the final outcome as determined according to the rules of the Game and/or terms and conditions, and the Player Online Account must be updated accordingly.

b) Wagers associated with an incomplete Game which can be continued must be held by the CIS until the Game completes. Player Online Accounts must reflect any funds held in Incomplete Games.

10.3 Cancellation of Incomplete Games

Wagers associated with an incomplete Game that can be continued, but remaining undecided for a time period specified in the terms and conditions of participation, can be voided and the Wagers forfeited or returned to the Player provided that:

a) The Game rules and/or the terms and conditions must clearly define how wagers are to be handled when they remain undecided beyond the specified time period and the CIS may be capable of returning or forfeiting the wagers, as appropriate.

b) In the event that a Game cannot be continued due to a CIS action, all wagers must be returned to the Players of that Game. By way of exception and in cases of peer to peer Games, the Licence Holder may return the wagers or part of them and/or credit additional amounts to the Players based on each Game outcome as determined upon game interruption, and according to the rules of the Game. All the aforementioned practices and criteria shall be notified to the HGC.

Article 11

Shutdown and Recovery

1.1 General Statement

The CIS must have the following shutdown and recovery capabilities:

- a) The Gaming Platform must be able to perform a graceful shut down and only allow automatic restart on power up after the following procedures have been performed as a minimum requirement:
 - i) Program resumption routines, including self-tests, complete successfully;
 - ii) All critical control program components of the Gaming Platform have been authenticated—certified using an approved method; and
 - iii) Communication with all components necessary for Gaming Platform operation have been established and similarly authenticated.
- b) The CIS must be able to identify and properly handle where master resets have occurred on other remote gaming components which affect the game outcome, win amount or reporting.
- c) The CIS must have the ability to restore the system from the last backup.
- d) The CIS must be able to recover all critical information from the time of the last backup to the point in time at which the Interactive Gaming System failure or reset occurred.

Article 12

Malfunction

The Gaming Platform must:

- a) Not be affected by Player Device malfunctions other than to institute the incomplete games procedures in accordance with the requirements on incomplete Games;
- b) Must include a mechanism to void bets and pays in the event of a malfunction of the Gaming Platform itself if a full recovery is not possible.

Article 13

Geolocation

The CIS and the Player System must be able to reasonably detect the physical location of an authorised Player attempting to access the service from, and must not permit wagering capabilities while the Player is in an area where this type of gaming is disallowed.

Article 14

Commercial Communication/Advertising

All advertising or marketing material within the CIS that is displayed or otherwise conveyed to the Player shall not:

- a) Consist of indecent or offensive graphics and/or audio as determined by the Authority;
- b) Obscure the Game play area or obstruct a Game in progress;
- c) Contain content which contradicts the game rules or terms and conditions of the Website; and
- d) Specifically target Players who have been excluded from play.

The Licence Holder must conform with the provisions specified in the Regulation and the decisions of the HGC on matters of Commercial Communication concerning Games of Chance.

The use of contact data, which have been used to set up the Player Online Account, in any manner for Commercial Communication purposes without the Player's consent is not allowed.

The HGC may demand direct suspension of any Commercial Communication action that is contrary to the provisions in force and to the Regulation.

Article 15

Player Loyalty Programs

15.1 General Statement

If Player loyalty programs are supported by the CIS, the following principles shall apply:

- a) Use of the Player tracking data must not breach the privacy policy;
- b) Redemption of Player loyalty program points earned must be a secure transaction that automatically debits the points balance for the value of the prize redeemed;
- c) All Player loyalty database transactions are to be recorded by the CIS; and
- d) If the Player loyalty program is provided by an external service provider, the CIS must be capable of securely communicating with that service.

15.2 Disclosure of Player Loyalty Promotions and Bonuses.

To avoid dispute and confusion, the following disclosures must be made to the Player for any player loyalty promotions and/or bonuses;

- a) The CIS must make readily-accessible to the Player all terms and conditions governing each available promotional or bonus feature;
- b) The terms and conditions must be clear and unambiguous, in particular where bonuses or promotions are limited to certain tables or non-tournament play or when other specific conditions apply; and
- c) All bonuses and promotions must comply with the current legislation and regulation.

Article 16

Reporting

16.1 General Reporting Requirements

Documentation generated by the CIS shall be available upon request and for the interval defined for each required report. All reports must be generated by the system, even if the period specified contains no data

to be presented. The report generated shall indicate all required information and contain an indication of 'No activity' or a similar message if no data appears for the period specified. The CIS must provide a mechanism to export the data generated for any report to an acceptable format (i.e. PDF, CSV, etc.) as specified by the Authority for the purposes of data analysis and auditing/verification. The system must retain the report data for a time period specified in the relevant provisions. The CIS clocks must be used for all time stamping.

16.2 Player Session Report

The CIS must be able to provide a 'Player Session Report' (or similarly named report) on demand. Said report must contain the following information at a minimum:

- a) Unique Player Session ID;
- b) Unique Player ID;
- c) Session start time;
- d) Session end time;
- e) Relevant geolocation information (identification of the geographic location of the person or device via the Internet) if available;
- f) Amount wagered during Session (total and by transaction);
- g) Amount won during Session (total and by transaction);
- h) Promotional credits received during Session (total and by transaction);
- i) Promotional credits wagered during Session (total and by transaction);
- j) Funds deposited to the authorised Player's Online Account during Session (total and by transaction);
- k) Funds withdrawn from the authorised Player's Online Account during Session (total and by transaction);
- l) Reason for Session termination;
- m) Player Online Account balance at the start of the Session;
- n) Player Online Account balance at the end of the Session; and
- o) Funds remaining in Incomplete Games (total and by transaction).

16.3 Gaming Performance Report

The CIS must be able to provide a 'Gaming Performance Report' (or similarly named report) on demand over the specific period of the report and at a minimum for the specific intervals of month to date (MTD), year to date (YTD) and life to date (LTD) for each individual game (e.g. payable).

The report must contain the following information at a minimum:

- a) Interval selected;
- b) Unique Game Identifier;
- c) Total wagered;
- d) Total amount won;
- e) Total amount contributed to the progressive pool, if applicable;

- f) Total amount refunded; and
- g) Total funds remaining incomplete games.

16.4 Gaming Revenue Report

The CIS must be able to provide a 'Gaming Revenue Report' (or similarly named report) on demand over the specified period of the report and at a minimum for the specific intervals of month to date (MTD), year to date (YTD) and life to date (LTD). The report must contain the following information at a minimum:

- a) Total amount of non-promotional deposits to site maintained Player Online Accounts;
- b) Total amount of non-promotional withdrawals from site maintained Player Online Accounts;
- c) Total amount of all non-promotional funds currently held in site maintained player accounts.

16.5 Progressive Jackpot Configuration Report

The CIS must be able to provide a 'Progressive Jackpot Configuration Report' (or similarly named report) on demand for each progressive pool on the Website during the specified time period of the report. The report must contain the following information at a minimum:

- a) Unique ID and name of progressive pool;
- b) Date and time progressive pool was placed into play;
- c) Contribution parameters (amount per day, percentage of minimum participation/pot, etc.) for all primary or secondary pools, including any diverted amounts;
- d) Unique payable identifier of each participating game;
- e) Total amount of wagers eligible for the progressive jackpot;
- f) Total amount of progressive jackpots won;
- g) Total jackpot contributions won;
- h) Jackpot start-up or other seeds which are not funded from contribution;
- i) Current amount for each jackpot prize offered in this jackpot pool;
- j) Current value of jackpot contributions diverted (for other purposes);
- k) Date and time of jackpot retired;
- l) Amount transferred;
- m) Date and time the jackpot was transferred, if applicable;
- n) Progressive jackpot limit value, if applicable; and
- o) Amount exceeding limit, if applicable.

16.6 Progressive Jackpot Won Report

The CIS must be able to provide a 'Progressive Jackpot Won Report' (or similarly named report) on demand for each progressive pool on the site during the specified time period of the report. The report must contain the following information at a minimum:

- a) Unique ID and name of progressive pool;

- b) Unique payable identifier of the game;
- c) Unique Player Session ID;
- d) Unique Player ID;
- e) Game cycle ID;
- f) Date and time of progressive jackpot award;
- g) Progressive jackpot level hit;
- h) Amount of Progressive Jackpot;
- i) User ID and name of the employee processing the win if applicable; and
- j) User ID and name of the supervisor confirming the win, if applicable.

16.7 Significant Event Report

The CIS must be able to provide a 'Significant Event Report' (or similarly named report). The report must contain the following information at a minimum:

- a) Failed system side login attempts;
- b) Significant periods of unavailability of the CIS, or any critical component of the CIS (e.g. when a transaction cannot be performed);
- c) Large wins (single or aggregate over a specified time period);
- d) Large transfers of funds (single or aggregate over a specified time period);
- e) System voids, overrides and corrections;
- f) Mandatory deactivation of an authorised Player;
- g) Any other activity requiring employee intervention and occurring outside of the normal scope of system operation; and
- h) Other significant or unusual events.

16.8 Change Notification Report

The CIS must be able to provide a 'Change Notification Report' (or similarly named report) for all changes to system, game or event configurations. Licence Holders (Operators) must provide a comparison report between previous settings and the new ones relating to the Game or event. The report must contain the following information at a minimum:

- a) Audit trail of information changed/modified by administrator accounts;
- b) Changes to date/time on master time server;
- c) Changes made to Game parameters; and
- d) Identification of the employee who made changes to Game parameters (e.g., game rules, payout schedules, house edge percentage, rake percentage, etc.).

Rake is a sliding scale commission received by a casino running a poker game.

16.9 Exclusions Report

The CIS must be able to provide a 'Player Exclusions Report' (or similarly named report) for all Players excluded from play and/or registration, regardless of whether they are excluded by themselves, the Licence Holder (Operator) or the Authority. The report must contain the following information at a minimum:

- a) Unique Player ID;
- b) Type of exclusion (permanent, self-excluded, etc.);
- c) Date exclusion commenced;
- d) Date exclusion ended;
- e) Reasons for exclusion; and
- f) Number of times the Player has been excluded (at the time of the report).

16.10 Account Balance Adjustment Report

The CIS must be able to provide an 'Account Balance Adjustment Report' (or similarly named report) on demand for each day's adjustments per authorized Player ID. The report must contain the following information at a minimum:

- a) Authorised Player's name and account number;
- b) Date and time of account balance adjustment;
- c) Unique transaction number;
- d) User ID and name of the employee handling the Player Online Account balance adjustment transaction, if applicable;
- f) Amount of the Player Online Account balance adjustment;
- g) Player Online Account balance prior to adjustment;
- h) Player Online Account balance after the adjustment;
- i) Type of Player Online Account adjustment;
- j) Reason/description of adjustment to Player Online Account balance.

16.11 Promotional Account Summary Report

The CIS must be able to provide a 'Promotional Account Summary Report' (or similarly named report) on demand, for any Player loyalty promotions and/or bonuses which is redeemable for cash, monetary game play credits or merchandise. The report must contain the following information at the minimum:

- a) Beginning balance for promotion type;
- b) Total amount of awards by promotion type;
- c) Total amount used by promotion type;
- d) Total amount expired by promotion type;
- e) Total adjustment amount of by promotion type; and
- f) Ending balance by promotion type.

16.12 Licence Holder Revenue Report

The CIS must be able to provide a 'Revenue Report' (or similar report) to be used for taxation-related information. The report must contain at a minimum the following information for each event and each market in the context of that event:

- a) Date and time each event/incident starts/ends;
- b) Total amount wagered;
- c) Total amount won paid to the Player;
- d) Total amount of cancelled wagers;
- e) Commission and taxes collected;
- f) Event and market IDs;
- g) Incident status (in progress, complete, confirmed, etc.).

16.13 Player Activity Limits Report

The CIS must be able to provide a 'Player Activity Limits Report' (or similar report) on demand related to any kind of limit (time limit and/or monetary threshold) set by the Player on a daily, weekly and monthly basis as well as to any limits exceeded by the Player . The report must contain at a minimum the following information:

- a) Unique Player Online Account ID;
- b) Category under which the Player Activity Limit falls;
- c) Date the Player Activity Limit was generated;
- d) Date the Player Activity Limit was changed;
- e) Start date of the Player Activity Limit;
- f) Player Activity Limit duration set anew;
- g) Player Activity Limit amount set anew;
- h) Previous Player Activity Limit duration;
- i) Previous Player Activity Limit amount;
- j) Drawee/originator who sets the limit;
- k) Unique Player Session ID within the Licence Holder's system during which the Player changed or set the limit value;
- l) Time limit exceeded by the Player;
- m) Limit amount exceeded by the Player;
- n) Unique Player Session ID within the Licence Holder's system during which the Player exceeded the Player Activity Limit;
- o) Indicator showing the Player Activity Limit exceeded during wagering;
- p) Unique Player Session ID during which the Player exceeded the Player Activity Limit;
- q) Unique Peer to Peer Session ID during which the Player exceeded the Player Activity Limit;
- r) Unique Poker Tournament ID during which the Player exceeded the Player Activity Limit;
- s) Unique Poker Tournament Transaction ID during which the Player exceeded the Player Activity Limit;
- t) Date the Limit was exceeded; and
- u) Date of Player participation in a Game for the first time after the Limit was exceeded.

16.14. Affiliates Report

The CIS must be able to provide an 'Affiliates Report' (or similar report) on demand related to any information regarding an Affiliate as well as his/her payouts made by the Licence Holder. The report must contain at a minimum the following information:

- a) Unique Affiliate ID granted by the HGC;
- b) Unique Affiliate ID granted by the Licence Holder;
- c) Affiliate Status;
- d) Unique identifier of the Cooperation Agreement concluded between the Affiliate and the Licence Holder, granted by the Licence Holder;
- e) Unique Affiliate Payout ID as recorded in Licence Holder's systems;

- f) Affiliate payout;
- g) Currency used to pay the Affiliate;
- h) Payment instrument used by the Affiliate to receive payouts from the Licence Holder;
- i) Name of the Payment Services Provider used by the Affiliate to receive payouts from the Licence Holder; and
- j) Unique Account ID within the Payment Instrument used by the Affiliate to receive payouts from the Licence Holder

Chapter 3.

Article 17

Game Requirements

17.1 Introduction

This section of the document shall set forth the technical requirements for the rules of play and related Player Interfaces.

17.2 Player Interface

17.2.1. Player Interface

The Player Interface is defined as the interface within the Client Software in which the Player interacts often referred to as 'gaming window'. The Player interface shall meet the following requirements:

- A) Any resizing or overlay of the Player Interface must be mapped accurately to reflect the revised display and touch/click points.
- b) The functions of all touch/click points represented on the Player Interface must be clearly indicated within the contact/click point area and/or within the Game rules. No touch/click points or keyboard inputs shall be hidden or undocumented anywhere on the Player Interface.

17.2.2. Game Cycle

A Game Cycle consists of all activities and communications over the duration of a game. Where multiple games are accessible from a games lobby, Players may play more than one Game Cycle at a time in separate gaming window instances.

a) Game Cycle Start:

- i) After the Player Online Account balance has adequate funds;
- ii) After the Player has nominated the number of credits to bet on that Game;
- iii) After the Player presses a 'play' button (or similar input).

b) The following Game elements are considered to be part of a single Game Cycle:

- i) Games which trigger a free game feature and any subsequent free games;
- ii) 'Second screen' bonus feature;
- iii) Games with Player choice (e.g., Draw Poker or Blackjack);
- iv) Games where the rules permit wagering of additional credits within the Game Cycle (e.g. Blackjack insurance); and
- v) Secondary game features (e.g. Double-up/Gamble).

c) A Game Cycle is considered complete when the final transfer on the Player's credit meter takes place or when all credits wagered are lost.

17.3. General Game Requirements

17.3.1. Game information

The following requirements apply to game information, artwork, paytables and help screens which include all written, graphical and auditory information provided to the Player either directly by the game interface or from a webpage accessible to the Player via a hyperlink located in a conspicuous location.

- a) Game and Player Device usage instructions shall be clearly stated and shall not be misleading or unfair to the Player.
- b) All statements and graphics within the game information, artwork, paytables and help screens shall be accurate and not misleading.
- c) All Game rules and payable information must be available to the Player directly on the Player interface or accessible from the Player Interface via a hyperlink without the need for funds deposits or funds staked.
- d) All game rules and payable information must be sufficient to explain all of the applicable rules and how the Player can participate in all stages of the Game.
- e) Paytable information must include all possible winning outcomes, patterns, rankings, combinations and their corresponding payouts with a designated denomination/currency. All displayed pays must be theoretically possible.
- f) There shall be sufficient information related to any award payout adjustments such as fees, rakes, sliding scale commissions, etc. taken by the house.
- g) Where the Artwork contains game instructions specifying a maximum win, then it shall be possible to win this amount from a single Game (including Game features or other Game options).
- h) The artwork shall contain the theoretical percentage Return to Player percentage (%RTP) and fully explain how this %RTP was determined (i.e. minimum, maximum, average, etc.) and thus how the patron may realize it (i.e. participation/bet requirements). For Games which offer bonus bets and require a base game bet, the minimum theoretical %RTP of the bonus bet shall take into account the fact that a base game bet must be placed.
- i) If the Artwork advertises the actual %RTP, the number of game plays related to said calculation must be advertised along with the period during which the game plays were played.
- j) If random/mystery prizes are offered, the maximum value obtainable from the random/mystery prize shall be indicated. If the value of the random/mystery prize depends on credits wagers or any other factors, this shall be stated.

k) Multiple Wins.

The Artwork should clearly state the rules for prize payments where multiple wins are possible.

- i) A description of what patterns will be paid when a pay line may be interpreted to have more than one individual winning pattern.
- ii) Where the Game supports multiple pay lines, the Artwork should display a message indicating that scattered wins on different pay lines are added or the equivalent.
- iii) Where the Game supports scatters, the Artwork should display a message indicating that scattered wins are added to pay line wins, or equivalent, if this is the rule of the game.

iv) The Artwork should clearly communicate the treatment of coinciding scattered wins with respect to other possible scattered wins. For example, the Artwork should state whether combinations of scattered symbols pay all possible prizes or only the highest prize.

v) The Artwork should clearly communicate the treatment of coinciding game outcomes.

l) Extra Lines.

If it is possible to bet on multiple lines and it is not clearly obvious which reel positions are part of each of the possible lines, then the additional lines shall be clearly displayed on the Artwork and appropriately labelled. The additional lines shall either be shown on the displayed artwork or be available for display on a help screen or permanently displayed on all game-play screens, in a location separate from the actual reels.

m) Multipliers.

Where multiplier instructions are displayed on the Artwork, there shall be no confusion as to whether the multiplier applies.

n) Symbols/Objects.

All game symbols shall be clearly displayed to the Player and not be misleading in any way. Game symbols should retain their shape throughout all artwork, except while animation is in progress.

o) Substitutes/Wilds

The Artwork should clearly state which symbols may act as a substitutes/wilds and in which winning combinations the substitute/wild may be applied.

p) Scatters

The Artwork should clearly state which symbols may act as a scatter and in which winning combinations the scatter may be applied.

q) Upcoming Wins.

The game shall not advertise upcoming wins unless the advertisement is accurate and mathematically demonstrable or if the Player has directly advertised current progress to that win (e.g. he/she has 2 of 4 tokens collected).

r) Card Games

The requirements for Games depicting cards being drawn from a deck are as follows:

i) Games which utilize multiple decks of cards must clearly indicate the number of cards and card decks in play;

ii) Cards once removed from the deck shall not be returned to the deck, except as otherwise specified by the rules of the Game depicted; and

iii) The deck shall not be reshuffled except as otherwise specified in the rules of the Game depicted.

s) Multi-Wager Games

The following requirements shall apply to multi-wager games:

i) Each individual Wager to be played shall be clearly indicated so that the Player has no doubt as to which Wagers have been made and the credits per Wager.

ii) Each winning prize obtained shall be displayed to the Player in a way that clearly associates the prize to the appropriate Wager. Where there are wins associated with multiple wagers, each winning Wager may be indicated in turn.

t) Game information, Artwork, paytables and help screens should not be indecent or offensive in any way or form.

17.3.2. Information Displayed

The following Game information shall be visible or easily accessible to the Player at any time during a Player Session:

- a) The name of the Game being played;
- b) Restrictions on play or betting, such as any play duration limits, maximum win values, etc.;
- c) The player's current session balance;
- d) The current Bet amount. This is only during the phase of a Game where the Player can add or place additional bets for that phase;
- e) The current placement of all Bets (e.g. Roulette numbers, Blackjack insurance, etc.);
- f) The denomination of the bet;
- g) The amount won for the last completed game (until the next game starts or betting options are modified);
- h) The Player options selected (e.g., bet amount, lines played) for the last completed game (until the next game begins or new selection is made);
- i) Initial Player selection options are to be described (e.g., selection of a runner in a horse race should identify name, number and expected payout). Player selection options, once the game has commenced, should be clearly displayed on the screen (cards held, hit, split, keno numbers etc.);
- j) The winning amount for each separate Wager and the total winning amount shall be displayed on the screen.

17.3.3. Forced Game Play

- a) The Player must not be forced to play a Game just by selecting it.
- b) It must not be possible to start a new game in the same Player Interface instance before all relevant meters have been updated on the CIS and all relevant connections and Player session balance has been updated.
- c) If an auto play mode is incorporated, it must be possible to turn this mode off at any time during game play.

17.3.4. Game Fairness

Games shall not be designed to give the player a false expectation of better odds by misrepresenting any occurrence or event.

- a) Games that are designed to give the Player the perception that he/she has control over the Game due to player skill, when they actually do not (i.e.: the game outcome is random) must fully address this behaviour in the game help screens.
- b) The final outcome of each Game must be displayed for a sufficient time period to allow the Player to verify the Game outcome.

17.3.5. Return to Player

Theoretical return percentage limits are laid down in the relevant provisions. Moreover, the requirements shall be established which detail how these percentages must be calculated. An evaluation in accordance with these requirements and policies will be independently conducted by the testing laboratory.

17.3.6. Odds

The Authority may establish policy regarding award odds. An evaluation in accordance with these policies will be independently conducted by the testing laboratory.

17.3.7. Game Outcome

All critical functions, including generation of the result of each Game (and the return to the Player) must be generated by the Gaming Platform and be independent of the Player Device.

- a) Game Outcome must not be affected by the effective bandwidth, link utilisation, bit error rate or other characteristic of the communication channel between the Gaming Platform and the Player Device.
- b) Determination of events of chance that result in a monetary award must not be affected or controlled by anything other than numerical values derived in an approved manner from the certified RNG (Random Number Generator), where applicable, and in conjunction with the rules of the Game.
- c) Each possible permutation and/or combination of Game elements which produces winning or losing game outcomes shall be available for random selection at the initiation of each game, unless otherwise stated by the Game.
- d) Results specified in accordance with the resulting combinations based on the rules of the Game must be applied immediately.
- e) Where the game requires sequence or mapping of symbols or outcomes (e.g., the position of hidden objects within a maze) to be set up in advance, the symbols or outcomes should not be re-sequenced or remapped, except as provided for in the rules of the Game.
- f) The Game must display the outcomes in a clear and accurate manner, without substituting the way the outcome is presented, using alternative means of presentation which indicate an unsuccessful outcome as 'near win'.
- g) Unless otherwise specified by the rules of the Game, events of chance within Games should be independent of and not correlated with any other events within the Game or events within previous Games.
- h) For some types of Games, such as spinning reel Games, unless otherwise disclosed to the Player, the mathematical probability of a symbol appearing in a position for any Game outcome must be constant.

17.3.8. Simulation of Physical Devices

Where a Game is represented or implied to include a simulation of a real-life physical device (e.g., the spinning of wheels, the rolling of dices, the tossing of coins, the dealing of cards, etc.), the behaviour of the simulation must follow the expected behaviour of the real-life physical device unless otherwise stated in the Game rules. That is:

- a) For Games that intend real-life physical simulation, the visual representation of the simulation must correspond to the features of the real-life physical device.
- b) The probability of any event occurring in the simulation that affects the outcome of the Game must be equivalent to the real-life physical corresponding device. For example, the odds of getting any particular

number in Roulette where there is a single zero (0) and a double zero (00) on the wheel, shall be 1 in 38. The odds of drawing a specific card or cards in poker shall be the same as in the live game.

c) Where the Game simulates multiple real-life physical devices which would normally be expected to be independent of one another, each simulation must be independent of the other simulations.

d) Where the Game simulates real-life physical devices that have no memory of previous events, the behaviour of the simulations must be independent of their previous behaviour, so as to be non-adaptive and non-predictable in practice.

17.3.9. Games with Time Dependencies

a) For Games where the outcome is affected by the time to respond to a game event, the Gaming Platform must only offer the Game after informing the Player of any handicap associated with the communication channel. Games which are inherently unfair will not be approved.

b) Rules must clearly describe the procedure in case of player disconnection from the network server during a Game of this nature (e.g. internet connection outage, PC crash, etc.).

17.4. Game/Bonus Features

17.4.1. Game/Bonus Features

This section refers to Games where one or more features/bonus prizes may be paid to the Player. In general terms, bonus prizes are awarded as a result of some second (or subsequent) screen animation and, unless otherwise advertised to the Player, the bonus game should be part of the overall payable theoretical %RTP. For games which support bonus features, the Artwork should address the following topics:

a) The Game shall display clearly to the Player which Game rules apply to the current Game state. These rules shall be made available to the Player prior to the start of the bonus Game versus during the bonus game.

b) The Game shall clearly display to the Player possible win amount ranges, multiplier ranges, etc. which can be obtained by Bonus play.

c) For bonus features which do not occur randomly during a Game play, sufficient information shall be displayed to the Player to indicate the current status towards triggering the next bonus feature.

d) If the Game requires obtaining several events/symbols to activate a bonus, the number of events/symbols collected shall be indicated.

e) Where applicable, the Game shall display rules for cases when the correct number of events/symbols needed to trigger the bonus are not accumulated.

f) If the accumulation of tokens may lead to free games, the number of possible lines and credits per line to be wagered during the free games shall be indicated.

g) If the bonus sequence consists of more than one feature game, the number of games in the bonus sequence that are remaining shall be displayed.

h) The Game must not adjust the likelihood of a bonus occurring, based on the history of prizes obtained in previous games except that the Player has been clearly informed of said possibility prior to his/her participation in the Game (i.e. Games shall not adapt their theoretical return to Player based on past payouts).

i) If a game's bonus is triggered after accruing a certain number of events/symbols or combination of events/symbols of a different kind over multiple Games, the probability of obtaining like events/symbols shall not deteriorate as the game progresses (e.g., for identical events/symbols it is not permitted that the last few events/symbols needed are more difficult to obtain than the previous events/symbols of that kind).

j) If a Game allows the Player to hold one or more reels/cards/symbols for one or more respins/draws, held and non-held reels/cards/symbols must be clearly marked on the screen, and the method for changing holds clearly displayed to the Player.

k) If a bonus feature is provided in which a Player has to wager additional credits, the Player shall be given a choice whether to enter the bonus feature or not. A Player who elects not to enter the bonus feature shall be positioned to the base game in the mode it was in prior to the bonus. A Player who elects to enter the bonus feature but has insufficient credit balance to continue may:

i) utilize temporary winnings from the base game or previous stages to complete the feature, if allowed by the Game rules;

ii) authorise more funds to be transferred to the Player Online Account; and

iii) perform a combination of points (i) and (ii) above, if allowed by the rules of the Game.

17.4.2. Gamble Feature

The following requirements apply to games which offer the choice of gamble feature (these games can also use terms such as Double-Up, Triple-Up or Take-or-Risk). The Player must have a choice as to whether or not they want to participate. Unless otherwise advertised to the Player, the gamble feature should have a theoretical RTP of 100% and should not affect the overall payable theoretical RTP. For such games, the Artwork must address the following stated:

a) The prize limit (if applicable) and the maximum number of gamble available;

b) When the gamble feature is discontinued before reaching the maximum number of gambles available, the reason must be clearly stated;

c) Any unusual game conditions during which the gamble feature is not available shall be specified;

d) If the gamble feature offers a choice of multipliers, it must be clear to the Player what the range of choices and payouts is; and

e) Once the Player has selected a multiplier, it must be clearly stated on the screen which multiplier has been selected.

17.5. P2P Requirements

Bots are a type of AI which may enable the Player to learn the Game environment and its rules, and help him/her practice the Game before taking part in it.

17.5.1. Peer to Peer (P2P)

P2P game rooms are environments which offer Players the opportunity to gamble with and against each other. In these environments, the Licence Holder (Operator) usually does not engage in the gambling event as a party (e.g. house banked gaming) but provides the gambling service or environment for use by Players and takes a rake, fee or percentage for the service. Systems that offer P2P Games shall do the following unless otherwise specified in the Game rules:

- a) Provide a mechanism to detect and prevent Player collusion, artificial Player software, unfair advantages, and ability to influence the outcome of a Game or Tournament.
- b) Provide warnings about how Bots can affect a play so that Players can make a documented decision whether to participate and provide steps to report suspected player-bot usage. Terms and conditions on the Game shall clearly state the aforementioned topics;
- c) Prevent authorized Players from occupying more than one seat at each individual table;
- d) Provide authorised Players with the option to join a table where all authorised Players have been randomly selected;
- e) Inform authorized Players of the length of time each Player has been seated at a particular table;
- f) Must not employ artificial Player software to act as an authorised Player except in free play or training modes.

17.5.2. Computerised Players

The following requirements apply to the use of computerized Players in free play or in training modes:

- a) The software may employ Artificial Intelligence (AI) in order to facilitate Game play for demo, free games or training modes.
- b) The use of AI software must be clearly explained in the help menus.
- c) All computerized Players must be clearly marked at the tables so that Players are aware of which Players are not human.

17.5.3. Contests/Tournaments

An organized event that permits a Player to either purchase or be awarded the opportunity to engage in competitive play against other Players may be permitted providing the following rules are met:

- a) While enabled for tournament play, no game may accept real money from any source nor pay out real money in anyway, but shall utilize tournament specific points or chips which shall have no cash value.
- b) Gaming contests/tournaments rules are available to registered Players on the Licence Holder's Website where the gaming contest/tournament is being conducted. The rules shall include at a minimum:
 - i) All conditions which registered Players must meet to qualify for entry into, and advancement through, the contest/tournament.
 - ii) Any conditions relating to late arrivals or complete tournament no-shows and how auto-blind posting and/or initial entry purchase is handled.
 - iii) Specific information pertaining to any single contest/tournament, including the amount of money placed in the prize pool.
 - iv) The distribution of funds based on specific outcomes.

- v) The name of the organisation (or persons) that conducted the contest/tournament on behalf of or in cooperation with the Licence Holder (Operator), if applicable.
- c) The results of each contest/tournament shall be made available on the Website for the participants to review. Subsequent to being posted on the Website, the results of each contest/tournament shall also be available upon request. The recording of the results shall include the following:
 - i) Name of the event;
 - ii) Date(s) of the event;
 - iii) Total number of entries;
 - iv) Amount of entry fees;
 - v) Total prize pool; and
 - vi) Amount paid for each winning category.

Note: For free contests/tournaments (i.e. registered Player does not pay an entry fee), all information required by the above must be recorded apart from the number of entries, amount of entry fees and total prize pool.

17.6. Game Recall

17.6.1. Player Facing History

A 'replay last game' facility must be provided, either as a re-enactment or by description. The replay must clearly indicate that it is a replay of the entire previous Game Cycle and must provide the following information (at a minimum):

- a) The date and time the game started and/or ended;
- b) The display associated with the final outcome of the Game, either graphically or via a clear text message;
- c) Total player cash/credits at the start and end of a play;
- d) Total amount bet;
- e) Total cash/credits won for the prize (including Progressive Jackpots);
- f) The results of any Player choices involved in the game outcome;
- g) The results of any intermediate Game phases (e.g. gambles or feature games); and
- h) Amount of any promotional awards received.

17.6.2. Back-end History

For each individual game played, the following information is to be recorded by the CIS in addition to the above required information:

- a) Unique Player ID;
- b) Contributions to Progressive Jackpot pools;
- c) Game status (in progress, complete, etc.);
- d) The table number at which the game was played (if applicable);
- e) The payable used; and

f) The Game identifier and version.

Chapter 4. IT System security

Article 18

IT System Security Requirements

18.1 General Requirements

The Licence Holder's CIS and the Intermediate Control System's compliance with the following IT security requirements ensures that Player participation in games played via the CIS is secure and Players are not exposed to unnecessary risks. These security requirements shall apply to the following components of the Licence Holder's CIS:

- a) Components which record, store, process, share, transmit or retrieve sensitive Player information (e.g. credit/debit card details, user authentication information, Player online account balances etc.);
- b) Components which generate, transmit or process random numbers used to determine the outcome of games;
- c) Components which store a Player Wager and/or relevant outcome(s);
- d) Points of entry to or exit from the above systems and/or other subsystems which are able to communicate directly with core CIS subsystems; and
- e) Communications networks which transmit sensitive Player information and/or Player activity.

18.2 Information Security Policy

18.2.1 General requirements

The Licence Holder must have a recorded CIS Information Security Policy which clearly states the Licence Holder's approach to managing information CIS security and its implementation. The recorded Information Security Policy shall at a minimum:

- a) be set out upon decision of the Licence Holder or a body/person duly representing it;
- b) be published and notified to the HGC and to all external bodies involved and to its employees;
- c) be revised at regular intervals;
- d) be revised each time that there are major changes to the CIS and/or to procedures supported by the CIS, to ensure without fail its completeness and effectiveness;
- e) set out the responsibilities of the Licence Holder's staff and of any external bodies involved in the operation and maintenance of the CIS.

18.3 Administrative Controls

18.3.1 Human Resource Security

The Security roles and responsibilities of the Licence Holder employees in relation to the use of the CIS should be defined by the Information security policy. In particular, at a minimum:

- a) All Licence Holder employees (users) shall receive appropriate security awareness training and regular updates in organizational policies and procedures as needed for their job function.
- b) There is an approved classified access policy for Licence Holder CIS users, both at the physical level (physical premises) and software/hardware level, which must be revised depending on business needs, and Licence Holder security needs.

- c) All CIS users shall be provided with access rights to the system following an authorisation process for a specific use.
- d) User access rights to the CIS must be evaluated and monitored by the Licence Holder's management team at regular intervals.
- e) The access rights of all employees to information and data processing facilities shall be removed upon termination of their employment, contract or agreement or adjusted upon change.

18.3.2 Third-party services

The Information Security Policy must describe specific roles and responsibilities for all subcontractors/contractors and third-party users in relation to the use of the CIS. In particular, at a minimum:

- a) Agreements with third party service providers, involving accessing, processing, communicating or managing information or data processing facilities, or adding products or services to the Licence Holders data processing facilities shall meet all relevant security requirements.
- b) Services, reports and records provided by third parties shall be monitored and reviewed and controls shall be carried out at least on an annual basis.
- c) Changes to the provision of services, including managing and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and procedures involved, and re-assessment of the risks.
- d) The access rights of all subcontractors/contractors and third-party users to information and data processing facilities shall be removed upon termination of their employment, contract or agreement ends or adjusted upon change.

18.3.3 Asset Management

The Information Security Policy shall describe the persons responsible and accountable for all assets that house process or communicate controlled information, including those comprising the operating environment of the CIS and/or its subsystems/components. In particular, at a minimum:

- a) An inventory shall be drawn up and maintained for all assets holding controlled items.
- b) Assets shall be classified in terms of their criticality, sensitivity and value.
- c) Each asset shall have a designated owner for ensuring that the information and data from the inventory is appropriately classified, and defining and periodically reviewing access restrictions and classifications.
- d) A policy shall be included on the acceptable use of assets associated with the CIS and its operating environment.
- e) A procedure shall be implemented for managing unpluggable assets.
- f) The storage media included in de-commissioned equipment shall be safely removed and disposed of.
- g) Removable storage media shall be disposed of securely using documented procedures.

18.3.4 Encryption Key Management

The management encryption keys used throughout the Licence Holder's CIS shall follow defined processes in accordance with the Information Security Policy. In particular, at a minimum:

- a) There must be a documented process for obtaining or generating encryption keys.

- b) There must be a documented process for managing the expiry of encryption keys.
- c) There must be a documented process to revoke encryption keys.
- d) There must be a documented process for changing encryption keys.
- e) There must be a documented process for the storage of any encryption keys.
- f) There must be a method to recover data encrypted with a revoked or expired encryption key for a defined period of time after the encryption key becomes invalid.

18.3.5 Software Development Lifecycle

The acquisition and development of new software shall follow defined processes in accordance with the Information Security Policy. In particular, at a minimum:

- a) The CIS production environment shall be logically and physically separated from the development and test environments.
- b) Development staff shall be different from the staff responsible for transferring software and code to the production environment.
- c) There must be a documented method to verify that unauthorised software/code is not transferred from the testing environment to the production environment.
- d) There must be a documented process to ensure that data from the CIS production environment are not used in testing environment, except if modified in such a way as to ensure that they are not associated with specific persons/events.
- e) All documentation relating to CIS software and application development should be available for the duration of its lifecycle.

18.3.6 Change Control

The Information Security Policy shall contain an appropriate change control process for CIS software/programs. In particular, at a minimum:

- a) Program change control procedures for software/programs must be adequate to ensure that only properly approved and tested versions of software/programs are implemented on the production environment. Production change controls shall include at a minimum:
 - i) An appropriate software version control or mechanism for all software components;
 - ii) Details of the reason for the change;
 - iii) Details of the person making the change;
 - iv) Complete backups of previous software versions;
 - v) A policy addressing emergency change procedures;
 - vi) Segregation of duties between persons responsible for software development, testing and roll out on the production environment; and
 - vii) Procedures to ensure that software/program documentation is updated as a result of a change made to the production environment.
- b) All patches should be tested, whenever possible, on the testing environment configured identically to the production environment in which they are to be installed. Under circumstances where patch testing cannot be thoroughly conducted in time to meet the timelines for the severity level of the alert, then patch testing should be risked managed prior to its installation and depending on the degree of risk, the untested part

must either be isolated or removed, or installation must be done and testing after the fact.

18.3.7 Incident Management

A process for managing CIS-related incidents shall be documented in accordance with the Information Security Policy. In particular, at a minimum:

- a) The incident management process shall include a definition of what constitutes an CIS security incident.
- b) The incident management process shall document how security incidents are to be recorded and reported.
- c) The incident management process shall include a procedure to handle security incidents such as:
 - i) procedures to handle different types of security incidents;
 - ii) procedures for the analysis of the cause of the security incident;
 - iii) procedures for communicating the security incident to the parties concerned;
 - iv) procedures for reporting the security incident to competent administrative authorities (i.e. the HGC);
 - v) procedures for forensic evidence collection related to the security incident; and
 - vi) procedures for controlled recovery from the security incident.

18.3.8 Business Continuity and Disaster Recovery (BC & DR)

The Information Security Policy shall contain a plan to recover CIS operations in the event that the production environment is rendered inoperable. In particular, at a minimum:

- a) The disaster recovery plan must address the method of storing Player Online Account information to minimise data loss in the event the production system is rendered inoperable. If asynchronous replication is used, the method for recovering data should be described or the potential data loss should be documented.
- b) The disaster recovery plan must delineate the circumstances under which it will be revoked.
- c) The recovery plan must address the establishment of a recovery facility/site physically separated from the production site.
- d) The disaster recovery plan must contain the technical steps required to re-establish CIS functionality at the recovery site.
- e) The business continuity plan must address the processes required to resume administrative operations, after the activation of the recovered platform for a range of scenarios appropriate for the operational system context.

18.4 Technical Controls

18.4.1 Self-Monitoring

- a) The CIS must implement the self-monitoring of critical components (e.g. central hosts, network devices, firewalls, third-party links, etc.).
- b) A critical component which fails self-monitoring tests must be taken out of service immediately. The component must not be returned to service until there is reasonable evidence that the fault has been rectified.

18.4.2 Domain Name Service (DNS) Requirements

- a) The primary server used to resolve DNS queries must be physically located in a secure data center.
- b) All manner of logical and physical access, whether on-site or remote, to primary DNS server must be

done based on Classified Access.

- c) There must be at least one secondary server that is able to resolve DNS queries. The secondary servers must be located at separate premises to the primary server.
- d) Zone transfers between the primary server and the secondary servers must occur at least every 24 hours, and
- e) Zone transfers to non-authorised servers (arbitrary hosts) should be disallowed.

18.4.3 Monitoring

- a) The clocks on all relevant data processing systems of the Licence Holder or a security sector shall be synchronised with an agreed accurate time source.
- b) Audit logs recording user activities, exceptions and information security events shall be produced and kept for an appropriate time period, to facilitate future investigations and access control monitoring.
- c) System administrator and authorised system operator activities shall be logged.
- d) Log Information shall be protected against tampering and unauthorised access.
- e) Any modification, attempted modification, read access or other change or access to any record, audit or log must be detectable by the CIS via file version or timestamp checks. It must be possible to see the particulars of the user who has viewed or altered a log file and when.
- f) Procedures to monitor use of data processing facilities shall be put in place and implemented, and the results of monitoring operations must be reviewed quarterly or in accordance with the instructions from the Authority.
- g) Any errors shall be recorded, analysed and settled via appropriate steps.
- h) Network appliances with limited onboard storage shall disable all communication if the audit log becomes full or offload logs to a dedicated log serve

18.4.4 Cryptographic Controls

The Information Security Policy should put in place and contain rules for using cryptographic controls to protect information. In particular, at a minimum:

- a) Sensitive Information carried via communication lines should be encrypted. Typical examples of information that may require encryption are PINs and passwords, account numbers (including card numbers) and their details, encryption keys, Player IDs, fund transfers to and from Player Accounts, changes in account details (e.g. change of address, change of credit card, change of name, etc.) and game performance data (e.g. games played, amounts wagered, winnings, etc.).
- b) Data that is not required to be hidden but must be authenticated shall use a form of message authentication technique.
- c) Sensitive data must be encrypted on an end-to-end basis and must not appear on any LAN or WAN in an unencrypted format. This also relates to Sensitive Data transmitted between CIS computers within the Licence Holder's facilities.
- d) For Sensitive Data transmitted between CIS computers located in separate secure data centers, encryption is not required where communication route is secure in physical terms and precludes access by unauthorised persons.

- e) All communication between Licence Holder terminals and the CIS must be subjected to strict authentication controls and must also be encrypted using particularly secure methods when being transmitted outside the secure data centres.
- f) Authentication must be available through Secure Socket Link (SSL) and the security certificate issued by an internationally recognised digital certification issuing body.
- g) Encryption algorithms must be proven to be secure against cryptanalytic attacks.
- h) The Licence Holder must have approved procedures followed by reports of weaknesses in the encryption algorithms used in any part of the CIS (including for example – but not limited to – firewalls, authentication systems and the operating system for the Supervision and Control IT System. Where weaknesses are identified, changes in the encryption algorithms must be implemented immediately. Where changes cannot be installed, the algorithm must be replaced.

18.4.5 Access Controls

The Information Security Policy must put in place and include rules for the allocation of access privileges on the CIS based on the Licence Holder's business requirements and the principle of least privilege. In particular, at a minimum:

- a) A formal user registration and de-registration procedure must be in place for granting and revoking access method to all IT systems and the CIS services.
- b) All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be selected to substantiate the ID of a user.
- c) Use of generic passwords shall be limited, and where used the reasons for their use shall be formally documented.
- d) Password provision must be controlled through a formal management process.
- e) Passwords must comply with the best security practices in terms of complexity, validity and structure.
- f) Access to CIS applications and operating systems shall be controlled by a secure log-on procedure.
- g) In addition to passwords, in line with the above, appropriate authentication methods shall be used to control access by remote users.
- h) Any physical access to areas housing CIS components and any access to applications and operating systems must be recorded.
- i) The use of automated equipment identification equipment to authenticate connections from specific locations and equipment shall be formally documented and must be included in the regular review of access rights by the Licence Holder.
- j) Restrictions on connection times shall be used to provide additional security to high-risk applications.
- k) The use of utility programs which might be capable of overriding CIS control system and application controls shall be restricted and tightly controlled.
- l) Restrictions on connection times shall be used to provide additional security to high-risk applications.
- m) Appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.
- n) Telecommuting activities on the CIS shall not be permitted except under circumstances where security

of the endpoint can be guaranteed.

18.4.6 Network Security Management

The Information Security Policy must put in place and contain rules for the networks to be logically separated. In particular, at a minimum:

- a) The failure of any single item should not result in denial of service.
- b) An Intrusion Detection System/Intrusion Prevention System must be installed on the network which can:
 - i) Check both external and internal communications.
 - ii) Detect and prevent Distributed Denial of Service (DDOS) attacks.
 - iii) Detect and prevent programs whose objective is malicious control of CIS networks.
 - iv) Detect and prevent Address Resolution Protocol (ARP) spoofing.
 - v) Detect other Man-in-the-Middle indicators and sever communication immediately.
- c) Each server instance in cloud and virtualized environments should perform only one function (e.g. application server). Alternative equivalent secure mechanisms shall be considered as technology evolves.
- d) In virtualized environments, redundant server instances cannot 'run' (operate) under the same physical hypervisor.
- e) Stateless protocols (e.g. UDP) should not be used for sensitive data without stateful transport.
NOTE: Although HTTP is technically stateless, if it runs on TCP which is stateful, this is allowed.
- f) All changes to network infrastructure must be logged.
- g) Detection programs must be installed on all CIS applications and operating systems to identify and prevent malware. Most recent versions must always be used.
- h) CIS Network security should be tested by a qualified and experienced staff on a regular basis.
- i) Testing should include testing of the public interfaces and the internal networks.
- j) Testing of each security domain on the internal network should be carried out separately.

18.4.7 Firewalls

- a) A Firewall should be located at the boundary of any two dissimilar security domains.
- b) All connections to CIS hosts in the secure data centre must pass through at least one approved application-level firewall. The same also applies to connections to and from any non- IT system hosts used by the Licence Holder.
- c) The firewall must be a separate hardware device with the following characteristics:
 - i) Only firewall-related applications may reside on the firewall; and
 - ii) Only a limited number of user accounts may be present on the firewall.
- d) The firewall must reject all connections apart from those which have been approved.
- e) All data packets directed to the firewall must be rejected in the case where they reach interfaces with networks outside the baseline envelope. The objective is to restrict access to the firewall only to authorised workstations within the baseline envelope.
- f) The firewall must maintain an audit log of all changes to parameters which control the type of connections permitted through the firewall.

- g) The firewall must maintain an audit log of all successful and unsuccessful connection attempts. Logs should be kept for at least 90 days and be partially reviewed on a monthly basis for unexpected traffic.
- h) The firewall must disable all communication if the audit log becomes full.

18.4.8 Remote Access

Remote access is defined as any access from outside the CIS or system network, including any access from other networks within the same establishment. Remote access to the CIS shall only be permitted unless otherwise specified by the relevant provisions, and shall have the option to be disabled. Where permitted, it shall be governed by the CIS operating rules and the corresponding firewall. Remote access security will be reviewed on a case-by-case basis in conjunction with the current technology. In addition, there shall be :

- a) No unauthorised remote user administration (adding users, changing rights, etc.);
- b) Unauthorised access to databases is not permitted other than retrieving information by utilising existing features.
- c) No unauthorised access to the operating system.
- d) An activity log to provide information on the username, date and time of login, login duration and activity while logged in.
- e) A two-factor authentication (2FA) tool to ensure remote access.

18.4.9 Backup

Backup copies of information and software shall be taken and tested regularly in accordance with the backup policy.

18.5 Physical and Environmental Controls

18.5.1 Secure Areas

- a) Secure areas which contain IT systems and related CIS communications systems shall provide physical protection against fire, flooding, storms, earthquakes and other natural or man-made disasters.
- b) Secure perimeters (barriers such as walls, card control entry gates or manned reception desks) must be used to protect areas which contain CIS data processing systems/components.
- c) Secure areas must be protected by appropriate entry control to ensure that Classified Access is implemented.
- d) Any access must be logged and stored in a file.
- e) Secure areas must include an intrusion detection system, and attempts at unauthorised access must be logged.

18.5.2 Gaming Equipment Security

- a) CIS servers shall be located in server rooms which restrict unauthorized access.
- b) CIS servers shall be housed in racks located within a secure area.

18.5.3 Supporting Utilities

- a) Components shall be provided with uninterrupted and adequate primary power.
- b) Components shall be protected against power failure and other manner of interruptions which could arise due to errors in support operations.
- c) Components shall be protected against changes in temperature which could affect their proper and

uninterrupted operation.

d) Power or telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

e) There shall be physical protection against fire, flooding, storms, earthquakes and other natural or man-made disasters for IT systems and related CIS communications systems housed in Data Centers.

Chapter 5. Event Wagering

Article 19

Event Wagering

19.1 General Requirements

The following requirements shall apply only to wagering on events (in accordance with the Regulation) where the Player places wagers on events/markets which are to occur in the future. The requirements stated in this Article are general in nature and do not apply to specific types of sports, contests, matches or wagers. The intent is to cover sports, contests, matches and wager types currently known and permitted by the applicable provisions and to provide the framework for future types.

19.2 Wagering Requirements

19.2.1 Wagering Information

The following sections describe the information which must be made available to the Player regarding the events/markets (and associated wager types) available on the CIS, and the methods for placing a wager:

- a) A list or equivalent representation of all available wager types must be made available to the Player.
- b) The Player must be able to view descriptions of the wager types prior to placing wager (via a hotlink) to a help/rules screen.
- c) The description of each wager type must include all available betting options for that wager type.
- d) A list or equivalent representation of all active events/markets must be made available to the Player.

19.2.2 Placing Wagers

- a) No wager amount may be greater than the current balance of the Player's Online Account.
- b) The method of placing a wager is to be straightforward, with all selections (including their order, if relevant) being clearly obvious to a typical Player.
- c) When the wager involves combining events/markets, such as Doubles/Trebles bets, such groupings must be clearly obvious to the Player, given the combination of information on the betting page and the help/rules screen.
- d) There must be a clear notification that the wager has been accepted by the system and details of the actual wager accepted must be provided to the Player (e.g. displayed as a betting ticket) with wager details, coupled with generic wager information presented on the help/rules screen.
- e) If the wager attempt is rejected (in full or in part) by the Gaming Platform, the Player is to be informed of the reason(s) for the rejection.
- f) The Player's Online Account balance is to be debited by the amount of the wager when notification of acceptance of the wager by the system is received.
- g) Wager confirmation should include the amount of the wager accepted by the CIS.

19.2.3 Event/Market Close

- a) The system must implement an automatic bet close when the scheduled time for the event is reached.
- b) There may be a manual override to the automatic close time.

- c) Players in a Player Session must be able to view when an event or market is closed (upon the Player's next interaction with the Website, which causes the on-screen information to be refreshed).
- d) It shall not be possible to place wagers on an event or market once it has closed. This requirement does not preclude the implementation of in-running betting.
- e) A cancellation grace period may be offered by the Licence Holder to allow Players to cancel wagers incorrectly placed. However, it must be short in duration from the placing of the Wager and must end before the start of the betting event.
- f) It is possible to re-open an event or market when the circumstances permit. Players must be able to view when an event or a market re-opens (upon the Player's next interaction with the Website, which causes the on-screen information to be refreshed).

19.2.4 In-Running Betting

The help/rules screen and/or terms and conditions for the website must contain an explanation to the player on how the Players who have more up-to-date information or faster internet connections and take advantage of the system delays shall be treated.

19.3 Results

19.3.1 Posting Results

- a) The CIS must inform the Player of how reliable official results for betting events are obtained and published.
- b) The CIS must clearly inform the Player of the means by which a winning wager will be determined.
- c) The rules available to the Player must clearly state what is to occur when there is potential for multiple events/markets to share the same winning outcome (e.g. a dead heat).
- d) The rules available to the Player must clearly describe the situation of winning results being entered for betting events which were not offered for wagering.
- e) The rules available to the Player must clearly state what is to occur when only a portion of a betting event is withdrawn, covering subjects such as:
 - i) Circumstances when all Wagers on that portion of the betting event are lost when withdrawn.
 - ii) Circumstances when all Wagers on that portion of the betting event are refunded when withdrawn, and
 - iii) Handling of the withdrawn portion of the betting event for Wagers involving multiple events/markets (e.g. parlays).
- f) If a betting event is abandoned for any reason, all Wagers involving solely events/markets associated with that betting event must be refunded in full.
- g) Wager types involving multiple events/markets (e.g. parlays) are to be treated as if every selection for that leg of the abandoned event is a winning wager (in order to allow the parlay wager to remain active) but with a 1.00 payout (i.e. no profit to the Player) which in turn causes the potential payout for the overall parlay wager to be adjusted accordingly.

19.3.2 Entering Results

- a) Results cannot be entered for an event/market unless the event/market is closed. This does not preclude the settling of events/markets within any given sport/contest/match before that sport/contest/match is concluded and the results come out.
- b) Results entry must include the entry of all information which may affect the outcome of all wager types offered for that event/market, whether any such wagers were actually placed or not.
- c) Results may be altered but not after they are confirmed, except where there is a resettlement.

19.3.3 Displaying Results

- a) It is accepted that the system will unavoidably be subject to a certain degree of results confirmation and synchronization delay for updates to the information as displayed on the player's screen, and it is possible that the information may only be updated at the Player's next interaction with the website, which causes the on-screen information to be refreshed.
- b) Players in a Player Session must be able to view the results when an event/market is closed.
- c) The Player must be able to view the results of any decided/concluded event/market, once they have been confirmed.
- d) Players must be able to view any change of results.
- e) When individual wager amounts are gathered into pools, the Player must be able to view the dividends of all decided/completed wagers, once they have been confirmed.

19.4 Winnings

19.4.1 Payment of Winnings

Winning wagers are to be directly credited to the Player's Online Account when the results of the event/market have been entered, confirmed and settled. If the Player is not in an active Player Session when the results are entered and confirmed, it is acceptable to transfer the winnings the next time the Account is addressed e.g. next Player Session or account withdrawal request.

19.4.2 Rounding

Where the calculation of payouts involve rounding, information on how the system handles these circumstances must be provided to the Player through the help/rules screen which must clearly specify what is to occur:

- a) Rounding to what level (e.g. 5 cents);
- b) Rounding up, down or true rounding; and
- c) Metering of rounding amounts must be done in accordance with the relevant instructions.

19.4.3 Withdrawn Selections

The rules available to the Player must clearly state what is to occur when only a portion of a sport/contest/match is withdrawn, covering issues such as:

- a) Circumstances when all wagers on that portion of the sport/contest/match are lost when withdrawn;
- b) Circumstances when all wagers on that portion of the sport/contest/match are refunded when withdrawn.
- c) Handling of the withdrawn portion of the sport/contest/match or for wagers involving multiple events/markets (e.g. parlays); and

d) Handling of reinstated selections, especially if 'Field' selections are offered.

19.4.4 Abandoned Events

a) If a sport/contest/market is abandoned for any reason, then all Wagers involving solely events/markets associated with that sport/contest/market are to be refunded in full.

b) The Licence Holder must specify according to the terms and conditions, when an event is considered to be abandoned (for example if 24 hours have not elapsed since the moment it was initially scheduled).

c) Wager types involving multiple events/markets (e.g. parlays) are to be treated as if every selection for that leg of the abandoned event/market is a winning wager with odds of 1 (in order to allow the parlay bet to remain active).

19.5 Fixed Odds Wagers

19.5.1 General Statement

This section relates to specific requirements for types of bet types where the payout is to be fixed when the wager is placed. Players must be able to access all current odds/payouts for all available events/markets at all times. In addition to the general requirements, the following requirements shall also apply:

19.5.2 Wagers

a) If the wager could have involved more than one prize table, the system must store and the confirmation must indicate to which prize table it applies.

b) If the wager involves bet types where the prize table may change dynamically, the system must store them and the confirmation must indicate the prize table payout(s) (e.g. odds) which will apply to this wager should it win.

19.5.3 Limitation of Liability

The rules available to the Player must clearly state circumstances where potential liability may be reduced for future events/markets by any means such as:

a) Prorating – abatement of large winners in an event/market when the overall payout liability is large;

c) Liability limits – wagers shall be automatically rejected if the liability for an event/market exceeds a predefined limit; and

c) Partial wager acceptance /wager rejection – any circumstances where a wager is partially or completely rejected. This is commonly followed by a change in odds/payouts.

19.5.4 Prize Payout Modification

a) The rules made available to the Player must clearly state circumstances when it is permitted to dynamically modify the odds/payouts on an event/market.

b) Players must be able to view when odds/payouts are changed.

c) Subsequent access to odds/payouts, e.g.: via a hotlink, must show current values.

d) It is accepted that the system will unavoidably be subject to a certain degree of synchronization delay for updates to this information as displayed on the Player's screen, and information may only be updated at the Player's next interaction with the website, which causes the on-screen information to be refreshed. To ensure player fairness, the system must specify situations where the Player has placed a wager for which the associated odds/payouts have changed (but not yet refreshed on the Player's screen), and notify the Player accordingly and ask for confirmation of the wager with respect to the new odds/payouts.

19.5.5 Adjustments to Fixed Prize Payouts

The rules made available to the Player must clearly state the circumstances when the odds/payouts are to be adjusted, such as:

- a) Multiple winning outcomes (e.g. dead heats);
- b) Withdrawal selections for which wagers are refunded;
- c) Abandoned legs of parlays; and
- d) Prorating.

19.6 Pari-Mutuel Wagers

19.6.1 General Statement

This section relates to specific requirements for bet types where individual wagers are gathered into pools. The results of the event of each pool are divided up by the total bet of winning selections to form a unit payment amount for that bet type.

19.6.2 Commission

The level of commission for each bet type must be fully displayed in the Artwork.

19.6.3 Dividends

The rules for dividend calculation must be clearly specified to precisely determine the following:

- a) Dividend formula;
- b) Handling of withdrawn selections;
- c) Handling of multiple winners of a bet type with dead heats, abandoned events etc.;
- d) Handling of postponed events; and
- e) Handling of circumstances where there are no winners of a pool must be clearly stated. Subjects which are to be covered are:
 - i) Countback levels;
 - ii) Progressive jackpots; and
 - iii) Pool refunds (with or without commission subtracted).
- f) The treatment of minimum prize payouts, calculation of other dividends and possible pool subsidies.
- g) The treatment of 'Field' wagers where changes of the state of selections' withdrawn status can occur e.g. selection reinstatement.

19.6.4 Wagers

- a) The Player must be able to view reasonable up-to date prospective odds/payouts for simple wagering pools.
- b) The Player must be able to view reasonably up-to-date values for total investments for all simple wagering pools.
- c) It is accepted that the system will unavoidably be subject to a certain degree of synchronization delay for updates to this information as displayed on the player's screen, and information may only be updated at the player's next interaction with the website, which causes the on-screen information to be refreshed. To ensure Player fairness, the system must identify situations where the Player has placed a wager for which

the associated odds/payouts have changed (but have not yet refreshed on the Player's screen), and notify the Player accordingly and ask for confirmation of the wager given the new odds/payouts.

d) For complex wagering pools, there may be limitations to the real-time accuracy of the pool estimates displayed to the Player.

e) The Player must be able to view the results of all decided events from the moment the results are confirmed.

f) The Player must be able to view the dividends of all decided bet types including those not yet confirmed.

g) The Player must be able view withdrawn selections (cash amount) for all events.

19.7 External Wagering Systems

19.7.1 General Statement

This section refers to requirements for event types where wagers placed through the CIS are forwarded to an external wagering system which controls the wagering, processes results and determines winning wagers. An example might be the CIS interfacing to a totalisator system.

19.7.2 Communications

Communication with an external wagering system must meet the requirements stated in Section entitled 'Technical Controls'.

a) The Licence Holder (Operator) concerned must justify the security level associated with all communications by means of a formal risk analysis.

b) All communication shall be recorded in a log as per the requirements of the transaction logs.

19.7.3 Information

a) If the external wagering system provides pari-mutuel wagering facilities for the CIS, it must periodically pass the current dividends estimates for active pools to the CIS. Cautionary notes must accompany said estimates.

b) If the external wagering system provides progressive jackpot facilities for the CIS, it must periodically pass the current progressive jackpot amounts to the CIS. Cautionary notes must accompany such projections (especially if cancellations are permitted).

c) If the external wagering system provides fixed-price wagering facilities for the CIS, where the odds/prize table can dynamically change, it must pass the current odds to the CIS whenever odds change.

d) The external wagering system must pass change of event status information to the CIS whenever a change occurs, including:

- i) Withdrawal/reinstated selections;
- ii) Altered event starting time;
- iii) Event closed/open;
- iv) Results entered/modified;
- v) Results confirmed; and
- vi) Event abandoned.

19.7.4 Wagers

- a) Wagers placed on the CIS must receive clear acknowledgement of acceptance, partial acceptance (with details) or rejection by the external wagering system.
- b) If the cost of the wager is set by the external system, there must be a positive confirmation sequence in place to enable the Player to accept the bet cost and the CIS to determine that there are enough funds in the Player Online Account to cover the wager cost. This activity shall be performed by the CIS prior to making an offer to an external wagering system.
- c) The Player Online Account balance shall be debited an amount equalling the offer (and cost) to the external wagering system. The funds shall remain as a 'pending' transaction with details of the offer to the external wagering system recorded/logged in accordance with the transaction logging requirements. Upon receipt of acknowledgement (which shall be logged) from the external wagering system, appropriate adjustments shall be made to pending accounts and the Player Online Accounts (if a refund is required due to partial acceptance or rejection of the offer).
- d) Cancellation requests from the CIS must receive clear acknowledgement of acceptance or rejection by the external wagering system.
- e) The Player Online Account balance is not to be credited by the CIS until final confirmation is received from the external wagering system including the amount of the cancel.

19.7.5 Results

When results are entered and confirmed on the external wagering system, each winning wager placed from the CIS must be transferred to it along with the amount of the win. Player Online Accounts are to be updated with the winning amounts.

19.7.6 Restart and Recovery

The process for all wagering activities between two systems is not to be adversely affected by the restart/recovery of either system (e.g. wagering transactions are not be lost or duplicated because of recovery of one system or the other).

19.8 Wager History and Logs

19.8.1 Wager History

For games which involve wagering on a future event, such as with sports wagering, a 'Wager History' must be provided. The history shall clearly indicate that it is a history of previous bets (wagers) and provide the following information (at a minimum):

- a) The date and time the wager was placed;
- b) A description of the final outcome of the game upon which the wager was placed, either graphically or via a clear text message;
- c) Total Player cash/credits upon placing the wager;
- d) Total Player cash/credits once the wager is settled;
- e) Total amount wagered including any multipliers;
- f) Total cash/credits won for the wager (including Progressive Jackpots);
- g) Any Player choices involved in the Wager;
- h) Results of any intermediate wager phases.

19.8.2 Logs

All event wagering transactions of significance must be logged on the CIS.

The decision as to what consists of transactions of significance will be made on a case -by- case basis, and at a minimum shall include:

- a) All communications including offers to place, amend or cancel a Wager made by the Player and before the offer is accepted;
- b) Wagering Acceptance (sells), rejections (including reason for rejection) and cancels;
- c) Wins added to the Player Online Accounts;
- d) Change to odds/payouts, commission, percentages, or other payout selections (not including dynamic odds/payout settings); and
- e) Change of event/market status:
 - i) Start/stop wagering;
 - ii) Results entry/modifications/confirmation;
 - iii) Withdrawal/reinstatement of wager types within the event/market;
 - iv) Abandoned events/markets; and
 - v) Alteration/override or start times.

Chapter 6. Live Dealer Requirements

Article 20

Live Dealer Requirements

The following requirements apply where a wager is placed online. The entire process must be viewed by all remote Players through real-time remote audio and video feed.

20.1 General Requirements

20.1.1 Definition

Live dealer games utilizing internet interfaces are limited to table games conducted by a real dealer using real gaming equipment with video and audio sent to all remote Players along with instructions received from each player using streaming, narrowcast, broadcast or other technology.

NOTE: Player shall mean a remote Player.

20.1.2 Information to be displayed

Information must be provided to the Player in real time and shall include all game play information which would be available from the online table game equivalent. Such information shall include:

- a) Date and time;
- b) Table number and location;
- c) Table minimum and maximum wagers;
- d) Number of decks used, if applicable;
- e) Amount wagered;
- f) Game outcome;
- g) Vigorish amount, if applicable;
- h) Payout odds, where applicable; and
- i) Amounts won or lost.

20.1.3 Incomplete Games

If a remote Player does not for some reason complete an action required of them to allow a game to continue within the allotted time:

- a) The Gaming Platform must complete the Game on behalf of the Player.
- b) The Game must be completed using an optimum strategy for that particular Game.
- c) The Player must not re-join the particular instance of a Game where the Gaming Platform has begun to complete the Game on behalf of the Player.
- d) Any winnings resulting from the Game must be credited to the Player Online Account.
- e) Any losses arising from the Game shall be retained in accordance with the game rules.
- f) Game results must be available to the Player and reference must be made to any decisions made by the Gaming Platform on behalf of the Player.
- g) Other Players in the Game instance must be able to complete their own Games (unless they cannot or do not take their turn).

20.1.4 Win Notification

Where the winning Player uses an internet interface/gateway, he/she must be notified of the win directly through the Player Online Account, including the amount won, in due course upon completion of the Game.

20.1.5 Player Application Requirements

Player applications must have sufficient resources to meet the minimum system requirements as set forth by the live dealer system and as advertised to the remote Player.

20.2 Betting by Internet Interface

20.2.1 General Statement

The following requirements apply only to Live Dealer games via an internet interface or to Games which effectively constitute an effective internet interface or gateway to an existing traditional/land-based Game already operating in a live environment.

20.2.2 Game Fairness

The following information shall be readily available through the Game's internet interface or gateway throughout a Player Session where applicable:

- a) Sufficient information to identify the particular Game selected.
- b) Game play and the payout rules shall not rely on sound to convey their meaning.
- c) All charges imposed on the Player such as fees or vigorish.
- d) Rules which describe procedures in place to deal with game interruptions caused by discontinuity of data flow, video and voice from the network server during a game (e.g. internet connection outage or wagering terminal malfunction).
- e) Players must be informed of any betting opportunity relying on live monitoring of an event (e.g. betting in play) that such live transmissions may be subject to delay or interruption. Where a delay is obvious or created by the system, the scale of the delay should be disclosed to the Player.
- f) The rules, Artwork and Functionality of the Game, as made available to the Player using the internet interface/gateway, must include no less information than that available to the Player using the traditional/land-based method, where applicable.
- g) Players who participate in the Game (or placing a wager in the case of wagering on a future event) using the internet interface/gateway must be no more or no less eligible to win the game than Players using the traditional/land-based method.

NOTE: Nothing herein shall preclude the possibility of implementing promotions on the Internet interface/gateway or the traditional/land-based method alone.

20.3 Automated Recognition Devices

20.3.1 General Statement

Game symbols applied in live dealer games must be automatically registered by automatic recognition devices. Game symbols applied in live dealer games shall be reported to the gambling system. Game rules for live dealer games shall be programmed into the gambling system. Any equipment used for scanning or otherwise detecting cards must be tested for reliability and all consumables used must be checked for defects prior to processing in order to prevent play being disrupted. Log of all tests must be maintained.

20.3.2 Manual Override

Automated recognition devices used for recognition and registration must be equipped with a manual operation mode which allows corrections of an erroneous result (where the detection equipment misreads a card, the position of the ball, etc.). The participant must be informed that the manual mode is active. Each time that the manual operation mode is activated, tracking should be enabled to allow for further review.

20.4 Simulcast Control Server

20.4.1 General Information

Games for remote Players shall utilize a simulcast control server to record all wagering activity and game results. The Simulcast Control Server shall:

- a) Provide the remote Player with real-time visual access to the live Game being played;
- b) Prevent anyone from accessing the wagering outcome results prior to finalize a wager;
- c) Record dealer verified game results before posting; and
- d) Be equipped with a mechanism to void game results if necessary.

20.4.2 Information Recording

Game logs must be maintained and game events collated into statistics that can be analysed for trends relating to game performance, staff and/or locations in the gaming area. The live dealer studio may use its own surveillance camera (CCTV) and split live fee to video transmission, or there must be a separate network of video involved. for video. A continuous recording must be made of all games played so that:

- a) The date and time of each Game can be determined to an accuracy of one second relative to the clock used by the system.
- b) The sequence of Games relative to each other can be determined.
- c) Each wager, win, loss, Player decision and dealer action can be determined.
- d) All game events are clearly identifiable and distinguishable.
- e) The sequence of events within each Game instance can be determined.
- f) All cards and Game results must be clearly visible along with a separate icon depicting a matching outcome on the Player screen.
- g) The recording shall be sufficient to prove whether the game rules are being complied with and identify discrepancies.
- h) The recording can be reviewed by Licence Holder (Operator) in the event of a dispute between a dealer and a Player.
- i) The recording can be reviewed by the Authority in the event that the Player is not satisfied with the review by the Licence Holder (Operator).
- j) The recording must be kept for the time period specified in the Regulation.

20.5 Operational Requirements

20.5.1 Equivalency of Signal

- a) Each Players shall have equivalent quality of video/audio feed from the live dealer system. Procedures should be in place to measure and verify this equivalency whenever communications are initiated, including reconnection due to signal interruptions or re-initiation when the signal was severed.

b) Player Devices shall have sufficient resources to meet the minimum system requirements as set forth by the live dealer system.

c) A minimum signal connection requirement for the Player's application connection shall be established, enforced and disclosed to the Players.

20.5.2 Reporting

Internal statistical results reviews must be regularly conducted to monitor Game performance, payout percentages, and to detect irregularities and variances. Policies and procedures for conducting results reviews, and investigation procedures to be undertaken in the event that material variances are identified, must be documented. Procedures for the completion of gaming operations reports should be implemented. Gaming operations reports shall include:

a) Procedure violation report;

b) Incident report; and

c) A report from the casino employee responsible for gaming tables (Pit boss report).

20.6 Live Dealer Studio Requirements

20.6.1 Live Dealer Studio Environment

The following requirements shall apply to Live Dealer Studios:

a) The physical security policy and procedures shall be reviewed periodically to ensure that risks are identified, mitigated and underwritten by contingency plans.

b) Security perimeters (barriers such as walls, card-controlled entry gates or manned reception desks) shall be used to protect live dealing premises and operations.

c) Physical protection against damage from fire, flood, earthquake, typhoon and other natural or man-made disaster shall be designed and implemented.

d) Access to premises shall only be permitted to authorised personnel.

e) Access points such as delivery and loading areas, and other points where unauthorised persons may enter the premises shall be controlled and isolated from operations areas to avoid unauthorised access.

f) The actual gaming area must be defined and have appropriate physical security controls.

g) Gaming servers and communications equipment shall be installed in a secure location or protected to reduce the risks of environmental threats and risks, and the probability of unauthorised access.

h) Gaming servers and communications equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

i) Computer and communications equipment must be properly maintained to ensure its continued availability and integrity.

j) All items of equipment containing storage media shall be checked to ensure that all sensitive data and licensed software have been removed prior to disposal.

k) Policies and procedures shall be in place to enable a suitable response to any computer or communications security issue.

20.6.2 Fixed Gaming Equipment

- a) Gaming equipment used in live dealer gaming operations must meet minimum standards set forth in the relevant provisions.
- b) Gaming equipment should be installed according to a defined plan and records maintained of all installed equipment.
- c) Gaming equipment should be inspected and cleaned at regular intervals to ensure that it is free from defects or mechanisms that could interfere with fair play.
- d) Obsolescent gaming equipment should be destroyed in a manner which ensures that the device, and any data stored in the device, cannot be used.

20.6.3 Consumable Gaming Equipment

- a) Consumables used in live dealer gaming operations must meet minimum standards set forth in the relevant provisions.
- b) Procedures must be implemented for tracking the inventory of consumables from receipt, through storage, installation, use, retirement and destruction. All consumables must have an associated audit trail to show the staff who had access to the consumables at any given time for any given operation.
- c) Periodic random inspections should be carried out on the consumables in use, from disbursement to retirement.
- d) Used consumables must be destroyed in a manner which prevents their accidental re-use in the Game, and which puts them permanently beyond use.

20.6.4 Staffing

- a) Procedures should be in place to perform background checks on the past life, relatives and friends (background checks) of newly recruited staff.
- b) Staff must undergo adequate training in the gaming procedures they will be using.
- c) Staff must be trained in and regularly reminded of any physical behaviour which is prohibited.
- d) Policies and procedures concerning rotas and shift patterns and allocation must be documented in writing.
- e) Documentation must be kept to allow staff records to be audited and investigations to be performed where staff members are either involved directly or where their presence in a particular place and/or time is crucial to understanding a chain of events.
- f) Procedures for the termination of staff shall be documented.
- g) A supervisory member of staff should always be present when gaming is taking place.
- h) Staffing logs must be maintained for each table.

20.6.5 Gaming Operations

- a) Separate procedures should exist for each Game and new Games must have their procedures in place before being offered to Players.
- b) Clear procedures relating to anomalous events that may occur during live dealing operations must be documented in writing and understood by staff. Documented procedures should cover, at a minimum:
 - i) Incorrect card detection by automated equipment;

- ii) Dropped cards;
- iii) Misdeals;
- iv) Re-spins;
- v) Aborted games; and
- vi) Table closure.

c) Consistent card shuffling procedures must be in place and the shuffling of cards must be logged. Card shuffling procedures shall include a verification of the card count.

d) Any equipment used for scanning or otherwise detecting cards must be tested for reliability and all consumables used must be checked for defects prior to processing to prevent play being disrupted. Logs of all tests must be maintained.

e) Policies and procedures must be in place to identify and replace automated scanning equipment that shows an unacceptable level of errors.

f) Procedures must be in place to describe the operations of the pit station.

g) Procedures must be in place to demonstrate that a person would not be able to assume all duties relating to card management and that there is a segregation of responsibilities prior to play, during play and after play.

h) Game logs must be maintained and game events collated into statistics that can be analysed for trends relating to game performance, staff and/or locations in the gaming area.

i) Procedures should be in place to deal with any video, voice or data stream disruptions during a game.

j) Procedures should be in place relating to additional surveillance systems used to supplement pit boss observations.

k) Where Players are able to chat with dealers, a defined procedure should be in place for the use of chat features.

l) Procedures should be in place to deal with Player disconnection during a Game.

m) Procedures should be in place to ensure that the CCTV footage is captured in such a way that precludes interference or deletion.

n) Gaming operations reports must be maintained.

o) The gaming reports and records procedures must be reviewed at regular intervals to ensure that risks are identified, mitigated and underwritten by contingency plans.

p) Equipment and procedures must have a level of randomness consistent with that seen in live casinos to ensure their fairness and integrity.

q) Card shoes and similar devices must be tamper- proof once they have loaded to preclude malfunction or attempts to sabotage, and to also preclude interference prior to play.

r) Procedures should be in place to prevent collusion, Player fraud, and impermissible use of gestures and/or words/phrases/sounds by dealers.

s) Procedures should be in place to enable Players seek help.

Article 21

Requirements for Electronic Playing Card Shuffling and Dealing Devices

21.1 Random Number Generator

21.1.1 General Requirements

The Random Number Generator (RNG) and mechanical devices shall ensure that the results of the playing cards are random. The results shall:

- a) Be statistically independent;
- b) Comply with the desired random distribution;
- c) Pass various recognised statistical tests; and
- d) Be unpredictable.

21.1.2 Applied Tests

The test laboratory may employ various recognised tests to determine whether or not the random values produced by the random number generator successfully pass the desired confidence level of 99%. These tests shall include, but are not limited to:

- (a) Chi-square test;
- (b) Equi-distribution (frequency) test;
- (c) Gap test;
- (d) Overlaps test;
- (e) Poker test;
- (f) Coupon collector's test;
- (g) Permutation test;
- (h) Kolmogorov-Smirnov test;
- (i) Adjacency criterion tests;
- (j) Order statistic test;
- (k) Runs tests (patterns of occurrences should not be recurrent);
- (l) Interplay correlation test;
- (m) Serial correlation test potency and degree of serial correlation (outcomes should be independent of the previous Game);
- (n) Tests on subsequences; and
- (o) Poisson distribution.

21.1.3 Background RNG Activity

The RNG shall be cycled constantly in the background between Games and during game play at a speed which cannot be timed by the Player.

21.1.4 RNG Seeding

The first seed shall be randomly determined by an uncontrolled event. After every Game, there shall be a random change in the RNG process (new seed, random timer, delay, etc.). This will verify that the RNG does not start at the same value each time. Alternatively, it is permissible not to use a random seed. However, the manufacturer must ensure that the Games will not synchronize.

21.1.5 Scaling Algorithms

- a) If a random number with a range shorter than the one provided by the RNG is required for some purpose within the device, the scaling method (i.e. conversion of the number to the lower range) shall be designed in a manner that all numbers within the lower range are equally probable.
- b) If a particular random number selected does not fall within the range of equal distribution of the scaling values, it is permissible to discard that random number and select the next in sequence for the purpose of scaling.

21.2 Non-Volatile Memory (NV) – Memory Requirements

21.2.1 General Requirements

Non-volatile memory (NV) shall be used for storing all data considered vital to the continued operation of the Gaming Device. Contents of the NV memory may include, but are not limited to, the shuffling device configuration data (i.e. the number of decks used, different shuffle methods, etc.) and Game configuration data (i.e. the type of Game – Poker, Blackjack, etc. and any variant of the Game – Draw Poker, Stud Poker, etc.).

21.2.2 Maintenance

Non-volatile memory storage (NV) shall be maintained according to a methodology that in most circumstances enables errors to be identified and corrected. This methodology may include, but is not limited to, signatures, checksums, partial checksums, multiple copies and the effective use of validity codes.

21.2.3 Comprehensive Checks

Comprehensive checks of the NV memory shall be performed once shuffling process has initiated, but prior to the start of the shuffle and upon completion of the shuffle prior to the cards being used for Game play. Said methodology shall detect failures with an extremely high degree of accuracy.

21.2.4 Unrecoverable NV memory

A unrecoverable corruption of the NV memory shall result in an NV memory error. Upon detection, the device shall meet the requirements laid down in Section entitled 'Program Interruption and Resumption' hereof.

21.2.5 Non-Critical Memory Space

NV memory space which is not critical to the security of the Gaming device does not need to be validated.

21.3 Program Storage Device Requirements (PSD)

21.3.1 General Requirements

All program storage devices should:

- a) be secured behind a fully closed door, panel or compartment so that they are not openly accessible and shall meet the requirements set out in Section 21.8 'Cover/Lid Open/Close' hereof;

- b) contain sufficient information to identify the software and the sequence number of the data packet stored on the device, in the form of labels, if applicable, or on screen;

NOTE: The process used to identify the software and the sequence number of the data packets shall be evaluated, where appropriate.

- c) contain information that allows the device to validate the contents of the program storage device upon:
 - i. Power up after initial installation; and
 - ii. Processor reset.

21.3.2 Non-Critical PSD Space

Space in the program storage device which is not critical to the security of the Gaming device does not need to be validated.

21.4 Control Program Requirements

21.4.1 General Requirements

Each device shall employ an proven mechanism to internally authenticate the program files prior to use or loading. The control program shall ensure the integrity of all individual controlled program components during execution of said components. Control programs must be subject to self-checks for possible corruption due to failure of the program storage media.

21.4.2 Authentication Method

The device must utilize an integrity check method with a secured hashing algorithm of at least 128 bits (e.g. MD5). However, Cyclic Redundancy Check (CRC) calculations must be used at a minimum (at least 16 bit). The test laboratory shall approve any other methodologies implemented.

21.4.3 Authentication Mismatch

If unexpected data or inconsistencies are detected, the device shall meet the requirements specified in Section entitled 'Error conditions' hereof.

21.4.4 Independent Control Program Verification

The device shall be able to allow an independent software integrity check to be performed from an outside source and is required for all control programs that may affect the integrity of the device. This must be accomplished by being authenticated by an independent external software device. The proper operation of the software must be validated either by an independent external device connected through a port to the relevant medium or, otherwise, by removing all relevant material so that it can be verified externally.

This integrity check will provide a means for field verification of the software to identify and validate the program. Prior to device approval, the test laboratory shall approve the integrity check method.

NOTE: If the authentication program is contained within the device software, the manufacturer must receive written approval from the test laboratory prior to submission.

21.5 Communication protocol

21.5.1 General Requirements

For devices communicating with other systems (e.g. prior Game result display device, electronic card table, etc.), the device must accurately function, as indicated by the applicable communication protocol.

21.5.2 Display of Game Results

For devices that are required to communicate results of the Game with another device or system (e.g. prior game result display device, electronic card table, etc.), it shall do so with a very high degree of accuracy.

NOTE: In the event of any inaccuracy occurs, a dealer override feature may be permissible to correct the inaccuracy. If the device does not support a dealer override feature, then the device must meet the requirements specified in Section entitled 'Error Conditions' hereof.

21.5.3 Security Information Protection

The operation of the device shall ensure that Sensitive information transferred between the device and other systems are not viewable through any display mechanism supported by the device. This includes, but is not limited to, validation information, security PINs, credentials, secure seeds and keys.

21.6 Error Conditions

21.6.1 General Requirements

Should an error occur, the shuffling device must stop working (lock-up) and be equipped with an appropriate indicator (e.g. sound alarm or light) to alert the operator. If a display screen is present, a message describing the error type shall be displayed.

21.7 Program Interruption and Resumption

21.7.1 Interruption

After a program interruption (e.g. processor reset, or any error condition), the shuffling device shall enter a lock-up condition and shuffle or deal must be nullified. Upon detection, the device must meet the requirements specified in Section entitled 'Error conditions' hereof.

21.7.2 Restoring Power

If the shuffling device is powered down while the device is in an error condition, upon restoring power, the specific error message shall continue to be displayed and the Gaming Device shall remain locked-up. This is:

- a) unless power down as part of the error reset procedure;
- b) the device checks for the error condition during power supply restoration or cover closing and detects that the error is no longer in existence.

21.7.3 Simultaneous Inputs

Programs must not be adversely affected by the simultaneous or sequential activation of various data inputs and outputs that could, intentionally or not, cause malfunctions or invalid results.

21.7.4 Resumption

Upon program resumption, the device must meet the requirements specified in Section entitled 'Control Program Requirements' hereof.

21.8 Cover/Lid Open/Close

21.8.1 Cover/Lid Open Procedures

There must be mechanisms to detect the opening of the cover, lid or access to any other critical portion of the shuffling device that may affect the integrity or security of the unit. Upon detection, the device shall meet the requirements specified in Section entitled 'Error Conditions' hereof. Critical portions of the shuffling device include program storage media and the cards after the shuffling process has been initialized.

21.9 Hardware Requirements

21.9.1 Device Identification

Each electronic shuffling device or card shoe shall bear at least the following information:

- a) The manufacturer's name;
- b) A unique serial number;
- c) The model number; and
- d) The date of manufacture.

21.9.2 Electrostatic Interference

Protection against static discharge requires that the electronic shuffler or card shoe device's conductive housing be earthed in such a way that static discharge energy shall not permanently damage or permanently inhibit the normal operation of the electronics or other components within the device. Should the operation of the device be temporarily disrupted when subjected to significant electrostatic discharge greater than human body discharge, they shall be able to recover and complete all interrupted operations without loss or corruption of any control or critical data information associated with the device. The tests shall be carried out with a severity level of a maximum of 27 kV air discharge.

21.9.3 Safety of the Device

Both electrical and mechanical components within the device along with its design features shall not expose its users to any kind of physical risk. The independent certification laboratory/test laboratory shall not be entitled to verify the findings arising from any Safety and Electromagnetic Compatibility (EMC) testings performed, since product manufacturers or purchasers are solely responsible to do so. Such Safety and Electromagnetic Compatibility testings should be set forth in specific legislation or regulation, and should be carried out either by the manufacturers or purchasers of these products. The independent certification laboratory/test laboratory is not responsible to carry out such testings and bears no responsibility for the device Safety and Electromagnetic Compatibility. Therefore, it shall not be able to verify any findings related to the aforementioned issue.

21.10 Device Functionality

21.10.1 Card Shuffler Functionality

Card shufflers must be designed so that:

- a) the order of inserting the cards in the shuffler does not affect the outcome of the game.
- b) their operation cannot be interfered with or interrupted, other than by turning off the power, without being detected.
- c) during operation, the card shuffler shall be able to dispense playing cards and not leave any marks, scuffs or abrasions, or cause any damage to the cards which would enable Players to recognise them;
- d) the card shuffler does not provide any kind of information related to the current Game being played, which could lead to the:
 - i. prediction of the Game outcome;
 - ii. tracking of the cards played and cards remaining to be played;
 - iii. analyzing the probability of the occurrence of an event relating to the Game;

- iv. developing a strategy for playing or betting to be used in the Game.
- e) The card shuffler may use ancillary devices that help meet the aforementioned requirements. Ancillary devices shall not affect the outcome of the shuffle.

NOTE: Ancillary devices shall perform according to the design and the operating specifications set forth by the manufacturer.

21.10.2 Shoe Functionality

The requirements laid down in this Section relate to the specific portion of the device that is used for collecting cards to be distributed by a dealer to the Game Players. Shoes are devices designed and constructed in such a way as to maintain the integrity of the Game. Mechanisms and controls shall be in place to prevent the tampering of any card loaded into the card shoe. Card shoes, where supported, must be designed to:

- a) facilitate the dealing of cards without revealing their face value;
- b) have a cover that serves to obscure the back of the cards in the shoe;

NOTE: The back of the cards do not need to be completely obscured and may be exposed to the extent necessary to permit the cards to be dealt from the shoe.

- c) shall not leave any marking on the cards which may assist any person to predict the outcome of a Game;
- d) shall not contain any hidden compartments.

21.10.3 Card Recognition

If card identification software is used, it shall:

- a) ensure a high degree of accuracy when identifying the value and suit of the card
- b) not provide any information that may be used to compromise the cards in the current shuffle or dealing shoe;
- c) not interfere with or modify the behaviour of the device;
- d) have a role-based access control to restrict access to the Game history, where this is supported.

21.10.4 Card Count

If card count technology is used, the card shuffler must be equipped with an accurate count.

NOTE: Card count in this Article shall refer to the number of cards, not the technique or strategy known as 'card counting' utilized during card games such as Blackjack.

21.10.5 Hand Formation

If cards dealt technology is used, then the device shall:

- (a) ensure that all hands dealt meet the requirements of the 'Random Number Generator Requirements' Section of this Article;
- (b) ensure that the correct number of playing cards is dealt, with a high degree of accuracy to ensure that extra cards are not dealt to Players.

21.10.6 Game History

If the device is capable of displaying the display the history of Game results, it shall do so with 100% accuracy.

NOTE: Voided rounds due to any machine malfunction are not required to be included in the Game history.

21.10.7 Multi-Game

If the device is capable of shuffling or shuffling more than one type of Game, the device shall give an indication (i.e. display the Game on the display screen, sequence of lights, etc.) to the current game being shuffled or dealt.

Article 22

Table Games Devices and Materials Requirements

22.1 Gaming Tables

22.1.1 General Requirements

Gaming tables must be made of robust materials, their design principles must not expose the Player to any physical risk and they must be used for and ensure the fair play of the Game for which they are intended.

22.2 Storage Boxes

22.2.1 General Requirements

The following storage boxes must be placed on the Gaming tables:

- a) Value Chips Box (float). This box must be placed on the table, protected by a special transparent cover (plexiglass) and be locked when the table is closed. The Casino's value chips must be placed inside this box. As far as the roulette table is concerned, there must be a special transparent safe construction (plexiglass) where coloured chips are to be placed when the table is not being used;
- b) Drop Box. The drop box must be placed and secured (locked) on the Gaming tables. This box must be made of a durable material and be equipped with a notch so that only the table's banknotes and relevant forms can be inserted. It must also close automatically in a mechanical way not allowing the banknotes or forms to be removed from the box.
- c) Tips Box. The tips box shall be placed and secured on Gaming tables. It shall also be made of a durable material and be equipped with an appropriate notch to allow the insertion of tips.
- d) House Edge (Baccarat, Chemin de Fer, Banco Punto). This float may be similar to the one mentioned above.

22.3 Table Felts

22.3.1 General Requirements

The felts of the tables must be made of a durable, fire-retardant and stain-resistant material and must preserve their initial form when used (non-stretch). They must not negatively affect the operation of monitoring system, not expose the Player to any physical risk and they must be used for and ensure the fair play of the Game for which they are intended.

22.4 Roulette Balls

22.4.1 General Requirements

Roulette balls must have a diameter of 18 to 21 mm and must be entirely made of a non-metallic material to provide anti-magnetic protection. Moreover, they must not expose the Player to any kind of physical risk and must be used for and ensure the fair play of the Game.

22.5 Chips

22.5.1 General Requirements

Chips must be made of a durable material. They are produced from a single matrix which is unique for each Casino. They must not expose the Player to any kind of physical risk and must be used for and ensure the fair play of the Game.

Chips may be equipped with radio frequency identification technology (RFID).

22.6 Dice

22.6.1 General Requirements

The dice must be a perfect cube made of a durable material and meet the following requirements:

- a) It must comprise smooth and uniform surfaces;
- b) Its sides must be 20 to 25 mm long and its angles must be right angles;
- c) It must be transparent, except for the parts of the cube where, without protrusions and without disturbing the cube's balance, the pips/numbers, the letters and the Manufacturer's number shall be depicted;
- d) Slanted or rounded edges or hollow points are not permitted;
- e) Its weight must be equally distributed on all faces;
- f) The pips/numbers shall have the same diameter. They must be white and represent numbers 1 to 6;
- g) The pips shall be placed as follows:
 - i. The one-pip side must be opposite the six-pip side;
 - ii. The two-pip side must be opposite the five-pip side; and
 - iii. The three-pip side must be opposite the four-pip side;
- h) Dice manufacturing accuracy shall be less than or equal to 0.5 microns (μm).

22.7 Decks

22.7.1 General Requirements

A casino Games deck is a standard 52- card deck, not including jokers, which is used for and ensures the fair play of the Game. The decks must comprise plastic-coated and waterproof or 100% plastic cards.

22.8 Roulette Wheels

22.8.1 General Requirements

Roulette wheels should be made of a durable material. They must not expose the Player to any physical risk and must be used for and ensure the fair play of the Game.

22.8.2 Types

The only roulette wheel types which are allowed to be used are those used for American Roulette and European/French Roulette. There are two types of wheels, which must have:

- 1) a single zero, with thirty-seven numbered positions, which correspond to the numbers from 1 to 36 and one 0, in the following order: 0-32-15-19-4-21-2-25-17-34-6-27-13-36-11-30-8-23-10-5-24-16-33-1-20-14-31-9-22-18-29-7-28-12-35-3-26, and

- 2) a double zero, with thirty-eight numbered positions, which correspond to the numbers from 1 to 36, one 0 and one 00, in the following order: 0-28-9-26-30-11-7-20-32-17-5-22-34-15-3-24-36-13-1-00-27-10-25-29-12-8-19-31-18-6-21-33-16-4-23-35-14-2.

22.8.3 Structure

The roulette wheel must comprise a cylinder, inside which there is a movable disc supported by a metal support. This disc must be divided into thirty-seven or thirty-eight distinct positions (cases). Separation of the cases into equal parts can be achieved by using small fixed metal separators (number separators) or in another secure manner that completely prevents the ball from being placed and stabilised between two separate cases. These positions must be coloured, alternately red and black, and must correspond to numbers from 1 to 36, not in ascending order, as well as to one zero or to one and two zeros, which cannot be red or black.

22.8.4 Operation

The roulette wheels must be of cutting-edge technology and bear the special security seal of their manufacturing plant. Roulette wheel rotation may be changed by an automatic electromechanical mechanism which must be integrated into the wheel within a closed locked case. Moreover, its operation shall be based on a special software which contains an 'RNG' (random number generator).

22.8.5 Balance

Wheels shall be equipped with equalisers to ensure the wheel's balance as well as the randomness of the Game.

22.8.6 Safety

When the table remains closed, the roulette wheel shall be protected by a specific transparent cover (plexiglass) and be secured with special numbered protective devices made of durable material.

Chapter 7. Intermediate Control System

Article 23

Requirements of the Intermediate Control System

The specifications of the overall technical solution for online gaming supervision in Greece are described in detail herewith. Initially, the architecture of the suggested system is presented in the form of block diagrams so that the structure of such a system may be comprehended. Next, the specifications for the forms of data to be exchanged through the system and stored in it are defined. This data relates to the interactions among system, Players, the Licence Holder's platform and HGC.

The most important subsystem of the suggested solution is the safe data storage server (Safe), which receives Licence Holders' data at predefined frequency. The safe storage server (Safe) is a certified subsystem and ensures the appropriate, secure and seamless storage of data relating to the Game (player activity, financial activity, Player Accounts, predetermined reports, etc.), not allowing changes of data stored in it, both by the Licence Holder and by the Authority.

23.1 Overall Architecture

The general system architecture shall comprise four (4) different systems, which are listed below and are analysed herewith. The main systems which constitute the total architecture are:

- a) The Player interface;
- b) The Licence Holder's central platform (CIS);
- c) The Intermediate Control System;
- d) The Authority's infrastructure.

Schematically, the system's topology is depicted in the figure below.

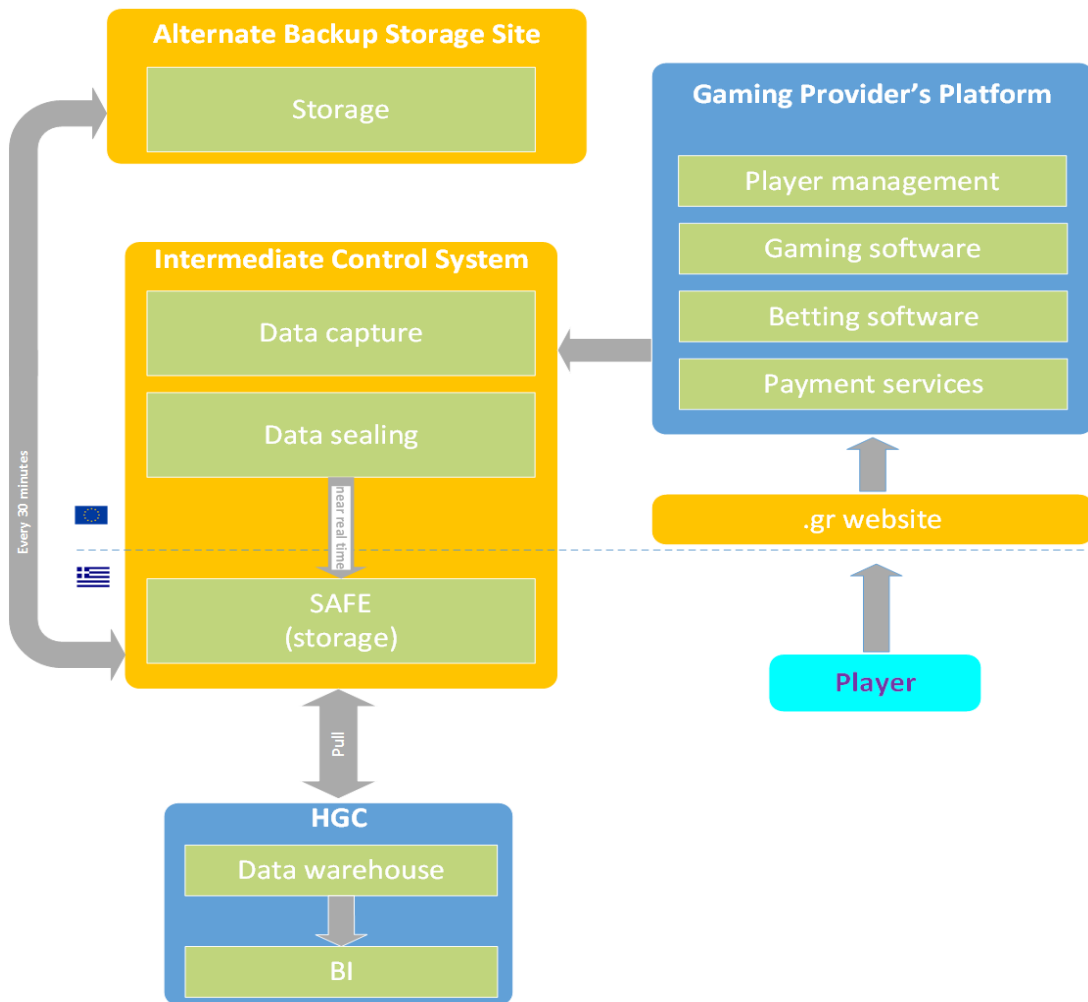


Figure 1. Technical Solution Topology

The Licence Holder is obliged to implement the Intermediate Control System in accordance with the specifications set out below.

The main functions of the Intermediate Control System are data collection from the Licence Holder's central platform (data capture), the safety of such data (integrity, authenticity, confidentiality, availability) (data sealing) and their permanent storage in the safe storage server (Safe).

The Authority should have access to the safe storage server in order to retrieve the structured data sets required for its auditing and supervisory role.

The technical specifications of the above systems are described in detail below, placing emphasis on the Intermediate Control System subsystems.

23.2 Data Capture

As mentioned above, the Licence Holder is obliged to implement the data capture subsystem, within the Intermediate Control System. Data capture subsystem shall execute the following functions:

- It shall extract data from the Licence Holder's main platform (CIS);
- It shall convert the extracted data to the appropriate format that meets the specifications set by the Authority (data models);

- c) It shall store the data (after having executed several data security functions) to the safe storage server (Safe).

23.2.1. Data Format

The appropriate data exchange format between the Authority and the Licence Holder is data exchange through XML (Extensible Markup Language) files. XML language is currently a widely used open standard for data definition and exchange. XML has been developed and maintained by W3C (World Wide Web Consortium).

Use of the XML language for the exchange of data guarantees controlled, safe and quick data stream between the two parties. At the same time, using a widely known open standard like XML language enhances interoperability of information systems among government bodies and corporations, as described in the Greek e-Government Interoperability Framework (Greek eGIF).

During the conversion of data extracted from the Licence Holder's main platform, the Licence Holder should follow the instructions described in each individual data model specified by the Authority. The data models are described by corresponding XML schemas. Before the data is stored and sealed in the safe storage server (Safe), they are validated as to their compatibility with the data model specified by the Authority (validate XML against XSD). The XSD files are available to interested parties through the Authority's website (<https://www.gamingcommission.gov.gr>).

The data follow UTF-8 format, and when reference to time is made, UTC standard shall be applied.

23.2.2. Maximum Delay

The maximum delay between each event and its insertion time in the Safe shall be two (2) hours. Therefore, the data must be forwarded and stored in the safe storage server (Safe) at least every two (2) hours.

23.2.3. Data Capture Subsystem Positioning

The data capture subsystem can be hosted within countries/jurisdictions specified in the Regulation.

The data centre which hosts the data sealing subsystem must meet the specifications described in Chapter entitled 'IT Infrastructure Security'.

23.3 Data sealing

23.3.1 Data sealing procedure

This section sets out in detail the data sealing procedure, in order to ensure data integrity and authenticity. In particular, the data sealing procedure includes a series of steps, as follows:

- Step 1: Create data packets (data batching) containing a number of records, as described in detail in the following sections.
- Step 2: The current batch is linked to the immediately preceding batch (chaining), by including a hash (SHA-256) of the latter and creating a 'chain' of batches.
- Step 3: Application of the digital signature to the data batches.
- Step 4: Data compression using a 'deflate' algorithm (RFC1951).
- Step 5: Time-stamping of compressed data according to XAdES-T standard.
- Step 6: Encryption of the compressed data using a symmetric, randomly generated one-time usage session key (AES-256).

- Step 7: Encryption of the session key with the Authority's public key (RSA-2048).
- Step 8: Data (from step 1), time-stamping (from step 5) and the encrypted key (from step 6) are all zipped together and permanently stored in the Safe.

23.3.1.1 Batching – Data Packets

The data shall be stored in the Safe in the form of data packets (batches). Each batch shall contain only one xml file for each data model. In the event that xml files belonging to different data model need to be sent, then data batches are created as many as the different data models. The data batch shall be time-stamped, as described in paragraph 23.3.1.5.

A data batch shall be created in the following cases:

- a) every two (2) hours maximum or as soon as the compressed received data volume exceeds 200 MB; and
- b) at the end of each day [00:00 (UTC +02:00)].

As long as no records are stored within two (2) hours, an empty data batch is created. An empty data batch shall not contain an xml data file, just the file containing the control information of the specific batch.

23.3.1.2 Chaining

In order to ensure a maximum degree of integrity and authenticity of the logged data, techniques for linking consecutive data batches shall be used before they are permanently stored in the server.

In addition, the chaining process should enhance the integrity and authenticity of recorded data, while ensuring their cohesion.

Through this process, the Authority shall be in a position to detect any deletion or change of stored data, regardless of whether this is considered a fraudulent activity or not.

Upon generation of the current batch, it shall be linked to the immediately preceding one through the inclusion of a hash (SHA-256) of the latter (cryptographic linking). The way of referencing hash values of previous batches creates a 'chain' of batches, as depicted in the figure below.

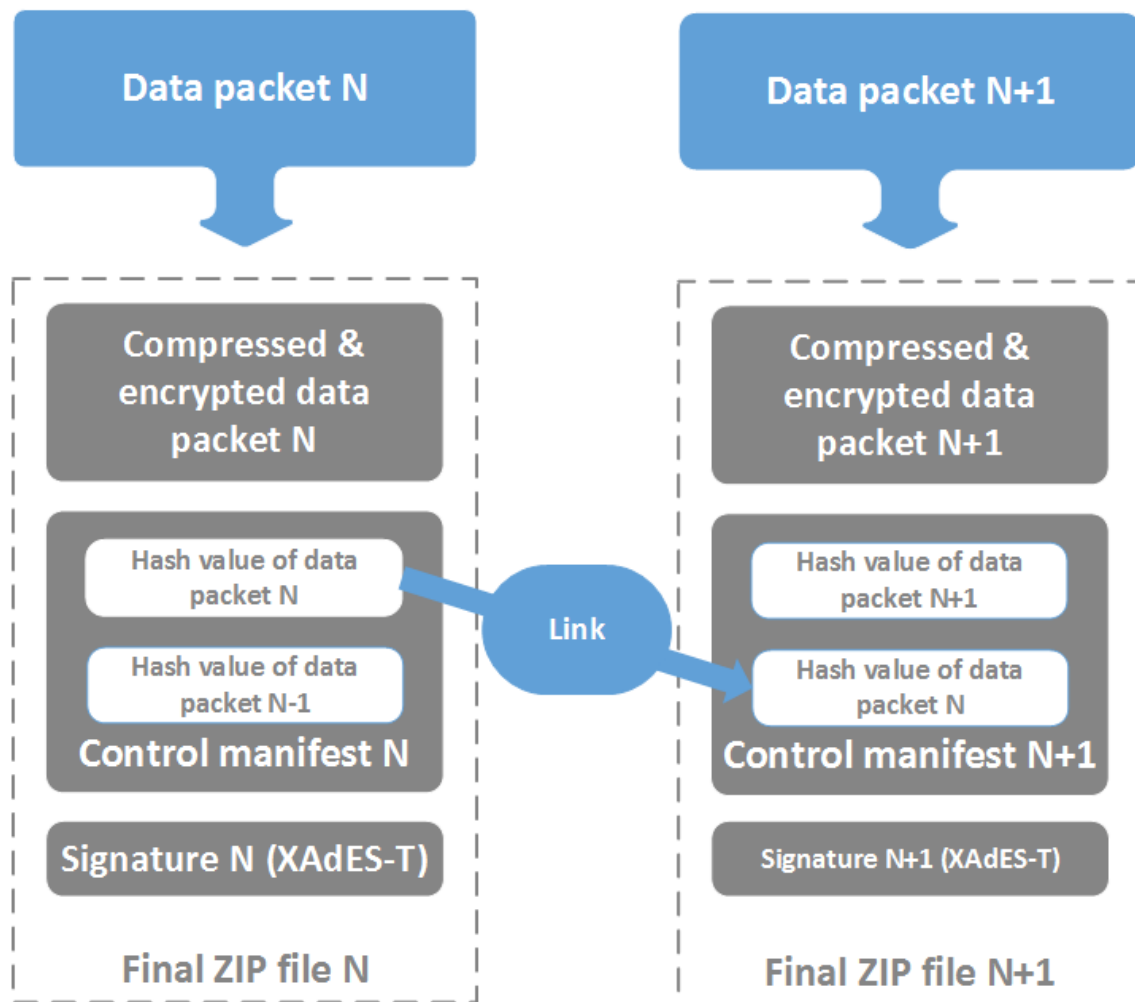


Figure 2. Process of Consecutive Batch Chaining

23.3.1.3 Digital Signature of Data

Batches stored in safe should be digitally signed to ensure their integrity and authenticity. The digital signature must be in line with the XAdES (ETSI TS 101 933) standard, which is an internationally widespread standard used for digital signing XML files.

Moreover, the XAdES standard incorporates security features in digital signatures, combining them with time-stamping, while it also implements cryptographic ‘tying’ of the signature using a signature policy that strengthens its legal value, covering the requirement that liability may not be denied.

Each Licence Holder must have its own digital signature key from internationally recognised organisations that issue digital certificates.

23.3.1.4 Data Compression and Encryption

The data batches shall be compressed using a ‘deflate’ algorithm (RFC1951) in order to reduce the volume of stored data in the safe storage server (Safe).

The compressed data packet is then encrypted to enforce confidentiality using a two-step procedure:

- Firstly, the safe storage server (Safe) dynamically generates a symmetric key (256 bit) for each batch in order to encrypt it, using the Advanced Encryption Standard (AES256).

- b) Then, the generated AES256 key shall be encrypted asymmetrically with the Authority's public keys (X.509 certificate) in accordance with the RSA2048 process (2048-bit RSA keys).

The above process is shown in the figure below.

In the second step, asymmetric encryption with more than one public key (X.509 certificates) must be possible, at the request of the Authority.

The digital certificate used in the procedure described above may be replaced by decision of the Authority.

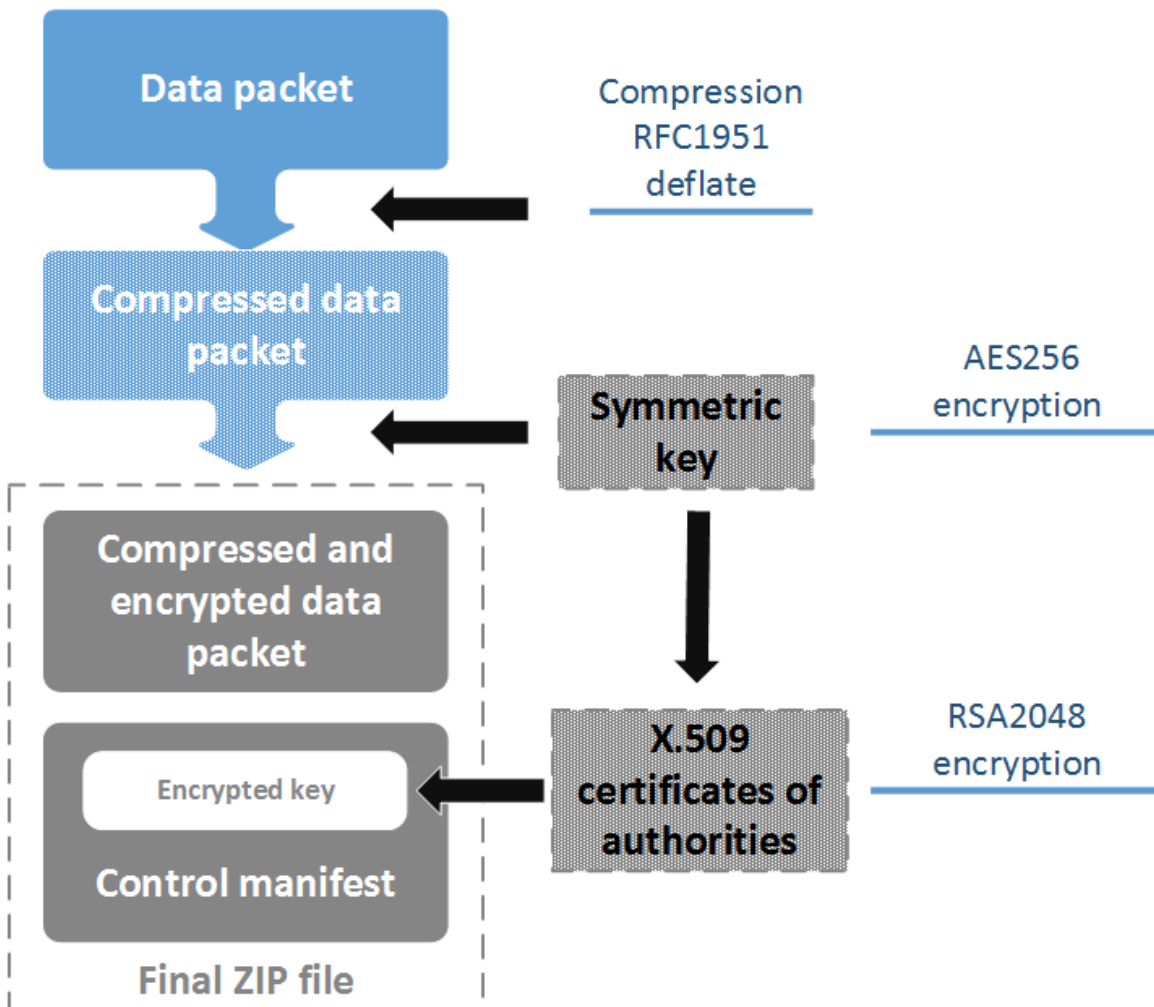


Figure 3. Data Compression and Encryption Procedure

23.3.1.5 Data Time-Stamping

Time-stamping is essential to enforce data integrity and precise data referencing to a specific point in time. Time-stamping shall be added in the form of a digital signature on each batch. The aforementioned digital signatures must be able to support timestamps by any Timestamp Server compatible with the European eIDAS timestamps standard ETSI EN 319 422 (RFC 3161). Finally, digital time-stamping signatures must be compatible with the XAdES-T standard.

23.3.2 Connection of the Data Sealing Subsystem with the Safe

The connection between the data sealing subsystem and the Safe shall be implemented by using secure end-to-end encryption technologies.

23.3.3 Data Sealing Subsystem Positioning

The data capture subsystem can be hosted within countries/jurisdictions specified in the Regulation.

The data centre which hosts the data sealing subsystem must meet the specifications described in Chapter entitled 'IT Infrastructure Security'.

23.4 Data Storage

23.4.1 Technical specifications for the safe data storage server

The Licence Holder is obliged to store on a secure data storing server the data relating to online Gaming as well as data exchanged between the Player, Licence Holder and financial institutions related to the Games.

The minimum technical specifications of the safe data storage server are listed below:

- a) The safe data storage server (Safe) must function as a separate subsystem which is physically detached from the Licence Holder's main platform.
- b) It is not permitted to store data in the Safe unless it is the modelled data specified by the Authority.
- c) The Licence Holder must ensure the necessary backup of all data, in accordance with the instructions specified in the relevant section. Safe data storage server and the alternative backup storage of Safe must be geographically separated, in accordance with the instructions specified in the relevant section. In addition, the data storage on a secondary storage medium (offline data), as defined in the relevant section, must be geographically separated from the backup of the Safe's data (alternative backup storage site).
- d) The certification of the Safe must be accompanied by the certification of the Licence Holder's information system.
- e) The Licence Holder must ensure that the Authority shall have secure online access to retrieve to both the safe data storage server (Safe) and the alternative backup storage subsystem, in accordance with the relevant section.
- f) Data stored in the safe data storage server must follow the naming and file/folder structure convention laid down by the Authority.
- g) Data stored in the Safe must be compliant with the data models and reporting instructions defined by the Authority.
- h) Data stored in the Safe must be compressed and encrypted, in accordance with the relevant section, so that only the Authority can have access to them.
- i) Licence Holders must certify and verify that the Intermediate Control System complies with the requirements laid down in herein.
- j) The Safe must be available 24/7, 365 days a year, with guaranteed uptime of at least 99.7%, measured on an annual basis.
- k) The Licence holder is responsible for the operation of the Safe and the Intermediate Control System.

- l) The Licence Holder must ensure that the Authority shall have access to the Safe, so that the following connection is possible: the Authority must have access to the Safe through an FTPS (FTP over SSL) connection. The Authority shall have access to the data kept in the Safe according to the specifications described in detail in the relevant section.
- m) Authority's access to the Safe and the alternate backup storage is only permitted from the predefined IP addresses which have been communicated to the Licence Holder by the Authority.
- n) The Licence Holder must comply with the specifications relating to the Intermediate Control System infrastructure maintenance and emergency handling, in accordance with the Gaming Regulation on the handling of changes to the Licence Holders' Information Systems.
- o) If the Authority detects a non-compliance of data with the models defined, the Licence Holder must respond without delay in order to correct them and submit them again. Communication between the Authority and the Licence Holder shall be carried out in accordance with the procedures laid down in the relevant section.
- p) The Authority must have physical access to the premises hosting the Safe and its alternate storage site, being able to navigate in their file system and copy their data to a detachable storage server.

23.4.2 Positioning of the Safe Data Storage Server

The Licence Holder must host the secure data storage server within Greek territory.

The data centre which hosts the Safe infrastructure must meet the specifications described in Chapter entitled 'IT infrastructure security'.

23.4.3 Data Segregation

Data stored in the Safe must meet the technical specifications laid down by the Authority. No other data is permitted to be stored in the Safe unless it is the modelled data specified by the Authority.

23.4.4 Format of Stored Data in the Safe Storage Server

After the data sealing procedure described earlier, the compressed and encrypted data packet shall be stored in the Safe.

Each data file stored in the Safe shall include the following information:

- a) The compressed and encrypted data packet (includes XML data record). This file will always have the name data.bin.
- b) The necessary control manifest (described in detail in the relevant section).

The above information shall be stored in zip format in the Safe. The resulting zip file shall be archived in the Safe in the folder structure of the corresponding day. The name of the resulting file shall be formed in accordance with the following convention:

<licenseholderid>_<serverid>_<seqno>_<YYYYMMDD>_<hhmmss>.zip

where:

- <licenseholderid> is the Licence Holder's registration number (lowercase letters);
- <serverid> is the name of the safe storage server;
- <seqno> is the data batch sequence number (10 numerals – leading zeros);
- <YYYYMMDD> is the generation date;

<hhmmss> is the generation time (24-hour format in UTC).

23.4.5 Structure and Labelling of Data Batches in the Safe Storage Server

In the safe data storage server, the final data files must be stored in Safe using the following folder structure in accordance with this specific labelling:

- LICENSEHOLDERID
 - YYYY
 - MM
 - DD
 - <LICENSEHOLDERID>_abc15_0000000001_<YYYYMMDD>_<hhmmss>.zip
 - <LICENSEHOLDERID>_abc15_0000000002_<YYYYMMDD>_<hhmmss>.zip
 - <LICENSEHOLDERID>_abc15_0000000003_<YYYYMMDD>_<hhmmss>.zip
 - ...
 - <LICENSEHOLDERID>_abc15_000000000N_<YYYYMMDD>_<hhmmss>.zip
 - YYYY
 - MM
 - DD
 - <LICENSEHOLDERID>_abc15_N+1_<YYYYMMDD>_<hhmmss>.zip
 - <LICENSEHOLDERID>_abc15_N+2_<YYYYMMDD>_<hhmmss>.zip
 - <LICENSEHOLDERID>_abc15_N+3_<YYYYMMDD>_<hhmmss>.zip
 - ...
 - <LICENSEHOLDERID>_abc15_M_<YYYYMMDD>_<hhmmss>.zip

23.4.6 Availability of Services

The guaranteed uptime of the secure data storage server and the other subsystems of the Intermediate Control System must be at least 99.7%. The Licence Holder must document to the Authority the maintenance of the system's availability at this percentage, by providing a relevant structural architecture plan of the systems.

In the event of the failure of any subsystem (data capture and/or data sealing), the data not yet received by the secure data storage server must be immediately received after the re-initiation of their appropriate function, so that the data cohesion, structure and time-wise is not compromised.

In addition, the Licence Holder shall provide to the Authority a disaster recovery plan for services.

23.4.7 Data Maintenance

The data must be maintained for a time period of up ten (10) years.

In particular, the data must be available online (immediately accessible) to the Authority, through the safe for at least five (5) years. Subsequently, the data can be stored in secondary storage devices (offline data) for the rest of the years until the completion of ten (10) years. Offline data must be maintained in the Intermediate Control System and within Greek territory. In any event the hosting of offline data cannot be carried out in the same geographical area where the Safe's backup is hosted (alternate backup storage site).

Within two (2) calendar days, at the most, the offline data must be made available to the Authority, through the safe storage server.

23.4.8 Backups

The data in the safe data storage server must be securely copied in an alternate storage site, to avoid data loss in case of a major destructive event of the main storage area.

The alternate storage site must be located at a distance of at least 20 kilometres away from the main safe data storage server and be synchronised with it every 30 minutes, through a secure connection dedicated for this purpose.

The Authority must also have classified remote access to the alternate storage site (as specified in the relevant section).

The data centre that hosts the alternate storage site infrastructure must be located within EU or EEA and meet the specifications described in the 'IT Infrastructure Security' chapter.

In the event of a major destructive event at the main storage site, the time required to restore it to full operation, with all data, to its former condition, shall not exceed five (5) calendar days, except in extraordinary events (like natural disasters). In such events, the Licence Holder shall request the Authority to extend the five (5) day limit.

The Licence Holder must inform the Authority without delay in the event of a major destructive event, justify in detail the causes of the event and submit a plan to restore the infrastructure to its former condition.

For the initiation of the data restoration from the alternate storage site to the main one, the Authority's approval is required.

23.4.9 Installation of a Trial Gaming Account for the Authority

The Licence Holder must set-up a trial gaming account for the Authority, to enable participation to the game under real-life conditions, except for the options to deposit money or make payments.

All activities of the trial Gaming account must, as regular player's date, be recorded in the safe data storage server.

23.4.10 Data Correction /Record Cancellation/Bet re-settlement

Where it is necessary to correct data that have already been sent for permanent storage in the safe storage server (Safe), the Licence Holder shall store the new record, keeping a reference to the record to be replaced. In particular:

- a) A new full record shall be generated, with the all corrected values as well as the values that remain unchanged and a special reference to the initial stored record (previous record ID). At the same time, the record to be changed shall be sent again, marked as 'Record which has been replaced by another record'.
- b) Where a record must be cancelled, the record to be cancelled is sent again, marked as 'Record that has been cancelled'.

Each record correction/cancellation requires adequate justification for the action taken as well as time-stamping, achieved through the use of the specific data model.

Where the amount allocated to a Player is redefined (bet-resettlement), the following shall apply:

In the event when the result of a football game, for example, has been erroneously registered in the Gaming system, and the winnings of one or more bets must be changed, the Licence Holder must report the difference in the winnings. For example, if the initial record stated that Player A won EUR 100,00 when in fact he/she won EUR 80,00, a new record will be generated, with the exact same fields, but a winning value of '-EUR 20,00'.

23.5 Data Access Management and Other Obligations of the Licence Holder

23.5.1 Data Access Methods and Management

Only the Authority may have access to the data stored in the main storage site.

The Authority must be able to access Safe via an FTPS (FTP-SSL, implicit) connection at portal 990. The use of a digital X.509 certificate issued by the Authority is required for access.

Access to the alternate storage site shall be granted in exactly the same way.

Access to the data maintained in the Safe and the alternate backup storage is only permitted from predefined IP addresses which have been specified by the Authority and communicated to the Licence Holder.

Transfer of data between the Safe and the Authority must be carried out via the internet, at minimum 8 Mbit/second. The Licence Holder must ensure that the connection is suitable for the smooth transfer of data.

The average time required for the Authority to gain access to the data (login time) may not exceed 15 seconds.

23.5.2 Data Access Availability

The guaranteed uptime of the secure storage server and the other subsystems of the Intermediate Control System must be at least 99.7%. When accessing data, the Authority must also have classified remote access to the alternate storage site, in the event that the main storage site is not available.

23.5.3 Physical Access to the Intermediate Control System

At the Authority's request, physical access to the data centers of the subsystems of the Intermediate Control System should be provided. In this context, in order to facilitate the Authority's auditing and supervisory role, data stored in Safe and alternate storage site should be accessible on-site by authorized Authority officials.

At the same time, the Authority must have the option to copy data from the Safe and the alternative storage site to a detachable storing device.

23.5.4 Maintenance of the Safe Storage Server (Safe) by the Licence Holder

The Licence Holder shall be the sole responsible for the maintenance and technical support of the infrastructure of the Intermediate Control System. The Licence Holder must comply with the procedures described in detail in the Gaming Regulation on the handling of changes in Licence Holder's Central Information Systems. In addition, as far as the safe storage server (Safe) is concerned, the requirements set out in the table below must also be complied with.

Table 1. Specifications for the Maintenance of the Safe's service window by the Licence Holder

Service type	Intervention time window	Maximum duration of intervention
Typical changes, patches, updates, etc.	• Maximum once every working day (Monday to Friday) 18:00-06:00. • Maximum 2 times a week, from Saturday 06:00 to Monday 06:00.	90 minutes
Time-consuming updates	At most 4 times a month, from Saturday 06:00 to Monday 06:00.	10 hours
Changes in the architecture or services	At most 4 times a year, from Saturday 06:00 to Monday 06:00.	24 hours

23.5.5 Significant – Extreme Emergency Events of the Safe Data Storage Server (Safe)

Should an extremely urgent incident which affects the seamless operation of the Safe, this must be communicated to the Authority and solved, in accordance with the provisions of the Gaming Regulation on changes' management in Licence Holder's Central Information Systems.

23.5.6 Licence Holder's Contact Persons on Technical Issues

In addition to the requirements relating to the different roles and persons laid down by the law as a prerequisite for issuing the licence, the Licence Holder must define at least the following technical roles:

- a) Head of operation and safety of the Intermediate Control System and other subsystems;
- b) Head of technical works and infrastructure maintenance.

23.6 Reports Environment

The Licence Holder shall maintain a reports environment to which the Authority may connect in order to gain access to financial data and player activity data stored in the CIS. No later than one (1) month after the

issuing of HGC Instructions describing in detail the specifications on how to implement the reports, the Licence Holder shall ensure access to said environment by the Authority.

The reports shall for the most part be centralised; reports relating to detailed elements may be requested.

The reporting system, at a minimum, must contain the reports described in detail in Article 16 entitled 'Reporting' hereof.

In consultation with the Licence Holder, the Authority may request the drawing up of additional reports or further analysis of the existing ones.

The reporting system will support, at a minimum, fifteen (15) users (users may have different roles), enabling the simultaneous use of the reports (concurrency) up to the level of at least 40%.

The reporting system should support data export to Excel and csv formats.

23.7 Data Models

23.7.1 Data Models

The data models are available on the HGC's website. (<https://www.gamingcommission.gov.gr>).

23.7.2 Data Model for the xml Control File

23.7.2.1 Labelling of the xml file

The xml control file must be named 'manifest.xml'.

23.7.2.2 Graphical representation of the xsd data model

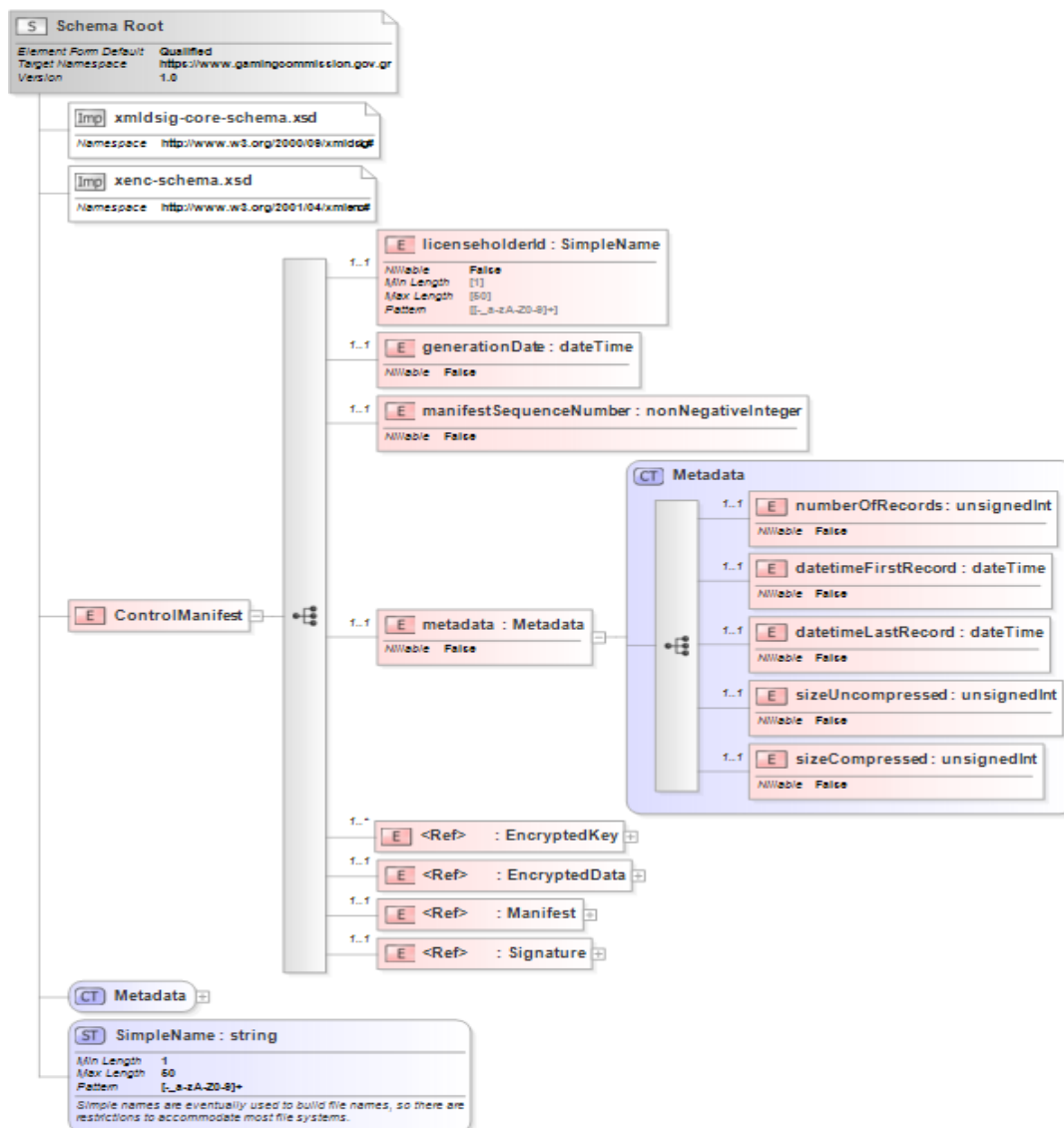


Figure 4. Data Model for the xml Control File

23.7.2.3 Detailed Description of the xsd Data Model

The control file is a supplementary xml file which accompanies each data batch stored in the Safe. It must include all the necessary control information (metadata) of each xml data file contained in each data batch. The most critical information contained in the control file relates to the identification of the interconnection of successive data batches (chaining hash values), the parameters used for compressing and encrypting data batches and the digital sealing of each data batch stored in the Safe.

In particular, the information contained in the control file shall be as follows:

- a) The unique identifier of the Licence Holder (hgc:licenseholderId);
- b) The unique identifier attributed by the Licence Holder to the server where the file is to be stored (10 lowercase letters-numerals) (hgc:serverId);

- c) The date and time (UTC) of generation of the control file (hgc:generationDate);
- d) The sequence number of the control file (hgc:manifestSequenceNumber);
- e) The metadata of the xml data file and data batch (hgc:metadata):
 - i. Number of records contained in the xml file (hgc:numberOfRecords);
 - ii. The date and time of the first record in the xml file (hgc:datetimeFirstRecord);
 - iii. The date and time of the last record in the xml file (hgc:datetimeLastRecord);
 - iv. The size of the uncompressed xml data file in bytes (hgc:sizeUncompressed);
 - v. The size of the compressed file xml data file in bytes (hgc:sizeCompressed);
- f) The dynamically generated symmetric key (AES256) with which the data file is asymmetrically encrypted, using the Authority's public key (X.509 certificate), according to the W3C XML Encryption standard (<https://www.w3.org/TR/xmlenc-core/>) (xenc:EncryptedKey);
- g) A reference to the encrypted data, according to the W3C XML Encryption standard (xenc:EncryptedData);
- h) The chaining information of consecutive data batches (chaining) (dsig:Manifest);
- i) The digital signature of the data batch, including its time-stamping, according to the XAdES standard (dsig:Signature).

Details on the methodology of compiling the xml control file are shown below.

/hgc:licenseholderId

Unique identifier of the Licence Holder.

/hgc:serverId

Unique identifier attributed by the Licence Holder to the server where the file is to be stored (10 lowercase letters- numerals)

/hgc:generationDate

Date and time (UTC) of generation of the control file.

/hgc:manifestSequenceNumber

Sequential counter of control manifests (whole number $N \geq 1$). This is identical to the sequence number of the data batch.

/hgc:metadata

The metadata of the xml data file and data batch (aggregated data).

/hgc:metadata/hgc:numberOfRecords

Number of records contained in the xml file.

/hgc:metadata/hgc:dateFirstRecord

Date and time of the first record in the xml file.

/hgc:metadata/hgc:dateLastRecord

Date and time of the last record in the xml file.

/hgc:metadata/hgc:sizeUncompressed

The size of the non-compressed xml data file in bytes

/hgc:metadata/hgc:sizeCompressed

The size of the compressed xml data file in bytes.

/xenc:EncryptedKey

The `<xenc:EncryptedKey>` element contains a dynamically generated symmetric key (AES256), with which the data file is asymmetrically encrypted, using the Authority's public key (X.509 certificate), according to the W3C XML Encryption standard. The element also contains an ID for the identification of the symmetric key `<xenc: CarriedKeyName>`.

According to the W3C XML Encryption standard, the structure of the specific element must be as follows:

```
<xenc:EncryptedKey Id="NameOfRegulator" xmlns="http://www.w3.org/2001/04/xmlenc#">
  <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
  <dsig:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <dsig:X509Data>
      <dsig:X509SubjectName>CN=Regulator,
      OU=Authority</dsig:X509SubjectName>
    </dsig:X509Data>
  </dsig:KeyInfo>
  <xenc:CipherData>
    <CipherValue>xyzi...rO+abc</CipherValue>
  </xenc:CipherData>
  <xenc:CarriedKeyName>K20</xenc:CarriedKeyName>
</xenc:EncryptedKey>
```

In the event that there are more X.509 encryption certifications of the supervisory authority/authorities, then more `<xenc:EncryptedKey>` elements must be generated, which will contain the same symmetric key and name, but will reference of the Authority's public key (X.509 encryption certification) (ds:X509SubjectName). An identifier will be set for the supervisory authority for which this element is generated as an ID of the `<xenc:EncryptedKey>` element. The ID will be communicated to the Licence Holder by the Authority.

As name for the identification of the symmetric key `<xenc: CarriedKeyName>` , the sequence number of the control file is used (e.g., 20), adding the prefix K (Key).

/xenc:EncryptedData

This element represents the report in the encrypted data, according to the XML Encryption standard. It contains the encryption algorithm (AES256) and the internal report to the symmetric key, through its name `<xenc: CarriedKeyName>`.

The reference to the encrypted data shall be expressed via a URL formed as follows:

- The URL of the zip file. The path corresponds to the tree structure of the Safe's folders. For Example: `<licenseholderid>_<serverid>_<seqno>_<YYYYMMDD>_<hhmmss>.zip`
- The path of the compressed and encrypted data.bin file, within the zip file. For example:

/data.bin

An ID shall be added to the final element <xenc:EncryptedData>, based on which the chaining of consecutive patches (chaining) shall be implemented, as illustrated below in the < dsig:manifest >description.

Consequently, the <xenc:EncryptedData>element will have the following structure:

```
<xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="D20">
  <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
  <dsig:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <dsig:KeyName>K20</dsig:KeyName>
  </dsig:KeyInfo>
  <xenc:CipherData>
    <xenc:CipherReference
      URI="/<licenseholderid>/2019/01/01/<licenseholderid>_abc15_20_20190101_155502.zip/
      data.bin"/>
    </xenc:CipherData>
</xenc:EncryptedData>
```

In the aforementioned example, the identification of the <xenc:EncryptedData> element (ID='D20') derives from the sequence number of batch (20), with the addition of prefix D (Data), due to the fact that reference is made to the data batch.

If reference has to be made in a control file, the sequence number of the control file is used (20), adding the prefix C (Control).

/dsig:manifest

To chain consecutive batches together, the <dsig:Manifest> element is used. This element derives from the XadES (XMLDSIG) standard. It contains two references to the data (current and previous batch), including their corresponding hash values.

The structure of this element summarised as follows:

- c) It contains a reference to the corresponding <dsig:Manifest> element of the zip batch previously generated, including the hash value of the xml data file generated on the basis of previously canonicalised xml data file (Exclusive XML Canonicalisation [XML-C14N] specification).

The reference to the encrypted data batch shall be made through a URL formed as follows:

- i. The URL of the previous zip file. The path shall correspond to the tree structure of the Safe's files, as defined in section 23.4.4.

For example:

<licenseholderid>_<serverid>_<seqno>_<YYYYMMDD>_<hhmmss>.zip

- ii. The path of the xml manifest within the previous zip file.

For example:

/manifest.xml

- iii. The reference to the ID of the <dsig:Manifest> element of the previous zip batch (<dsig:Manifest id='PreviousID'>). For example:

#<Id>

- d) It shall contain a reference to the <xenc:EncryptedData> element of the current control file, including the hash value of the xml data file generated based on the current canonicalised xml data file (Exclusive XML Canonicalisation [XML-C14N] specification). The hash value is generated from the non-encrypted and uncompressed xml data file.

Then, the conversion rules (decryption, decompression) that must be applied in order to verify the hash value of a data batch must be reported.

Consequently, the <dsig:Manifest>element will have the following structure:

```
<dsig:Manifest Id="C20">
  <dsig:ReferenceURI="/<licenseholderid>/2019/01/01/
  <licenseholderid>_abc15_19_20190101_145500/manifest.xml#C19">
    <dsig:Transforms>
      <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    </dsig:Transforms>
    <dsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
    <dsig:DigestValue>PreviousHashValue</dsig:DigestValue>
  </dsig:Reference>

  <dsig:Reference URI="#D20">
    <dsig:Transforms>
      <dsig:Transform Algorithm="Decryption algorithm"/>
      <dsig:Transform Algorithm="Decompress algorithm"/>
    </dsig:Transforms>
    <dsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
    <dsig:DigestValue>CurrentHashValue</dsig:DigestValue>
  </dsig:Reference>
</dsig:Manifest>
```

/dsig:Signature

This is the element that contains the digital signature of the data batch. A digital signature shall be added as an enveloped signature, according to the XAdES standard, including time-stamping (XAdES-T standard).

Chapter 8. IT Infrastructure Security

Article 24

Security of Online Gaming Systems and Subsystems

24.1 General Requirements

The security standards laid down by the HGC with regard to all the systems/subsystems and software used for conducting of online Gaming (CIS) are those described in the international certification standard ISO/IEC 27001, at least in the 2013 version.

By adopting the aforementioned standard, the HGC aims at mitigating the exposure of players to safety risks from the online gaming systems/subsystems and software. The systems/subsystems which the Licence Holder is obliged to certify the Central Information System (CIS) (including the Intermediate Control System) under ISO/IEC 27001 are:

In this context, the Licence Holder shall have the following obligations:

- a) No later than two (2) months after the issuance of the licence, the Licence Holder must submit to the Authority a technical security report, presenting all safety certificates the aforementioned systems/subsystems have, as well as a specific report on IT security measures applicable for them. The technical security report must be produced according to Appendix A of the ISO/IEC 27001:2013 certification standard, by independent and appropriate auditing bodies/companies, in accordance with the Regulation. The adequacy and transparency of the check must be documented in the Security Technical Report as well as the methodology of the check, the results and their documentation, and the Licence Holder's actions concerning any findings must be reported. The structure of this report is described in the section entitled 'Structure of the Security Technical Report', which follows. The report must be accompanied by a written confirmation from the contractor who will undertake the development and implementation of the information security management system according to ISO/IEC 27001, stating that the Licence Holder has initiated the procedures necessary in order to obtain ISO/IEC 27001 certification.
- b) The Licence Holder must submit the ISO 27001 certificate to the Authority no later than eighteen (18) months after the issuance of the licence.
- c) At least every eighteen (18) months from the date of the Licence Holder's certification under ISO 27001, the Licence Holder is obliged to submit its systems and subsystems (CIS) and the Intermediate Control System to a fresh security audit and also submit the relevant Technical Security Report to the Authority.
- d) In any event, upon expiry of the ISO 27001 certificate, the Licence Holder must promptly take action to renew it and to submit the new certificate to the Authority.
- e) The Licence Holder must have an appropriately staffed Information Security Organisational Unit for the management and control of the information security system, with employees who have the necessary certificates of competence [examples include: ISO 27001 lead auditor certification, certified information security manager (CISM), certified information system auditor (CISA)]. The Licence Holder's information security system procedures shall be reviewed at least on an annual basis. No later than two (2) months upon conducting Games, the Licence Holder shall submit a relevant report to the HGC documenting all mentioned above.

- f) The CIS and the Intermediate Control System must be subject to penetration testing at least once a year and a vulnerability scan at least once every six months. The results of the aforementioned tests must be forwarded directly to the Authority by each Certification Body (test lab), in accordance with the Regulation. The aforementioned procedures and tests shall be defined by relevant HGC Instructions. No later than two (2) months upon conducting Games, the CIS and the Intermediate Control System (provided that the latter operates productively) shall be for the first time subject to penetration testing and a vulnerability scan by the Licence Holder.

24.2 Security and Operation Specifications for the System/Subsystem hosting Data Centers

All systems and subsystems which constitute the overall architecture of the system (CIS, Safe and other subsystems of the Intermediate Control System, alternate storage site) must be hosted at data center infrastructures, that have powerful operation features in terms of the availability of services provided, security and resilience against catastrophic events, and business continuity.

The data centers must have the operation features which classify them at least at Tier 3 level, based on the classification of TIA 942 standard, or equivalent.

24.3 Structure of the Technical Report on the Safety of Systems and Subsystems

The Technical Report on the Safety of Systems and Subsystems for online Gaming must include:

- a) The details of the audited Licence Holder;
- b) The details of the auditing body/company and its experience in such audits;
- c) The date(s) the audit was carried out;
- d) The business profile of the audited Licence Holder, its business model and its Gaming activities;
- e) Information of other companies that may participate, directly or indirectly, with systems or software, in the conduct of Gaming by the Licence Holder;
- f) The Licence Holder's sites that the auditing body/company visited for carrying out the audit;
- g) The standard based on which the audit was carried out, i.e. ISO/IEC 27001: 2013;
- h) The executive summary of the audit, which contains a concise presentation of the auditing work, its results along with the opinion of the auditing body/company concerning the level of security of the Licence Holder's systems and software, per audit sector (according to the ISO/IEC 27001: 2013 standard);
- i) The scope of the audit (audit areas: gaming applications/systems, networks, databases, operating systems, interfaces), as well as a detailed listing of the audited systems and software;
- j) The methodology and the processes followed for conducting the audit (e.g. questionnaires, reports, comments on parameters and results), per audit area, as well as the audited system/ software;
- k) The persons involved in the audit and their capacity/role in the audited company, per audit area and audited system/software;
- l) The policies and processes audited, such as:
 - i. Information systems security policy
 - ii. User access policy

- iii. Application development and testing policy
 - iv. Service Level Agreements (SLAs)
 - v. Network services policy
 - vi. Policy on tracking, prevention and restoration for protection against malicious coding
 - vii. Data backup generation policy
 - viii. Safe data destruction policy
 - ix. Information storing policy (for the protection of information from non-authorised and/or malicious use)
 - x. Change management policy
 - xi. Policy on monitoring facilities that accommodate information systems
 - xii. Use of encrypted audits policy
 - xiii. Network diagram
- m) The results of the audit, per audit area and audited system/software, categorised as follows:
- i. Full Compliance
 - ii. Compliance with Comments (there is room to improve the safety procedures/measures).
 - iii. Non-compliance – Low Risk (actions must be implemented, within a specific time period, to mitigate Risk, without pausing the Licence Holder's operations)
 - iv. Non-compliance – High Risk (actions must be implemented, within a specific time period, to mitigate Risk, with parallel pause of the Licence Holder's operations)
- n) The evidence gathered from the audit process for the justification of the audit results (e.g. documents and reports examined, interventions carried out, the samples examined to verify compliance, etc.)
- o) The Provider's actions/management plan to solve matters detected during the audit
- p) Other audit-related factors (e.g. other certifications)

Chapter 9. Random Number Generator

Article 25

Random Number Generator characteristics

25.1 Random Number Generator General Requirements

The random number generator (RNG) must be cryptographically strong at the time of submission. Where more than one instance of a random number generator is used in the CIS, each instance must be separately evaluated and certified. Where each instance is identical, but involves a different implementation within a Game/application, each implementation must also be separately evaluated and certified. Analysis of the data and of the source code identification must demonstrate that any outcomes from the random number generator used in determining the symbol/outcome of the Game:

- a) are statistically independent;
- b) are fairly distributed (within statistically expected bounds) over their range;
- c) have passed various recognised statistical tests; and
- d) are cryptographically strong.

25.2 Applied Tests

The independent certification laboratory/test laboratory may use various recognized tests to determine whether or not the random values produced by the random number generator successfully pass the desired 99% confidence level. These tests may include, but are not limited to:

- a) Chi-square test;
- b) Equi-distribution (frequency) test;
- c) Gap test;
- d) Overlaps test;
- e) Poker test;
- f) Coupon collector's test;
- g) Permutation test;
- h) Kolmogorov-Smirnov test;
- i) Agency criterion test;
- j) Order statistic test;
- k) Runs tests (patterns of occurrences should not be recurrent);
- l) Interplay correlation test;
- m) Serial correlation test potency and degree of serial correlation (outcomes must be independent of the previous Game);
- n) Tests on sequences; and
- o) Poisson distribution.

NOTE: The independent certification laboratory/test laboratory shall choose the appropriate tests on a case-

by-case basis, depending on the RNG under view.

25.3 Scaling

The scaling method shall not compromise the cryptographic strength of the random number generator. Furthermore, the scaling method shall safeguard the distribution of the scaled values. For example, if a 32-bit random number generator with a range of all the set of integers in the closed interval $[0, 2^{32}-1]$ were to be scaled to the range of the set of integers in the closed interval $[1,6]$, so that the scaled values can be used to simulate the roll of a standard six-sided die, then each integer in the scaled range should theoretically appear with equal frequency.

In the example given, if the theoretical frequency for each value is not equal, then the scaling method is considered to have a bias. Consequently, a compliant scaling method shall have a bias equal to zero.

25.4 Hardware-based Random Number Generator

Because of their physical nature, the performance of hardware-based random number generators may deteriorate over time. The failure of a hardware-based RNG could have serious consequences for the Game/application, as Games may become predictable or exhibit non-fair distribution. Therefore, if a hardware-based RNG is used, there must be a dynamic/active, real-time tracking of the output with a sample size large enough to allow for reasonably high statistically powerful testing, so that game play is disabled when an output testing failure is detected.

25.5 Software-based Random Number Generator

The following requirements apply only to software-based random number generators.

25.5.1 Period

The period of the RNG, in conjunction with the methods of implementing the RNG outcomes, must be sufficiently large to ensure that all independent outcome combinations/permutations are possible for the given Games/applications.

25.5.2 Seeding/Re-Seeding

The Seeding/Re-seeding methods must ensure that all seed values used to start or initialise the random number generator are determined in such a way as not to compromise the cryptographic security of the random number generator.

25.5.3 Background Cycling/Activity

To ensure that the RNG outcomes cannot be predicted, appropriate background activity must be implemented between Games. Wherever a game outcome consists of multiple mapped RNG values, background activity must be implemented for the whole duration of the Game (i.e. between the selection of each mapped RNG value) to ensure that the game outcome does not consist of sequential mapped RNG outcomes. The rate of background activity must be sufficiently random, without intervention, so as to prevent prediction.

Chapter 10. Progressive Jackpot

Article 26

Progressive Jackpot requirements

26.1 Introduction

A Progressive Jackpot is a progressively increasing prize based on a function of credits that are bet or won. This includes prizes awarded based on criteria other than obtaining winning outcomes in the Game, such as 'Mystery Jackpots'. However, this does not include non-configurable, increasing prizes resulting from bonus features, which are part of the Game payable (Theoretical %RTP).

26.2 Progressive Jackpot Design and Operation

26.2.1 Progressive Jackpot Fairness

For a Progressive Jackpot the following rules must apply:

- a) All Players playing Progressive Jackpot Games must be made aware of the actions which would make them eligible to win the Progressive Jackpot.
 - b) Where Progressive Jackpot contributions form part of the RTP % calculation, the contributions must not be assimilated into revenue. If a Participation cap is established on any Progressive Jackpot, all additional contributions once that cap has been reached are to be credited to a diversion pool. The minimum return to Player must be achieved regardless of the number of betting units calculated.
 - c) The rules of the Game must incorporate how the Progressive Jackpot is funded and determined.
 - d) If a minimum bet amount exists, in order for a Player to win a Progressive Jackpot, the base Game (excluding the Progressive Jackpot) must meet the minimum Player return.
 - e) The current Progressive Jackpot amount should be displayed on all Player devices participating in the Progressive Jackpot. This display should be updated on all participating Player devices, at least every 30 seconds.
- NOTE: It is accepted that, depending on the medium, communication delays differ and are beyond the Licence Holder's knowledge or control. Server-to-client delays will vary from Player to Player and from message to message.
- (f) The rules of the Game must inform the players of the imperfections of the communications medium for the Game, and how this affects them.
 - (g) The rules of the Game must inform the players about any maximum awards and/or time limits that may exist for each Progressive Jackpot.
 - (h) For Progressive Jackpots offering multiple levels of awards, the Player must always be paid the highest amount, if a particular combination is won which triggers the highest paying award. This may occur when a winning combination may be evaluated as more than one of the available payable combinations (i.e., a Flush is a form of a Straight Flush and a Straight Flush is a form of Royal Flush). Therefore, there may be cases where the Progressive Jackpot levels shall be swapped to ensure that the Player is being awarded the highest possible value based on all combinations that may define the outcome.
 - (i) In the event that multiple Progressive Jackpots occur at approximately the same time and there is no way to know which jackpot occurred first, it must be ensured that these hits are considered to be simultaneous wins. Payments of awards for simultaneous wins must be carried out according to the rules of

the Game. The rules of the Game shall include information which addresses this situation.

26.2.2 Slave Progressive Jackpot Controllers

Where a 'Master Controller' uses 'Slave Controllers' to control a Progressive Jackpot, the following requirements shall apply:

- a) All 'Slave Controllers' must be time synchronised with the 'Master Controller'.
- b) The 'Master Controller' must be time synchronised with the CIS.
- c) Progressive Jackpot win events must be time-stamped and the Progressive Jackpot Controller must ensure that hits registered within a minimum time increment are considered to be simultaneous wins. Prize payout for simultaneous wins must be carried out in accordance with the rules of the Game.
- d) The minimum time 'window' (Progressive Jackpot Reset Period) must not be less than the longest time period required to:
 - i) Register that a Progressive Jackpot has been won;
 - ii) Announce the win on the displays of all participating Player devices with active sessions; and
 - iii) Reset the Progressive Jackpot meters.
- e) If supporting a progressive jackpot that is determined by increments of individual players wagers, the processing of receipt of increments from all Player devices, whether they are connected to the Master or Slave controllers, must be fair.

26.2.3 Progressive Jackpot Win Notification

The following requirements must be met when there is a jackpot win:

- (a) A winning Player must be notified of a Progressive Jackpot win by the end of the game in play;
- (b) All Players participating in the Progressive Jackpot must be notified that a Progressive Jackpot has been won at the time of the jackpot win; and
- (c) the Progressive Jackpot amount must be displayed on all Player devices participating in the jackpot at the time of the progressive jackpot win.

26.2.4 Progressive Jackpot Parameter Changes

The following requirements shall apply to configuring progressive jackpots:

- a) Once a Progressive Jackpot has started, any parameter changes must come take effect after the current Progressive Jackpot is won. These are 'pending' parameters.
- b) A Mystery Progressive Jackpot that uses a Hidden Progressive Jackpot amount in order to determine the Progressive Jackpot win must not change the Hidden Progressive Jackpot amount when the parameters change, if the Progressive Jackpot is active (i.e. had any Progressive Jackpot contributions are added to it).
- c) The CIS must provide a means of displaying current and pending Progressive Jackpot parameters.
- d) The CIS must record the values of all Progressive Jackpot meters, as well as all 'current' or 'pending' Progressive Jackpots parameters.

26.2.5 Partial Progressive Jackpot Redirection

Diversion Pool schemes where a portion of the Progressive Jackpot contributions are redirected to another pool, so that when the Progressive Jackpot is won, the diversion pool is added to the seed amount of the next Progressive Jackpot, are acceptable.

26.2.6 Progressive Jackpot Shutdown

In cases where a Progressive Jackpot has to be shut down (e.g. malfunction, loss of connectivity, unexpected termination), the following requirements shall apply:

- a) Players must be given a clear indication that the Progressive Jackpot is not operating (e.g. by displaying 'jackpot closed' on Player Devices);
- b) It must not be possible for the Progressive Jackpot to be won while in the shutdown state;
- c) If the Progressive Jackpot operates in conjunction with another Game (e.g. base game) and the Player return requirement is only met when Progressive Jackpot contributions are included, the other Game may only be offered when the Progressive Jackpot is available;
- d) Activation of the Progressive Jackpot from the shutdown state must return the Progressive Jackpot with the identical parameters including Progressive Jackpot value, and hidden win amount for Mystery Progressive Jackpot, as before the shutdown.

26.2.7 Progressive Jackpot Recovery

To enable recovery of the current value of the Progressive Jackpot amounts in the event of a CIS or Progressive Jackpot controller failure, either:

- (a) The current value of the Progressive Jackpot amount must be stored in at least two physically separate devices, or
- (b) The current value of the Progressive Jackpot amount must be able to be accurately calculated from other available metering information, which shall not be stored in the same CIS subsystem as the Progressive Jackpot amount.

In either case, all eligible Progressive Jackpot winners must be paid as soon as the value is recovered.

2. This decision shall enter into force as of its publication in the Government Gazette.

This Decision shall be published in the Government Gazette.

Athens, 24 July 2020