Governance of games of skill with remote participation

Decree of the Director General of the Autonomous Administration of State Monopolies (AAMS) on the 5th day of February 2010 published under G.U. n. 68 on the 23rd day of March 2010

Guidelines for the certification of gaming platforms

May 13, 2010

CONTENTS

INTRODUCTION

To request the authorization to deploy the games described in article 1(1) and 1(2), of the Decree of the Director General of the Amministrazione Autonoma dei Monopoli di Stato (AAMS) of the 5th day of February 2010 published under G.U. n. 68 on the 23rd day of March 2010, "Governance of games of skill and games of chance with fixed odds and non tournament card games with remote participation – hereinafter referred to as Decree - the concessionaire must forward to AAMS an application, including the design of the Remote Gaming System (RGS) and the game applications, as well as the related certification supplied by an Accredited Testing Facility (ATF).

The certification must be requested directly by the concessionaire from an ATF recognized by AAMS. The updated list of such facilities is maintained by the Administration and can be consulted on the website at http://www.aams.gov.it.

The ATF will supply the concessionaire with the outcome of the compliance evaluation performed on the technical solutions implemented in the gaming system, divided as follows:

- The analysis and certification of the gaming platform;
- The analysis and validation of the software source code which implements the algorithm used for random number generation;
- The execution of a series of statistical tests, the analysis of the results and the certification of the randomness of the random number sequences produced by the generator;
- The analysis and verification of the source code which implements the game software, as well as the emulation of all phases and possible results of the same.

Subsequent modifications of the essential characteristics of both the platform design and the game application, are subject to the prior approval of AAMS and possible renewal of the certification.

The technical testing required to issue the certification is described in the following Guidelines.

Please note that these Guidelines can be used only to certify platforms that offer games of skill with remote participation to the players.

Where the concessionaire uses technologies or platforms developed by a third party, it is nevertheless the responsibility of the concessionaire to ensure that each of the solutions adopted for each component of the gaming system is certified by the ATF, and therefore the relevant certification must be requested.

All costs related to the certification of the RGS and its subsequent maintenance are to be borne by the concessionaire.

The certification issued by the ATF does not in any way substitute for the authorization issued by AAMS at the end of the process, which concludes with the granting of the licence /concession which is the only title needed to operate remote games of skill.

The following Guidelines are stated in two parts:

- The description of the operational arrangements which the concessionaire must follow in order to obtain the compliance certificate from the responsible ATF;

- The technical requirements which the gaming platform must satisfy in order to be certified.

The gaming platform to undergo certification must be equipped with at least one game application on which the testing can be conducted.

It is within the authority of AAMS to update the present Guidelines if necessary, in order to take into account any developments in technology, changes to the legislative framework and testing methods.

Note: AAMS reserves the right to modify (or selectively apply) the requirements set forth in the following Guidelines as deemed necessary to ensure the integrity of gaming in the national territory. However, in order to ensure a consistent approach to enforcement, AAMS will not modify or selectively apply the requirements set forth in these Guidelines without first providing reasonable prior written notice to any other relevant bodies, on an as-needed and case-by-case basis.

These guidelines were drafted by examining and using parts of similar guidelines in force in other jurisdictions with an aim to:

a) Eliminate subjective criteria in analysing and certifying RGS operation;

b) Test those criteria which impact the credibility and integrity of RGS operation from the point of view of both the Player and AAMS;

c) Develop Guidelines that will ensure the honest, secure, auditable and correct operation of RGSs;

d) Establish that the testing of the communication protocol between the RGS and the centralised system of AAMS is not the responsibility of the ATF;

e) Recognise that non-gaming testing (such as EMC or LVD) should not be incorporated into these Guidelines but left to appropriate test laboratories that specialise in that type of testing;

f) To recognise that, except where specifically identified in these Guidelines, testing is not directed at health or safety matters, which fall instead under the responsibility of the owner of the gaming system;

g) Develop Guidelines that can be easily modified to allow for the introduction of new technologies or functionality;

h) Develop Guidelines that do not specify any particular method or technology for any element or component of an RGS. The intent is instead to allow the use of a wide range of methods and technologies and to encourage at the same time the development of new methods and technologies.

This document should not be construed to be a limitation on the use of future technologies; and the fact that it makes no mention of a given technology does not mean that such technology should be considered to be not permitted.

1. REQUIREMENTS FOR REQUESTING THE CERTIFICATION OF GAMING PLATFORMS

This section describes the process which the concessionaire will have to follow in order to secure the compliance testing of the gaming platform against the requirements laid out in this document, and the documentation which will have to be presented to the ATF.

Where the information has not been submitted or is not otherwise in the possession of the ATF, the concessionaire shall be asked to supply additional information, otherwise the total or partial refusal of an application together with testing delays may occur.

Where the concessionaire requests the certification of a gaming platform or part of it, previously subject to the approval of an ATF, it will in the certification request explicitly refer to the previous compliance testing process, producing documentary evidence of previous testing.

1.1 REQUEST FOR THE CERTIFICATION OF GAMING PLATFORMS IN JOINT VENTURE

For the purpose of these Guidelines, an RGS is considered a *Joint Venture* when two or more parties are involved in the production of the system.

Note: The above definition does not coincide with the legal definition of the term "joint venture". Due to the increasing number of joint ventures presented (with more than one party involved in the presentation of a product) and to avoid the risk of confusing said parties, for each presentation the following procedures must be observed .

The concessionaire is responsible for the preparation and the forwarding of the entire presentation and documentation requested, even in cases where components provided by other parties are used, and must identify all the components of the gaming system. This party constitutes the *principal representative* for the certification request.

If some components of a gaming platform have been previously certified by the same ATF, it will be the responsibility of the concessionaire to produce the documentary evidence needed to recognise the previous testing.

The party which presents the approval request must do so on its own letterhead. The ATF can direct all costs incurred during the entire testing and approval process to all the associated subjects in proportion to the testing carried out on the different components of the system in question.

The primary representative will be the contact in case of doubt. In any case the concessionaire will work with all of the parties involved until the completion of the evaluation.

Where a party would like to bind the ATF to confidentiality regarding the nature of the information dealt with (such as, for example, the review of the source code), it will be the responsibility of said party to stipulate a confidentiality agreement (NDA – Non-disclosure agreement) with the ATF. The information discussed within said confidentiality contract will not be disclosed by the ATF to other parties of the joint venture, but could be revealed by the ATF to the AAMS.

Once the procedure is complete, the ATF will release the documentation related to the certification to the principal representative.

The principal representative can then release copies of the approval documentation to any associated parties.

1.2 REQUEST FOR THE CERTIFICATION OF GAMING PLATFORMS

The *Request for the Certification of Gaming Platforms* means the request for the certification of a particular RGS for which the concessionaire has never previously requested certification.

In the case of *Modifications to previous requests,* including required changes to a previously completed certification of an RGS, whether previously approved or pending approval, please refer to *1.3 Request for the certification of modifications to a previously certified component of a gaming platform*.

Note: The compliance testing against the requirements in these Guidelines can take place at the concessionaire's facilities, at the ATF or both.

The request for certification of the gaming platform shall consist of a letter of introduction and a series of documents each related to a component of the platform itself, to be presented according to the following regulations:

1.2.1 LETTER OF INTRODUCTION

The request for certification must be accompanied by a letter of introduction on company letterhead forwarded to the ATF. The letter will include the following information:

a) A formal request for certification specifying that the RGS will be operated in the Italian jurisdiction;

b) The gaming platform for which certification is requested:

   i. In the case of software, the submitting party shall include the name of the manufacturer, supplier and identification files and revision numbers, if applicable.

   ii. In the case of hardware, the submitting party shall indicate the manufacturer, supplier, model number(s), part number(s) and revision number(s) of the associated components of hardware;

c) The details of where each component of the platform is located within the European economic space

d) A contact person who will serve as the main point of contact for technical questions raised during evaluation of the submission. This may be either the person who signed the letter or another specified contact.

1.2.2 PRESENTATION OF THE GAMING PLATFORM

'*Gaming Platform*' refers to the RGS software and hardware which drives the features common to all of the games, and which forms the primary interface to the RGS for both the player and the concessionaire:

a) The Gaming Platform provides the player with the means to register an account, modify their account information, open or close their own account, deposit and withdraw funds to / from their account and request account activity statements / reports. In addition, any web pages displayed to the player that relate to gaming offered on the RGS (excluding advertising), but are not an actual game screen;

b) The Gaming Platform provides the concessionaire with the means to review player accounts, enable / disable games, generate various gaming / financial

transaction and account reports, input game outcomes, enable / disable player accounts and set any configurable parameters.

The following paragraphs outline the submission requirements for a gaming platform.

1.2.2.1 Source Code

For the verification of the Gaming Platform the ATF reserves the right to possibly request to examine all the parts of the source code necessary to complete the tests described in these Guidelines. The source code under verification will be reviewed by the ATF in a secure, controlled, and supervised manner that is agreeable to the concessionaire, the ATF and the software vendor.

All submitted gaming platform source code shall contain, at least, the following information:

i) File / module / function name(s);

ii) Brief description of file / module / function purpose(s); and

iii) Edit History, including who modified it, when and why.

All submitted gaming platform source code shall be commented in an informative and useful manner.

All submitted gaming platform source code shall be correct, complete and able to be compiled.

Where necessary, the ATF must be provided with the necessary instruments for the compilation of the source code.

At the end of the verification process, ATF will send to AAMS the digest messages of each verified file/module/function.

1.2.2.2 Remote access console

For the RGS verification, it is necessary to supply – at the time of acceptance of the submission by the ATF – a system of remote access to each component of the RGS that is being verified, without time limits and with the administrator's privileges of the host appliance.

Said remote access must be available to the ATF at its facilities without the need to install additional equipment. The concessionaire who presents the submission must supply the complete documentation of the credentials to be used and of the modalities for remote access.

1.2.2.3 Documentation

The following documentation must be submitted for the gaming platform:

a) An all-inclusive functional description of the gaming platform (including website home page and all website peripheral pages),

b) Detailed functional descriptions of the following processes:

   i. Player Account Registration;

ii. Player Account Login (Username & Password);

iii. Player Interface to Player Account;

iv. Session management including the solution of possible problems (accidental disconnection, accidental browser or client shutdown,...);

v. Operator Interface to Player Account;

vi. RGS Accounting and Financial Reporting Capabilities;

vii. Player Protection / Exclusion Systems;

viii. RGS Payment Systems & Financial Institution Interfacing;

ix. Player Location & Identity Verification Software; and

x. Player Account Deactivation.

1.2.3 PRESENTATION OF THE GAMES

The request for RGS certification must include the presentation of at least one game and the complete list of all games to which the player can have access.

"Games" refers to RGS software which is specific to each individual game that is hosted / offered on the gaming platform. Each game is to be treated as a separate and distinct entity.

Any information and materials required to be submitted with respect to the games (as outlined herein) must be submitted for each individual game hosted / offered on the gaming platform.

If the games hosted / offered on the gaming platform belong to the same family of games (see Glossary), their common aspects shall be described once whereas the features of each game shall be described individually.

The following paragraphs outline the submission requirements for the games.

1.2.3.1 Source Code

The following requirements apply to all game source code submitted to the ATF for verification:

a) All game source code shall be provided to the ATF so that it can be examined in a secure manner in its own premises;

b) All submitted game source code shall contain at least the following information:

   i. File / module / function name(s);

   ii. Brief description of file / module / function purpose(s); and

   iii. Edit History, including who modified it, when and why.

c) All submitted game source code shall be shall be accompanied by explanatory technical documentation;

d) All submitted game source code shall be correct, complete and able to be compiled.

e) The ATF should be supplied with all tools necessary for the compilation of the source code.

1.2.3.2 Documentation

The following documentation must be submitted for each individual game hosted / offered on the gaming platform:

a) Game name;

b) Game version number(s);

c) Detailed game rules, including all options and bonus features;

d) A formal treatise of the derivation of the Percentage Return to Player (%RTP).

1.2.3.3 Emulation Capacity

The purpose of 'Emulation Capacity' is to facilitate the testing process.

Emulation Capacity is a mode of game operation that is alternative to the real mode (i.e.: to be activated and operated in the test environment only) whereby the tester verifies the critical game phases and simulates the critical winning combinations.

1.2.4 PRESENTATION OF THE RANDOM NUMBER GENERATOR (RNG)

'RNG' refers to RGS software and / or hardware component which generates random numbers used to generate the game symbols for each game on the gaming platform.

The following sections outline the submission requirements for an RNG.

1.2.4.1 Source Code

The following requirements apply to all submitted RNG source code:

a) All RNG source code shall be handed over to the AFT so that it can be examined in a secure manner in its own premises;

b) All submitted RNG source code shall contain at least the following information:

   i) File / module / function name(s);

   ii) Brief description of file / module / function purpose(s); and

   iii) Edit History, including who modified it, when and why.

c) All submitted RNG source code shall be accompanied by explanatory technical documentation;

d) All submitted RNG source code shall be correct, complete and able to be compiled.

Furthermore the ATF must be provided with:

e) necessary instruments for the compilation of the source code.

f) an instrument for the rapid extraction of a sufficiently large sample of random numbers to permit a statistical analysis of their distribution.

1.2.4.2 Documentation

The following documentation must be submitted for the RNG:

a) A list of all games connected to the RNG (including the associated mathematical Degrees of Freedom (DOFs) for each game);

b) For hardware-based RNGs:

   i) Type of hardware device used;

   ii) Technical specifications for hardware device;

   iii) Methods of connecting hardware device to RGS software; and

   iv) Details of all RNG / game implementation, including methods of scaling and mapping.

c) For software-based RNGs:

   i) Type of mathematical algorithm used;

   ii) Full details, in technical terms, of random number generation process and mathematical algorithm theory;

   iii) Details of the mathematical algorithm's period;

   iv) Details of the mathematical algorithm's range;

   v) Details of the methods for seeding;

   vi) Details of the methods for background cycling / activity, and

   vii) Details of all RNG / game implementation, including methods of scaling and mapping.

1.2.5 PRESENTATION OF THE INFORMATION SYSTEMS SECURITY (ISS)

'ISS' refers to the Administrative Controls, Technical Controls and Physical & Environment Controls necessary for the secure, safe and auditable operation of the RGS.

System overview diagrams and schematics that describe the basic architecture and typology of the RGS, and how that computer network is interconnected, must be submitted for the ISS. This documentation should include (but not necessarily be limited to) details of each of the following – where applicable:

a) Firewalls and Intrusion Detection Systems (IDS);

b) Servers and Operating Systems (OS);

c) Infrastructure and source code vulnerability assessment;

d) Hubs, Switches and Routers;

e) Relevant Internet Protocol (IP) Addresses;

f) Gateway and Access Points;

g) Application Entry Points and Web Forms (for application security);

h) Local Area Network (LAN) and Virtual Local Area Network (VLAN); and

i) All Documented Security Policies and Procedures.

1.3 REQUEST FOR THE CERTIFICATION OF MODIFICATIONS TO A PREVIOUSLY CERTIFIED COMPONENT OF A GAMING PLATFORM

In the case of modifications to the RGS or to one of its components, including the variations to a gaming platform certification previously completed, whether previously approved or pending approval, a partial request must be presented as described below.

The partial request is used even in the case where at their sole discretion, AAMS decides to submit under review and successive testing the presentation of updates (i.e.: revisions to existing hardware, software or control systems that are currently under review, certified or have been reviewed and not certified), to verify compliance with the applicable requirements set forth in these Guidelines.

In cases where AAMS deems necessary, in addition to the requirements in *1.2.1 Letter of Introduction*, the following information will be requested in order to establish the nature of the updates:

1.3.1 PRESENTATION OF GAMING PLATFORM UPDATES OR MODIFICATIONS

The presentation of a gaming platform's updates or modifications must include a detailed description of the software change(s) and module(s) affected, from both a functional perspective and a source code perspective, as well as the updated source code package for the RGS that shall undergo verification.

Where applicable, updated gaming platform functional specification documents (see Paragraph *1.2.2.3*) must also be submitted.

1.3.2 PRESENTATION OF UPDATES OR MODIFICATIONS OF A GAME

The presentation of a game's updates or modifications must include a detailed description of the software change(s) and module(s) affected, from both a functional perspective and a source code perspective, as well as the presentation of the entire updated source code of the game in question.

Where applicable, updated documents related to the game presentation (as per *1.2.3.2 Documentation)* must also be submitted.

1.3.3 PRESENTATION OF UPDATES OR MODIFICATIONS OF THE RNG

The presentation of RNG updates or modifications must include a detailed description of the software change(s) and module(s) affected, from both a functional perspective and a source code perspective, as well as the presentation of the entire updated source code of the RNG.

Where applicable, updated RNG design and implementation documents (as per *1.2.4.2 Documentation)* must also be submitted.

1.3.4 PRESENTATION OF UPDATES OR MODIFICATIONS OF THE ISS

The presentation of ISS updates or modifications must include a detailed description of the system change(s) and component(s) affected, as well as the reason(s) for the changes implemented by the concessionaire.

Where applicable, updated ISS design and configuration documents (as per *1.2.5 Presentation of the Information Systems Security (ISS)*) must also by submitted.

1.3.5 PRESENTATION OF THE EMERGENCY UPDATE OF THE RGS

If during the use of RGS, the concessionaire should detect hardware and/or software components malfunctions that could compromise the platform security and correct use, the concessionaire can apply the emergency update to the RGS in order to restore the system correct functioning.

Given the emergency features of the aforementioned update and to stop the detected malfunctions in time, it is possible to apply the mentioned update to the RGS before sending the update request to the ATF and the AAMS, only with regard to the hardware and/or software components that do not have direct or indirect impact on the game applications and on the RNG and its complementary elements.

Within the maximum period of time of two weeks, the concessionaire must obtain from the ATF the certification of conformity of the implemented change.

The update request must include the changed documents concerning the ISS design and configuration (see Paragraph 1.2.5).

1.4 REQUEST FOR PERIODICAL COMPLIANCE TESTING OF THE GAMING PLATFORM

For an already approved gaming platform a periodical audit of the hardware and software components as well as the RNG and the game software is foreseen every 12 months, in order to verify the complete correspondence of the system in operation with that previously evaluated and certified. For such a task the ATF must be presented with a specific request.

During the periodical compliance testing procedure, the ATF will also verify the field RTP of every game operative on the platform, through direct access to gaming data relative to the specified period.

It is the responsibility of the concessionaire to forward to AAMS the documentation related to the renewal of the certification within the established terms.

2. REQUIREMENTS APPLICABLE TO THE GAMING PLATFORM

Below are the applicable requirements that the RGS has to satisfy in order to be certified. The requirements are subdivided according to the principal components of the gaming platform

2.1 GENERAL CHARACTERISTICS OF THE RGS AND RELATIVE ARCHITECTURE

The description of the general characteristics of the RGS and of the relative techno-functional architecture has to conform with the content in paragraph '*Description of the architecture and of the structure'* of the '*Guidelines for the predisposition of the design document of the gaming platform'* (Attachment A of the decree related to the governance of skill games with remote participation and games of chance with fixed odds and non tournament card games with remote participation).

2.2 REQUIREMENTS OF THE PLAYER REGISTRATION AND REQUIREMENTS OF THE PLAYER ACCOUNT

2.2.1 AGREEMENT

1. The player's registration process must include an agreement to the terms and conditions of game play.
2. The player can only advance to games with cash prizes if they take an action to acknowledge the agreement.

2.2.2 VERIFICATION

1. To begin playing the player must hold a player account that has been validated by the concessionaire according to the current norms in effect.
2. The RGS must request the location, age, identity and tax code (Codice Fiscale) of a player before allowing them game access.
3. The RGS must allow the player to view the player account contract, conforming to the format approved by the AAMS, and must ensure said contract is explicitly accepted.
4. The RGS must have the capability to deny access to under-aged persons.
5. The RGS must have the capability to deny players, within the Italian jurisdiction, to access internet sites managed by the operator outside of the operator's limits which are defined by the license/concession released by the AAMS. In addition the technical measures adopted for the geolocalization of IP addresses of single players must be described.
6. Player access to an RGS must involve at least a user ID and password.
7. Initial passwords are set by the player; however, any subsequent password resets must be issued in a secure manner. The password has to be coded according to the current norms in effect.

2.2.3 PASSWORD RECOVERY QUESTIONS

1. Players must be asked to nominate a number of challenge questions and the relative answers at the time of registration.

2. The challenge questions must be used by the RGS (or by the help-desk staff) in the event the password or PIN is forgotten (i.e.: to identify the person requesting to access the account or change the password).

3. Challenge questions may be randomly chosen and asked at the time of log-in to further reduce the possibility of a player using an account not belonging to the registered player. This is not a requirement but a recommendation. It is suggested that the player be given the option to turn this security feature on or off.

2.2.4 UNDER AGED PERSONS

Access to the game shall not be allowed to players declared as minors.

2.2.5 CONTROLS OVER GAMES ACCESS

The RGS must not permit a person to participate as a player in a game with cash prizes, unless the person is registered as a player.

2.2.6 PLAYER ACCOUNT

1. A player must only be permitted to have one active account per concessionaire.

2. A new account for a person must not be created if the reason for the deactivation of a previous account indicates that the person must not be permitted to establish another account.

3. Player accounts must be protected against forms of illicit access or removal. This includes internal access by the Operator's staff and external access by malicious users or other unauthorized parties.

4. Withdraws from a player's account on the RGS must be paid according to the current norms in effect.

5. Any funds left in a player's account that is to be de-activated are to be remitted in the name of the owner of the account.

2.2.7 SECURITY

1. The RGS must employ:

   1.1. Automatic verification procedures - which are triggered at a minimum on a daily basis - of the integrity of the critical files determined by the ATF during the verification, related to the software installed on every component of the system, including the software of each game application and sending to the control system of digest messages of each verified file/module/function.

   1.2. The execution of blocking procedures triggered by events that signal the malfunctioning and/or the attempted tampering of any component of the RGS.

2.2.8 USER INACTIVITY TIMEOUT

1. Unless the RGS is capable of 'polling' to confirm user connections, it must implement a 15 minute user inactivity timeout.

2. If a session is terminated due to a user inactivity timeout, the end player device must notify the player of session termination. No further game play is permitted until the RGS and the end player device establish a new session.

2.2.9 PLAYER ACTIVITY STATEMENT

1. On request by the player, a transaction report must display winnings, losses and timestamps for each play with regards to the period requested, and a summary of these details.

2. Reports must include sufficient information to allow the player to reconcile them to their own records at session level.

2.2.10 PLAYER FUNDS MAINTENANCE

1. All deposit, withdrawal or update of the game account balance transactions must be maintained in a system audit log .

2. The RGS must maintain a log of all authorisation numbers provided by the credit card issuers following approval of credit card transactions.

3. At any time the player must be able to withdraw credits from the game account according to the manners and times stated in the current norms in effect.

4. The RGS must not permit the withdrawal of funds in excess of the player's balance.

5. The RGS must not allow the concessionaire to extend credit to the player.

6. The RGS must not permit the direct transfer of funds from one game account to another.

2.2.11 GAME SESSION

1. The RGS must give the player an electronic identifier such as a digital certificate or a username and a password to establish a session.

2. A session finishes if:

    a) The player notifies the RGS that the session is finished (i.e.: logs out),

    b) A player-inactivity timeout is reached, or

    c) The operator terminates the session under approved and documented circumstances

2.2.12 UNCLAIMED FUNDS FROM INACTIVE ACCOUNTS

1. In case of unclaimed funds from inactive accounts, it is necessary to begin a documented process. An account is considered to be inactive if the player has not logged into the account for a time period of three years.

2. The RGS has to communicate to the player the condition explained in the above point.

2.3 REQUIREMENTS CONCERNING PRIVACY

2.3.1 GENERAL NORMS

1. The concessionaire must publish on its gaming platform the rules for the protection of privacy, which must be easily accessible to the player.

2.3.2 USE OF DATA

1. The concessionaire is obliged to maintain the privacy of information related to the current state of player accounts, with the exception of cases where the disclosure of such information is necessary by law.

2. The RGS must ensure that access to the information is restricted to the person supplying the information and to authorised operator and AAMS staff. This includes internal access through concessionaire's and AAMS' access control lists, and external access through username and password.

3. The concessionaire and AAMS acknowledge that they are both subject to the provisions of the current law in force and that in carrying out their respective obligations under these Guidelines, they will at all times comply with prevailing privacy legislation.

4. The concessionaire must ensure that information obtained about people's gaming habits is not used to encourage irresponsible gaming behaviour.

2.3.3 CONSENT

1. In order to complete the registration process, the player must offer consent to the privacy policy by taking an action, such as checking a box in the privacy policy, or selecting an acceptance button.

2. The default of consent shall always be NOT to accept.

3. Where data is to be used for purposes not directly related to the offering of a gaming product (including, but not necessarily limited to, the use of such data for inclusion in a mailing list), additional specific consent must be granted by the player.

4. Should the user withhold this additional specific consent this must not in itself be a ground for the operator to refuse access to the game to this person.

2.3.4 COOKIES

Where cookies are used by the RGS, the player must be informed of the usage during the registration.

2.3.5 REGULATORY USAGE

1. The privacy policies must inform the player that the concessionaire and AAMS have access to their account information.

2.4 REQUIREMENTS FOR THE PROTECTION OF THE PLAYER

2.4.1 GENERAL INFORMATION

1. The RGS website entry window must contain a clearly visible warning that gambling can be harmful if not undertaken in moderation and that minors are forbidden to play. The warning must address the issues of responsible gaming and the protection of minors.

2. The gaming platform entry window must contain a link to a web page dedicated to the player protection with the objective of responsible behaviour.

3. The player protection page must contain at least:

   a) Information about potential risks associated with gambling, and where to get help for gambling addiction;

   b) Meaningful and accurate information about games and related rules;

   c) A list of the player protection measures that can be invoked by the player, such as session limits and bet limits, and an option to enable the player to invoke those measures;

   d) A link to the terms and conditions the player agreed to be bound to by entering and playing on the site;

   e) A link to the concessionaire's privacy policy;

   f) A link to the internet website of AAMS;

   g) A clear and simple system to inform the player of the right to make a complaint against the concessionaire and to enable the player to notify AAMS of the making of such a complaint. The system must include a link to AAMS's website homepage.

4. All account-related windows on the site (particularly the deposit window) must provide a readily accessible link to the player protection / responsible gaming page.

5. The player protection / responsible gaming page must be readily accessible from any screen available where game play may occur, including the interface of any downloadable *client*.

6. No game play may occur where the links used to supply information on player protection / responsible gambling are not displayed or are not operational.

7. The operator must regularly test all links to the services supplied by third parties relative to game problems. Where the service is no longer available, or not available for a significant period of time, the concessionaire must provide an alternative support service.

2.4.2 LAST LOG-IN TIME DISPLAY

When a player logs in to the RGS, both the date of when they last logged in and the time (expressed in hours-minutes-seconds) must be shown.

2.4.3 SECURITY INFORMATION

1. The RGS must advise the player to keep their password and login ID secure.
2. The RGS must advise the player to be aware of what mechanisms exist to detect if there is unauthorised use of their account.

2.4.4 SELF-EXCLUSION

1. Players must be provided with an easy and obvious mechanism to self-exclude from game play.
2. At a minimum, this self-exclusion mechanism must be accessible from the player protection / responsible gaming page.
3. The player must be provided with the option to self-exclude temporarily for a specified period of time, as defined in the Player's account agreement, or permanently.
4. In the case of temporary self-exclusion, the RGS must ensure that:
    a) Immediately upon receiving the self-exclusion order, no new bets or deposits are accepted from that player, until the time of the temporary self-exclusion has expired, and
    b) During the temporary self-exclusion period, the player is not prevented from withdrawing any or all of their account balance, provided that the system acknowledges that the funds have cleared.
5. In the case of permanent self-exclusion, the RGS must ensure that:
    a) Immediately upon receiving the self-exclusion order, no new bets or deposits are accepted from that player, until the time of the permanent self-exclusion has been revoked,
    b) The player is paid in full for their account balance, provided that the system acknowledges that the funds have cleared, and
    c) Players are provided with a mechanism to revoke the self-exclusion order, using a special process to be identified by the concessionaire.

The list of players, including their tax code (Codice Fiscale), who have decided to self-exclude permanently, has to be communicated in writing to the AAMS. Please pay special attention to the fact that with both temporary and permanent self-exclusion, the player cannot be permitted to create another account.

2.4.5 EXCLUSION FORCED BY THE CONCESSIONAIRE

1. The RGS must provide a mechanism by which the concessionaire can exclude a player from the RGS under the terms of the Player's account agreement.

2. This mechanism must include a register of reasons for the exclusion.

3. Immediately upon activating the exclusion, access to the game or new deposits from that player cannot be allowed, until the time of the exclusion has been revoked.

4. During the exclusion period, the player must not be prevented from withdrawing any or all of their game account balance, provided that the system acknowledges that the funds have cleared, and that the reason(s) for exclusion would not prohibit a withdraw.

2.4.6 SELF-LIMITATION

1. The RGS must provide players with an easy and obvious mechanism to self-limit their game play and make it available according to the current norms in effect.

2. At a minimum, this self-limitation mechanism must be accessible from the player protection / responsible gaming page.

3. The RGS must prevent access to the player that has not set the parameters for self-limitation as per the current norms in effect.

4. Immediately upon receiving any self-limitation order, the RGS must ensure that all specified limits are correctly implemented in the system.

5. It is acceptable that self-limitations take effect the next time the player logs in to the RGS; however, the player must be clearly informed of the limitations that will be applied.

6. The ATF will verify that a system has been put in place that allows the player to reduce the severity of self-limitations, but only upon at least seven days notice.

7. Self-limitations must not be compromised by external time events, such as leap-years and daylight savings adjustments.

8. Self-limitations must not be compromised by internal status events, such as self-exclusion orders and self-exclusion revocations.

9. The self-limitation mechanism must include a deposit limit per time period: an overall maximum deposit limitation over a specified period of time (for example: daily, weekly,...). Furthermore, when the RGS undergoes the periodic conformity verification check (after 12 months), by that time it shall also include the following options:

    a) Bet limit per game – a limitation of the maximum single bet amount per individual game,

    b) Bet limit per time period – a limitation of the maximum bet amount over a specified period of time (eg.: daily, weekly, etc...),

2.4.7 LIMITS IMPOSED BY THE CONCESSIONAIRE

1. It is acceptable for the concessionaire to set limits (such as those listed above) on players, and vary those limits from time to time.

2. Players must be notified in ample advance of any operator-imposed limits.

3. The regulations 7 and 8 of Paragraph 2.4.6 “Self-limitation” in this document also apply to operator-imposed limits.

2.4.8 TRANSACTION LOGGING

1. Adequate logging of the relative operations of player accounts must be arranged, in order to ensure that dispute resolution is transparent (for detailed requirements refer to *2.7 Data logging requirements* of this document).

2. Adequate backups of player account transactions must be arranged, in order to ensure all player account balances can be recovered in the event of a disaster rendering the RGS inoperable (for detailed requirements refer to Paragraph 2.7 of this document).

2.4.9 MALFUNCTION

1. The eventual unrecoverable malfunction of gaming hardware / software must result in the voiding of affected game bets and pays, as well as the return of affected bets, except for the various conditions foreseen for specific types of games (for example, interactive tournament games). The concessionaire is in charge of the total reimbursement of game plays.

2. The terms and conditions of game play must clearly define the rules by which these unrecoverable malfunctions of gaming hardware / software are addressed.

2.5 RNG REQUIREMENTS

1. With respect to the application of the RNG requirements listed in this document, it is accepted that the requirement of unpredictability will not be relevant to certain applications. The ATF in charge must determine if the predictability is relevant to the application being tested and whether to apply these requirements accordingly.

2.5.1 GENERAL INTRODUCTION

1. Any RNG outcomes used for game symbol selection must be proven to:

   a) Be statistically independent,

   b) Be uniformly distributed, within statistically acceptable bounds (confidence intervals associated with certain reliability levels, sample size and sample variability),

   c) Pass statistical inferential tests at the 95% confidence level,

   d) Be unpredictable, even for an attacker who has knowledge of the algorithm, the algorithm’s implementation within the game(s) / application(s) to which it is connected, and the initial seed value (initial value used to seed the algorithm).

2. Game symbol drawing must not be influenced, affected or controlled by anything other than numerical values derived from the RNG in conjunction with the rules of the game.

3. As game symbols are drawn, they must be immediately used as directed by the rules of the game (i.e.: they are not to be discarded due to adaptive behaviour by the game).

2.5.2 SCALING

1. The method of scaling (i.e.: converting raw RNG outcomes of a greater range into scaled RNG outcomes of a lesser range) must be linear, and must not introduce any bias, pattern or predictability.

2. The scaled RNG outcomes must be proven to pass various recognised statistical tests.

2.5.3 MAPPING

1. The methods of mapping (i.e.: converting scaled RNG outcomes into actual game symbols / game outcomes) must also be linear.

   Note: it is accepted that certain game implementations require exemption from this requirement, such as instances where mapping is purposefully used to create the necessary probabilities for various game outcomes, as provided by the rules of the game.

2. The mapped RNG outcomes must be proven to pass various recognised statistical tests.

2.5.4 SELECTION OF RNG

The RNG can either be software-based, hardware-based, or a combination of both, at the discretion of the Concessionaire. However, the final implementation must comply with the requirements of this document.

2.5.5 HARDWARE RNG

Due to their physical nature, hardware-based RNGs can potentially 'break down' over time. Accordingly, failure of a hardware-based RNG could have serious consequences for the RGS functioning and exhibit an unfair distribution of game symbols. If a hardware-based RNG is used, some form of dynamic / active, real-time monitoring of the output is required, such that game play is disabled in the event that a failure is detected

2.5.6 SOFTWARE RNG

The following requirements apply only to software-based RNGs.

2.5.6.1 Period

As regards skill games, the period of the RNG must be sufficiently large to ensure the possibility to generate all the game symbols for the given games / applications

2.5.6.2 Interval

The interval of rough results generated by the RNG must be sufficiently large to provide adequate precision and flexibility when scaling and mapping.

2.5.6.3 Seeding/ Re-seeding

1. The methods of seeding / re-seeding implemented in the RNG must ensure that all seed values are determined securely, and that the resulting sequence of symbols is not predictable.

2. Unless proven to have no adverse effect on the randomness of the game symbols generated by the RNG outcomes, seeding and reseeding must be kept to an absolute minimum.

3. If for any reason the background cycling / activity of the RNG is interrupted, the next seed value for the RNG has to be generated by random event.

2.5.7 BACKGROUND CYCLING / ACTIVITY

This is not applicable to games of skill.

2.6 GAME REQUIREMENTS

2.6.1 GAME FAIRNESS

1. Games must not be designed to give the player a false expectation of better odds by falsely representing any event.

2. Near-miss games that are specifically designed to give the player the perception that they almost won the top prize (i.e.: with a frequency greater than that which would naturally occur given the game rules), in order to induce the player to continue gambling, are not permitted.

3. Each game must be accompanied by associated rules (complete with %RTP value) and game instructions.

4. The rules of the game and instructions of play must be available online to the player.

5. The rules of the game must not be unfair or misleading.

6. Game rules must not be changed during a session unless effective notification is given to player.

7. Game rules must not be changed in the interval between a player making a bet and the outcome as well as the payment of winnings for the bet.

8. Games must operate and interact with the player strictly in accordance with the published rules.

2.6.2 INADMISSIBILITY OF ADAPTIVE BEHAVIOUR IN GAMES

This is not applicable to games of skill

2.6.3 INADMISSIBILITY OF FORCED GAME PLAY

The simple selection of a game from the game menu must not force the player to take part to the game.

2.6.4 GAME PLAY REQUIREMENTS

1. The following information must be displayed on the game screen, or readily accessible via a direct link:
   a) Game name,
   b) Instructions (and restrictions) on game play, including the indication of all prizes and special features,
   c) Current account balance displayed in currency,
   d) Unit and total bet.
2. The following principles must be followed where games are provided in different language versions:
   a) Each language version of the same game must provide the same mechanism of determination of the payout/winnings,
   b) Each language version must be consistent with the instructions (and restrictions) for that version,
   c) All game information must be provided in the language specified for that version, and
   d) The game instructions (and restrictions) must carry the same meaning across all language versions so that no one version is advantaged or disadvantaged.

2.6.5 GAME DESIGN

1. All critical functions, including the generation of the game symbols of any game, must be generated by the RGS, independently of the end player device.
2. The game outcome determination must not be affected by the effective bandwidth, link utilisation, bit error rate or other characteristic of the communications channel between the RGS and the end player device.
3. Multiple versions of one game (i.e. the mechanism of determination of the payout/winnings) are not acceptable, except where those alternative variations have been approved by the AAMS.

4. The %RTP for skill games and tournament based card games must be 80% or greater.

5. The %RTP for each game must be specified by the Concessionaire in the game documentation.

6. Where a game is represented or implied to include a simulation of a real-life physical device, the behaviour of the simulation must be identical to the expected behaviour of the real-life physical device. That is:

   a) 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 must be equivalent to the real-life physical device,

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

   d) Where the game simulates real-life physical device that have no memory of previous events, the behaviour of the simulations must be independent, thus not correlated to their previous behaviour, so as to be non-adaptive and unpredictable in practice.

7. Games that are not completely independent of game play history (e.g.: metamorphic games) must:

   a) Display clearly to the player which game rules apply to the current game status

   b) Provide to the player sufficient information to indicate the current status towards the triggering of the next metamorphosis of the game (e.g.: the eventual need of game credits will have to be indicated, the number of missing game credits or the total number to activate the subsequent metamorphosis, in addition to the number of credit games collected up to that point),

   c) Not adjust the likelihood of a metamorphosis occurring based on the history of prizes obtained in previous games

   d) Not be designed in such a manner to be misleading to the player.

2.6.6 GAME PLAY

1. Game play that requires monetary payment (i.e.: play-for-real) can only occur during a game session (i.e.: after the player has logged in, and before the player has logged out).

2. Where external links are used to supply game information as required by these Guidelines, game play must not occur if said information is not available. The availability of this information must be checked (either manually or automatically) at least daily:

   a) Where a broken external link is uncovered, and it relates to game-specific information only, then the associated game(s) must be taken offline (either manually or automatically) if the link is not repaired within one hour

b) a broken link is uncovered, and it relates to the website as a whole, then all games must be taken offline (either manually or automatically) if the link is not repaired within twelve hours.

3. In the event that a game cannot be continued due to an RGS malfunction, all bets must be reimbursed to the players of that game, with the exception of the various foreseen conditions for specific game types (e.g.: interactive tournament games). The operator is in charge of the total reimbursement of game plays.

4. If the RGS extends an invitation to play a particular game, it must accept all legitimate wagers (as defined by rules) for that game.

5. The methodology employed by a player to select and play a particular game must be transparent.

6. The RGS must clearly inform the players of all games available at that time.

7. The player must at all times be made aware of which game has been selected for play or is being played.

8. 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 previous game, and must provide the following information (at a minimum):

   a) The date and time the game was played,

   b) ID code of the game assigned by the AAMS, complete with timestamp;

   c) The display associated with the final outcome of the game, either graphically or via a text message,

   d) Amount of bet,

   e) Amount of the winning of the last game,

   f) Results of any intermediate game phases, such as gambles or bonus games.

2.6.7 GAME DISABLE

1. The RGS must provide to the concessionaire a disable option for each game variation offered, among those approved by AAMS.

2. When a game variation is disabled, all players playing that game variation must be permitted to conclude their current game in play. Exceptions can be made for multi-state game variations that are currently in play, where the player has ended their session in the middle of a hand, or a period of inactivity greater than 30 minutes has elapsed, during which time the operator must make all reasonable efforts to advise the player that their game must be finished. If a multi-state game variation is disabled in such a manner, the player must be advised that this has occurred the next time they log on to the RGS.

3. Once a game variation is disabled, it must not to be accessible to players after their current game has concluded.

4. The RGS must provide to the concessionaire full audit trails when disabling a game variation that is currently in play.

5. The RGS must also provide a disable option for all gaming offered on the RGS to be disabled, as a whole, by the concessionaire – with full consideration to the associated requirements listed above.

6. The RGS must also provide the concessionaire with a disable option for each single active game session, with full consideration to the associated requirements listed above.

2.6.8 INCOMPLETE GAME PLAYS

1. The RGS must provide a mechanism for a player to complete an incomplete game , with the exception of game play with indirect contest, before a player is permitted to participate in any other game. Incomplete games include:

   a) Loss of communications between RGS and end player device,

   b) RGS restart,

   c) Game disabled by RGS,

   d) End player device restart,

   e) Abnormal termination of gambling application on end player device, and

   f) The momentary interruption of game by a player that has followed an external link to a page in order to find more information on the game itself.

2. Upon reconnection by the player, the RGS must present the player the incomplete game for completion.

3. Multistage games that have been disabled by the RGS, may be terminated immediately upon the disable of the game.

4. Game phases associated with a partially complete game that can be continued must be held by the RGS until the game completes. Player accounts must reflect any funds held in incomplete games.

2.6.9 GAME ARTWORK (DISPLAYED INFORMATION)

This section refers to all forms of graphical and auditory information that is sent to the end player device for presentation to the player. The combination of all relevant information being presented to the player must comply with these requirements

2.6.9.1 Instructions and Information

1. All information presented on the gaming platform and games (whether visual or auditory, written or pictorial) must not be in any manner or form indecent, illegal or offensive (e.g.: pornographic or offensive to religion or race).

2. All information presented on the website and games must be available in Italian, and must be both grammatically and syntactically correct.

   Note: logos or copyright messages may be displayed. This does not preclude the display of the same information in other languages

3. All written information presented on the gaming platform and games must be clearly shown and must not be deceiving to the player.

4. All written information presented on the gaming platform and games must be truthful.

5. All game help / rules information must be clearly visible, or the means of displaying such information must be readily available, at all times.

6. All game help / rules information must be visible / available to the player without the need for money to be bet on the game.

7. All game help / rules information must be easily interpretable, non-ambiguous, and sufficient to explain all game rules.

8. There must be sufficient game help / rules information to allow a player to determine the correctness of prizes awarded.

9. The name of the game being played must be clearly visible to the player on the game screen.

10. The functions of all buttons represented on the website and games must be clearly indicated, preferably on the button.

2.6.9.2 Bet display

1. The bet denomination (and where applicable the tokenisation) of the game must be clearly visible on the game screen, or be able to be easily deduced.

2. Where the game uses game credits, the number of credits registered for each monetary unit for the current game must be displayed on the game screen.

3. The artwork must either state the maximum bet or it must be possible to deduce this information from the game help / rules.

4. The minimum bet (if not easily deduced) must be readily available to the player, either directly on the game screen or in the game help / rules information.

2.6.9.3 Result display

1. The display of the game outcome must not be misleading or deceptive to the player (e.g.: it must not inappropriately indicate a near-miss, as per paragraph 2.6.1, point 2).

2. The outcome of each game must be displayed for a reasonable length of time.

3. The nature of all prizes must be clearly indicated. If some prizes are in cash, and/or in other credits, this must be stated.

4. If the original artwork contains game instructions specifying a maximum win, then it must be possible to win this amount from a single game (including bonus or other game options). For example, if the artwork states that the maximum prize for a game is €2.000,00, it must be possible to win said sum in a game play.

5. To the extent that is practicable for the range of games offered, only one method of displaying win amounts should be used on the gaming platform so as to avoid confusion.

2.6.9.4 Multi-player games

1. Multi-player games (e.g.: Poker) with outcomes that can be affected through an external exchange of information between different players (e.g.: a telephone conversation) will not be permitted unless clear rules compensating controls or technology is put in place to ensure the appropriate management and that the prospect of cheating is addressed and minimised.

2. Multi--player games with outcomes that can be affected through the use of automated end player devices or ancillary computer systems (e.g.: chess) must have warnings in the game rules so that players can make an informed decision whether or not to participate.

3. RGS must ensure player fairness, to the extent possible, in the event of a communication loss to one or more end player devices during a multi-player game.

4. Game rules must cater for situations where the RGS loses connectivity with the player. The consequences must be explained to the player.

2.6.10 SPECIFIC REQUIREMENTS PER GAME

The appendices of these Guidelines detail any requirements that are specific for each type of game or game feature. It should be noted that a game or game feature need only comply with the requirements applicable to that particular type of game or game feature.

2.7 DATA LOGGING REQUIREMENTS

2.7.1 GENERAL REQUIREMENTS

1. The RGS must be capable of retaining and backing up all recorded information, as discussed in the following paragraph. Accordingly, among other implications, the number of digits to be used in all fields must therefore be based on appropriately projected performance and business.

2. All time stamping implemented throughout recorded information must make use of the 24-hour format, synchronized to UTC.

3. All time stamping implemented throughout recorded information must make use of a consistent format to be prescribed by the concessionaire.

2.7.2 PLAYER ACCOUNT INFORMATION

1. For each individual player account, the RGS must maintain and back up the following information; and be capable of reporting this information, for the period of time established by the current set of directives:

   a) Player identity details (including player identity verification results),

   b) Account details and current balance,

   c) Changes to account details, such as change of address, change of credit card, change of name,

d) Consent to use of personal data according to the privacy policy,

e) Any self-imposed player protection limitations,

f) Any self-imposed player protection exclusions,

g) Details of any previous accounts, including reasons for deactivation,

h) Deposit / withdraw history,

i) Game play history (i.e.: games played, amounts bet, amounts won, etc…).

2. For player accounts as a whole, upon request by the AAMS, the RGS must be capable of generating the following reports, for the period of time established by the current set of directives:

a) A list of all currently (or previously) active player accounts,

b) A list of all currently (or previously) inactive player accounts (including reasons for deactivation),

c) A list of all accounts for which the player has currently (or previously) imposed a player protection self-exclusion,

d) A list of all accounts for which the player has currently (or previously) been excluded from the site by the Operator (i.e.: involuntary exclusion),

e) A list of all accounts for which the player's funds have currently (or previously) been inactive for a period of time exceeding 36 months,

f) A list of all accounts for which one or more of the player's deposits and / or withdraws have exceeded a certain limit (i.e.: large deposits / withdraws). The limit must be configurable for single transactions, as well as aggregate transactions over a user-defined time period,

g) A list of all accounts for which one or more of the player's wins have exceeded a certain limit (i.e.: large wins). The limit must be configurable for single wins, as well as aggregate wins over a user-defined time.

2.7.3 GAME SESSION INFORMATION

1. For each individual gaming session (i.e.: player login time to logout time), the RGS must maintain and back up the following information, and be capable of reporting this information upon request:

a) Unique player ID,

b) Gaming session start and end time,

c) Game play information for session (i.e.: games played, amounts bet, amounts won etc…).

2. The RGS must be able to generate upon request a report on all currently active gaming session.

2.7.4 INFORMATION ON SINGLE GAME PLAYS

1. For each individual game played, the RGS must maintain and back up the following information, and be capable of reporting this information upon request:

a) Unique player ID,

b) Unique game identifier,

c) Game start time, according to RGS,

d) Player account balance at start of game,

e) Amount wagered,

f) Current game status (e.g.: in progress / complete)
Note: the RGS must maintain records of any game that fails to complete, and the reason why the game failed to complete

g) Game outcome,

h) Game end time, according to RGS,

i) Amount won, and

j) Player account balance at end of game.

2. The RGS must maintain and back up of a list of all games hosted by the gaming platform, including approved game versions; said information must be available upon request for a period of time established by the concessionaire.

2.7.5 SIGNIFICANT EVENTS INFORMATION

For significant events, the RGS must maintain and back up all the changes made by the Concessionaire to game parameters and be capable of reporting this information upon request.

2.8 TECHNICAL REQUIREMENTS

2.8.1 DATA TRANSMISSION AND MEMORIZATION

1. Where player account information and / or game play data is either being passed over communication lines (e.g.: the Internet), or being stored somewhere in the RGS, such data must be protected (i.e.: encrypted) commensurate with the sensitivity of that data with a protection level equivalent to that supplied by the protocol TLS with RSA at 1024 bit and 3DES. Examples of sensitive data that require encryption are:

   a) Player identity details (including player identity verification results),

   b) Credit and debit card details,

   c) PINs and passwords,

   d) Account details and balances,

   e) Player protection limitations,

   f) Player protection exclusions,

   g) Money transfers to and from player accounts,

   h) Changes to account details (e.g.: change of address, change of credit card, change of name, etc…), and

   i) Game play (i.e.: games played, amounts bet, amounts won, etc…).

2. Any sensitive or confidential information maintained by the RGS must be stored in areas of the system that are secured from unauthorised access, both external and internal.

2.8.2 SHUTDOWN AND RECOVERY

1. The RGS must be able to perform a graceful shutdown in the event of a simple power failure, and not restart automatically on power up.

2. In the event of a critical hardware / software failure, the RGS must be able to recover all critical information from the time of the last backup to the point in time at which the system failure occurred.

3. The concessionaire must have disaster recovery capability sufficient to ensure player entitlements are protected and audit ability is facilitated up to the point of the disaster.

4. The RGS must be able to recover from unexpected restarts of its central computers or any of its other components.

5. The RGS hardware platform and Operating System (OS) must be proven to be reliable.

2.8.3 SERVICE CONTINUANCE

1. The RGS must adopt trustworthy and resilient measures for systems and components, in order to guarantee the continuance of service.

2. The operator must self-equip with organizational, developmental and maintenance procedures, in order to guarantee the quality of the solutions adopted in said objective.

2.8.4 REAL-TIME DATA EXCHANGE BETWEEN THE RGS AND THE AAMS CENTRALIZED SYSTEM.

The RGS must have the capability of exchanging data in real-time with the AAMS central control system, through the proprietary communications protocol posted on the AAMS internet web site.

2.8.5 ACT OF CONTROL AND VIGILANCE BY THE AAMS

The RGS must allow access to AAMS to exercise the act of control and vigilance. In particular, the RGS must allow the remote access to data from game sessions, to both past and in progress game plays, to user account information via web interface through the use of an encrypted protocol (ex. SSL) and strong authentication mechanisms (ex. Smart cards, token cards, dynamic password).

2.9 INFORMATION SYSTEMS SECURITY REQUIREMENTS

The aim in setting out the following security guidelines is to ensure customers are not exposed to unnecessary security risks by choosing to participate in remote gaming.

The verification of security requirements will form part of the annual review of the RGS, and will apply to the following critical system components:

1. Electronic systems that record, store, process, share, transmit or retrieve sensitive customer information, e.g. credit/debit card details, authentication information, customer account balances;

2. Electronic systems that generate, transmit, or process random numbers used to determine the game symbols or virtual events;

3. Electronic systems that store results or the current state of a customer's gamble;

4. Points of entry to and exit from the above systems (other systems that are able to communicate directly with core critical systems); and

5. Communication network that transmit sensitive customer information.

2.9.1 SECURITY POLICIES AND PROCEDURES

1. Security policies and procedures must be documented and communicated to relevant employees.

2. A mechanism must be in place for the check and review of security policies considering material changes of the electronic systems in questions or the manners in which they are used.

2.9.2 PHYSICAL AND ENVIRONMENTAL SECURITY

1. All computer systems should physically reside in a data centre which enables the physical access to critical system components to be restricted to authorised personnel.

2. Sufficient supporting utilities such as power, cooling and fire suppression equipment must be provided in relation to the scale of the critical system components.

3. Intrusion detection systems must be in place and all access must be logged in an auditable form.

2.9.3 ADMINISTRATIVE CONTROLS

1. Updates to the systems, including patches, hot fixes, service packs and firmware updates, will be carried out using documented procedures and all changes will be logged.

2. A written disaster recovery plan must exist, with disaster recovery responsibilities and procedures clearly defined.

2.9.4 TECHNICAL CONTROLS

1. Virus scanners and / or detection programs shall be installed on all critical information systems.

2. Procedures must be in place for the management of all removable media, and all media which may contain critical data shall be disposed of securely and safely using formal procedures.

3. System monitoring must be in place to detect unauthorised information processing activities, and must include:

   a) Audit logs recording user activities, exceptions, and information security events,

   b) Audit logs of system administrator and system operator activities,

   c) Logging of system faults, analysis and corrective action taken,

   d) Protection of logging facilities and log information.

4. Access controls to ensure authorised user access and to prevent unauthorised access to information systems must be in place, and must include:

   a) A formal user registration and de-registration process for granting and revoking access to all information systems and services,

   b) Restriction and control of user privileges based on the level of responsibility of the user,

   c) Control of passwords through a formal management process,

   d) The use of appropriate authentication methods to control access by remote users,

   e) Automatic equipment identification to authenticate connections from specific locations and equipment,

   f) Controls over the physical and logical access to diagnostic and configuration ports,

   g) Segregation of groups of information services, users and information systems,

   h) Session time-out after a defined period of inactivity.

5. A formal key management process must be in place to control access to encrypted data.

6. Penetration testing of all external IP addresses should be conducted on a regular basis.

APPENDIX A: GAMBLE OPTION REQUIREMENTS

This appendix is not applicable to games of skill.

APPENDIX B: ROULETTE GAME REQUIREMENTS

This appendix is not applicable to games of skill.

APPENDIX C: DICE GAMES REQUIREMENTS

This appendix is not applicable to games of skill.

APPENDIX D: GENERAL CARD GAMES REQUIREMENTS

The following requirements apply to any simulations of card games that involve the dealing of cards from a deck or deck(s):

1. Card faces must clearly display the card value (e.g.: it must be obvious which is a Jack and which is a Queen).

2. Card faces must clearly indicate the suit (e.g.: it must be obvious which is a Spade and which is a Club). Hearts and Diamonds must be red; Clubs and Spades must be black, unless the player specifically chooses a four colour option in order to better distinguish the suits.

3. Jokers must be distinguishable from all other cards.

4. It must be clearly stated if more than one deck of cards is used in the game.

5. The artwork must clearly state if the rules of the game do not shuffle the deck after every game. In this instance, the artwork must indicate when shuffles actually do occur.

APPENDIX E: SINGLE-PLAYER POKER REQUIREMENTS

This appendix is not applicable to games of skill.

APPENDIX F: MULTI-PLAYER POKER REQUIREMENTS

The following requirements apply only to simulations of Multi-Player Poker games:

1. The artwork must provide clear indication if Stud Poker rules apply. Common Draw Poker must be assumed, if nothing is stated.
2. The artwork must provide a definition of winning combinations outside the scope of standard Poker (e.g.: Royal Flush with / without Wild Cards, Four of a Kind "Jacks or Better", Four Deuces (when Deuces are wild), etc…).
3. Wild card rules must be clearly explained (e.g.: Jokers Wild or Deuces Wild).
4. All special rules outside the scope of common Poker must be clearly explained.
5. When player options outside the scope of common Poker are available, they must be clearly explained on the artwork.
6. If some features are available only at certain tables, this must be made clear to the players.
7. The amount of rake taken by the Operator, as well as any additional fees, must be displayed on the game page or available through a hotlink.
8. The artwork must clearly indicate any variation in the rake amount based on the table, limit amount, number of players, or pool amount.
9. The tournament prize structure, if applicable, must be clearly explained to the players.
10. The disconnection protection policy must be clearly indicated on the game page or available through a hotlink.
11. Held and non-held cards, including recommended holds (if implemented), in Draw Poker or equivalent must be clearly marked on the screen, and the method for changing Holds clearly displayed to the player.
12. The RGS must state that the use of automated end player devices (BOTs) is not allowed. The player can be pointed to, and is allowed to use, game auxiliary tools that can help calculating probability. The concessionaire can make available a link to a site from which these applications can be downloaded
13. The artwork must clearly indicate the total amount the player has bet on the game currently being played. This amount must be updated every time the player places a wager.
14. The artwork must clearly indicate the prize amount the players are playing for at all times during game play (i.e.: the players' stakes less the Operator's rake). This amount must be updated each time a wager is placed.
15. Winning hands must be clearly labelled as to the win category (e.g.: "Full House").
16. Players shall not be permitted to play more than one hand in a game.
17. Players shall not be permitted to wager on another player's hand.

APPENDIX G: BLACKJACK REQUIREMENTS

This appendix is not applicable to games of skill.

APPENDIX H: LIVE DEALER GAMES

This appendix is not applicable to games of skill.

APPENDIX I: OTHER GAMES

This section applies to games that do not fall into any of the above categories.

1. Initial player selection options must be described.
2. Player selection options, once the game has commenced, must be clearly shown on the screen.
3. The winning amount for each separate wager and total winning amount must be displayed on the screen.

GLOSSARY

Term	Description
%RTP	In skill games the RTP is the percentage of wagers that are paid out to the player. In tournament games it is the percentage of wagers that are forming the pool.
ATF	Accredited Testing Facility
Background Cycling / Activity	If the software-based RNG is cycling in the background, it means that there is a constant string of random numbers being generated by the RNG, even if they are not actually required by the game at that time. Without background cycling / activity, one could predict the result of the next iteration of the function used to produce the random numbers if they knew the current values and the algorithm.
Gaming platform	'Gaming platform' refers to RGS elements that drive the features that are common to all of the games, and form the primary interface to the RGS for both the player and the Operator: • The Gaming platform provides the player with the means to register an account, log in to / out of their account, modify their account information, deposit and withdraw funds to / from their account, request account activity statements / reports, and close their account. In addition, any web pages displayed to the player that relate to gaming offered on the RGS, but are not an actual game screen, are considered to be part of the Gaming platform, and • The Gaming platform provides the Operator with the means to review player accounts, enable / disable games, generate various gaming / financial transaction and account reports, input game outcomes for sports betting events, enable / disable player accounts, and set any configurable parameters.
COBIT	Control Objectives for Information and Related Technology
DOF	Degree of Freedom. Equal to one less than the total number of possible outcomes (e.g.: with a 52-card deck, the degrees of freedom = 51).
EFT	Electronic Funds Transfer
EGD	Electronic Gaming Device
Emulation	All submitted games must be exhibit 'Emulation Capability' for testing purposes. This means that all games must have a mode of operation that is alternate to the standard / live version of the game (i.e.: to be activated and operated in the test environment only) whereby the game outcomes can be artificially introduced into the system by the user (i.e.: the tester), processed by the same game logic as the standard / live version of the game, and then displayed to the user for testing purposes.
Family of Games	A family of games is constituted by games that: - Share the same set of rules

	- Have the same %RTP - Share the same game math - Handle relative jackpots in the same way In summary, the games of a family might only present different graphic attributes, as it is often the case in slot-machine games.
FAQ	Frequently Asked Question
Game	'Game' refers to RGS software that is specific to each individual game that is hosted / offered on the gaming platform. Each game is to be treated as a separate and distinct entity.
ID	Identification
IDS	Intrusion Detection System
RGS	Remote Gaming System
IP	Internet Protocol
ISO	International Standards Organisation
ISS	Information Systems Security. Refers to the Administrative Controls, Technical Controls and Physical & Environment Controls necessary for the secure, safe and auditable operation of the RGS by the Operator.
LAN	Local Area Network
Mapping	Mapping is the process by which the scaled number is given a symbol or value that is usable and applicable to the current game (e.g.: the scaled number 51 might be mapped to an ACE OF SPADES).
Multi-Stage Game	A game having one or more intermediate steps that require player input in order to proceed. Poker and Blackjack are two examples of multi-stage games.
OS	Operating System
Period	Period is how long before the 'random' sequence repeats. Is the output from the RNG sufficient to provide all possible outcomes? In a 52-card deck, requiring an ordered straight flush on the first hand, and assuming that one draws all ten numbers (replacements included) at the beginning of the game, the required number of ORDERED outcomes so that each outcome may be achieved is 52P10 = 5.74 X 1016. 20 balls from 80 (e.g.: Keno) requires 80C20 = 3.54 X 1018 possible outcomes.
Progressive Jackpot Parameter change	Not applicable

Raw Values	The unscaled output of an RNG.
Range	Range is the actual size of the output from the RNG. A 32-bit RNG provides 232 possible outcomes (4.29 X 109). If one considers a 64-bit output, one can achieve 1.8 X 1019 different RNG outcomes.
Reseeding	Reseeding is when the RNG algorithm is restarted (given new initial seed values).
RNG	Random Number Generator. Refers to RGS hardware and / or software that determines random outcomes for use by all of the games hosted / offered on the gaming platform.
Scaling	Raw output from an RNG will normally have a range far in excess of that required for its intended use (e.g.: 32-bit RNG's have over two billion possible outcomes, but (for example) we have only to determine which of 52 cards to draw). Scaling is required to divide the raw output into smaller, and usable numbers. These 'scaled' numbers can then be mapped to particular card numbers, record numbers, symbols, etc… Consequently, raw output from an RNG will sometimes have a range far smaller than that required for its intended use (e.g.: 0 < raw output < 1). In these cases, scaling is required to expand the RAW output into larger usable numbers.
Seed	The common misconception is that a seed is the INITIAL VALUE of an RNG, and once started there is no use for a seed unless the RNG is restarted. The term 'seed' is frequently misused in the case of algorithmic RNGs. For these RNGs, the seed is the value used as the basis for the next iteration of the function that forms the RNG algorithm (i.e.: in most cases, the last value).
Seeding	Seeding is the method used to seed RNGs in the very first instance (i.e.: upon initialisation).
VLAN	Virtual Local Area Network