IAGR eGambling Guidelines

October 2018

Table of Contents

1. Overview of This Document

1.1 Background

The IAGR working group and technical subcommittee has worked together to create a multi jurisdictional forum to identify and agree to the aims and principles for effective operation of eGambling. This work draws on the experiences and expertise of a variety of jurisdictions and recognises there may be more than one way of meeting these objectives.

1.2 Scope of the Document

It is important to note that this document alone is not sufficient to cover all aspects of the regulation of eGambling. This document is a supplement to other reference materials on eGambling including materials developed by eGambling jurisdictions.

1.3 Future Review of this Document

eGambling is a dynamic and fast moving industry. This document is not intended to limit the use of new technology and we recognise it is important to regularly review the content. Therefore, the IAGR working group and technical subcommittee will continue to consider developments in eGambling and where appropriate propose amendments to this document.

1.4 Objectives of the Document

The objectives of this document are as follows:

1. To provide clear good practice guidelines for eGambling that contributes to the credibility and integrity of eGambling operations.

2. To outline minimum criteria that will contribute to fair, honest, secure and auditable eGambling operations.

3. To construct a reference document that can be easily changed or modified to allow for new technology.

4. To identify principles and good practice and not specify any particular method or technology, recognising instead that a wide range of existing and new methods and technologies may well be used to meet the guidelines contained in this document.

1.5 Use of the Document

This document is not intended to be a universally endorsed approach for regulating eGambling as each jurisdiction may have unique requirements and its own national laws and regulations and international obligations. However, it is intended to provide good practice guidance in key areas of eGambling regulation that jurisdictions can incorporate should they choose to do so.

The document is expressed in terms of each guideline being mandatory by use of the word *must* so that jurisdictions wishing to adopt the guidelines can do so by simply pulling out the relevant sections. However, as outlined above, it is for each individual jurisdiction to decide on whether they make the guidelines mandatory or optional and therefore whether they use *must* or *should*.

This document includes a number of sections that set out key guidelines for eGambling. Each section includes an overall objective and then goes into further detail setting out good practice in how to meet the overall objectives.

The good practice guidelines do not preclude a Regulator from setting its own requirements, requiring higher standards from gambling operators or from using alternative means of meeting the objectives. The ultimate approach that a jurisdiction adopts depends on its specific circumstances.

2. IAGR eGambling Standards Protocol

2.1 Agreed Objectives and Principles

The October 2006 meeting of the IAGR eGambling Working Group agreed the following objectives of the IAGR eGambling Standards Protocol:

1. To minimise harm to the vulnerable and promote responsible gambling;
2. To ensure probity, integrity and competence in operators; and
3. To ensure the fairness of games, the integrity of systems and the quality of services to players.

The working group also identified a number of regulatory principles for eGambling, including:

1. Player protection;
2. Exclusions;
3. Licensing controls;
4. Operational and technical standards;
5. Advertising;
6. Player registration; and
7. Financial transactions.

2.2 Development of Principles into eGambling Guidelines

The IAGR eGambling Working Group agreed that a technical subcommittee be formed to develop eGambling guidelines. This latest effort is an update of that original work and recognizes the evolution of technology and the expansion of eGambling throughout the world. Chapter 3 onwards sets out the good practice guidelines which develop further the practices and experiences of various eGambling jurisdictions.

3. Customer Registration and Accounts

3.1 Overall Objective:

The objective of this guideline is to identify controls that an operator should implement as part of the customer account registration process and on-going account integrity to ensure that:

1. The customer is clear about and accepts the terms on which he/she is contracting with the operator;
2. The operator has appropriate account controls in place;
3. The customer is aware of who the operator is and where it is licensed/regulated;
4. The customer's identity and entitlement to gamble (including age and, where necessary, location verification) is established; and
5. Access to customer data is controlled to protect against misuse.

Where other regulations or legislation exist for data protection the regulator should refer to those.

3.2 Good Practice Guideline:

3.2.1 Display of Licensed Status

1. The website must include clear statements that enable the customer to understand in which jurisdiction the particular operator and product are licensed and regulated. Hyperlinks or the use of a regulator logo to direct the user to the regulator issued licensee or website may further demonstrate the authenticity of the gambling facilities.

3.2.2 Terms & Conditions

1. Terms and conditions and general information provided to the customer must be easily accessible and stated in a clear and intelligible manner. Any acceptance of Terms and Conditions and any changes to the Terms and Conditions should be time stamped and recorded in the operator's patron file. Any changes to the Terms and Conditions shall be accepted by the patron.
2. The customer registration process must include the customer's agreement to the operator's Terms and Conditions and customers may only be permitted to gamble if they take an action to acknowledge the agreement. The regulator may specify conditions which customers may be required to be noticed of and specifically agreed to. (For example agree that underage gambling is illegal and that sharing your account with a minor is crime. Acknowledging protections regarding customer deposits).
3. It must be clear to the customer which operator they are gambling with and in which jurisdiction the operator is licensed. For whitelabelling arrangements it must be clear who the whitelabel provider is and where the provider is regulated.

3.2.3 Customer Identification

1. A person (a "customer") must only be permitted to gamble where they hold a valid account with the operator.
2. The operator must take reasonable steps to establish the age and identity of a person before allowing them to gamble. The means to achieve this may differ depending on the information that is available on customers in different jurisdictions. Where required, the operator must use an automated process to establish the age and identity of the person before allowing them to gamble.
3. The customer must be required to demonstrate their identity in order to access the Internet Gambling System (IGS) for gambling.
4. Where a customer's age or identity information is rejected by the operator, the customer must be afforded a means to attempt to resolve the rejection.
5. The operator must take reasonable steps, where required by legislation or regulation, to establish the location of the person.
6. Jurisdictions may allow customers to open a restricted account pending the completion of the Know Your Customer (KYC) process. The restricted status would provide limited wagering and deposit capability until after verification has been completed. For customers whose KYC has not been completed, withdrawals should not be permitted.
7. Restricted accounts should only be permitted for a limited time period specified by the regulator.

3.2.4 Under Aged Persons

1. Persons under the age of majority must not be permitted to gamble (i.e. Minors).
2. Customers must affirm that they are of legal age to gamble as part of the registration process and the operator must verify this information.
3. All gambling transactions in which a minor has participated must be made void – any amounts deposited or won shall be dispensed in accordance with jurisdictional requirements. (Regulations may require the funds to be returned to the minor or be retained by the regulator).
4. A record of any such voided transactions must be kept, including the reason for making the transaction void.
5. Customers must not be permitted to withdraw winnings until satisfactory completion of age verification.

3.2.5 Account Security

1. A secure process must be established for passwords to be issued/changed/re-issued to customers. This process may include:
    a. requiring the customer to provide answers to "challenge questions", such as town of birth, and requiring these questions to be correctly answered before re-issuing a password or allowing a customer to choose another password;
    b. issuing the password in such a way that only the customer must have access to it, for example emailing a new password to a customer's previously nominated email address or sending a text message to a mobile device; or
    c. requiring the customer to demonstrate their identity by other means such as user name and password.

2. Operator generated passwords must be issued securely and must be changed by the customer prior to gaining access to the IGS.
3. All customer accounts (including dormant accounts) on the IGS must be secured against unauthorised access or update. This includes unauthorised internal access (e.g.: by operator staff) and unauthorised external access (e.g.: by 'hackers') which can be identified through IP and device ID monitoring.
4. Where appropriate, the operator must be able to implement a user inactivity timeout that automatically logs the customer out and/or ends the customer's session after a specified period of inactivity.
5. The operator must advise the customer of ways they may keep their account details secure.

3.2.6 Customer Accounts

1. Each customer must only be permitted to have one active account at a time or an operator must be able to link multiple customer accounts to that individual. The operator shall ensure an adequate collusion detection process exists in the event multiple accounts can be created for one individual.
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. The operator shall have the ability to provide the customer an account statement upon request.

3.2.7 Customer Funds Controls

1. All transactions must be uniquely identifiable and maintained in a system audit log.
2. A deposit into a customer account must not be available for gambling until such time as the transaction has been approved by the appropriate issuing authority. This authorisation must be maintained in a system audit log.
3. Subject to any restrictions that may legitimately apply (i.e. on-going criminal investigations) a customer must be able to withdraw deposits from their account at any time.
4. Operators must provide clear and easily accessible information to customers about how they protect customer funds and the methods they use to do so and about how they deal with unclaimed funds from dormant accounts.
5. An Internet gaming operator may maintain an accredited bank account separate from all other operating accounts to ensure the security of funds held in patron Internet gaming accounts. The balance maintained in this account shall be greater than or equal to the sum of the daily ending cashable balance of all patron Internet gaming accounts, funds on game, and pending withdrawals.

3.2.8 Use of Customer Data

1. Operators must keep the customer's account information confidential, except where the release of that information is required by law.
2. The operator must ensure that access to customer information is restricted to the customer and authorised internal staff or authorised external agencies or regulatory staff.
3. The operator must ensure that information obtained about customer's gambling

behaviour is not used to encourage irresponsible gambling.

3.2.9 Customer Consent to Use of Data

1. The operator's privacy policy must be stated in a clear and intelligible manner.
2. The privacy policy must inform the customer of the extent to which the operator, authorised external agencies and regulatory staff, have access to their account information.
3. The customer registration process must include the customer's agreement to the operator's privacy policy.
4. The customer must only be permitted to gamble if they take an action to acknowledge the agreement.
5. Where the operator intends to use data for purposes not directly related to the offering of a gambling product (e.g.: for inclusion in a mailing list), additional specific consent must be granted by the customer. Withholding this type of consent must not be used as grounds to refuse to conduct business with a person. The agreement to the operator's privacy policy and any additional consents granted by the customer should be time stamped and recorded in the operator's patron file.

4. Customer Protection

4.1 Overall Objective:

The objective of this guideline is to identify controls that an operator should implement in the area of customer protection. This includes:

1. General information that should be provided to customers but also specific information on help and advice on problem gambling.
2. How to make a complaint against the operator.
3. A process to self-exclude from an operator's gambling products.
4. The means to keep track of gambling activity and implement self-imposed limits.

4.2 Good Practice Guidelines:

4.2.1 Responsible Gambling Information / Links to Help

The following information must be made available:

1. Customer protection and responsible gambling information must be easily accessible.
2. As a minimum, entry windows (entry pages or screens) and account related windows must contain a link to the operator's responsible gambling and/or customer protection information.
3. In addition, all account related windows (particularly the deposit window) must provide a hotlink to a reputable problem gambling service that has agreed to be linked to the site. Operators must select an appropriate problem gambling service or it may be prescribed by the jurisdictional government.
4. An operator may consider making available a link to a service that provides website filtering.
5. A list of the customer protection / responsible gambling options available to the customer (e.g.: session time limits, bet limits, etc), and a link to those options or instructions on how to access those options must be provided.
6. All links to problem gambling services provided by third parties are to be regularly tested by the operator. Where the service is no longer available or not available for a significant period of time, the operator must provide an alternative support service.
7. The responsible gaming information displayed by the operator shall be easily accessible. The jurisdiction may consider implementing a responsible gaming logo on each site whereby if the patron clicks on the logo, the patron will be presented with the responsible gaming information.

4.2.2 Self-Exclusion

1. Customers must be provided with an easy and obvious mechanism to self-exclude from the operator's gambling products for a predetermined amount of time (e.g.: six months, one year, etc). The information must make clear to the customer both the mechanism and the terms on which the self-exclusion order will be executed.
2. At a minimum, this self-exclusion mechanism must be accessible from the customer protection / responsible gambling page.

3. In the case of a self-exclusion as defined in point 1 above, the operator must ensure that:
    a. as soon as reasonably practicable following receipt of a self-exclusion order, no new bets or deposits are accepted from that customer;
    b. the customer's entire, cleared account balance is remitted to the customer using the customer's registered name and address;
    c. the self-excluded person must confirm to the operator that they wish to return from a self-exclusion before their account is re-instated; and
    d. the operator must take all reasonable steps to remove the self-excluded customer's details from any future marketing campaigns.
4. Operators must take all reasonable steps to ensure self-excluded persons are not permitted to create a new account with the operator.
5. A method should be in place, whether by the operators or the regulatory agency, that ensures if a customer self-excludes from one operator, all other operators in that respective jurisdiction will prevent the customer from creating an account with them. An option shall be made available by the jurisdiction, to allow for a patron to self-exclude without having to create an Internet gaming account.
6. In the case of temporary self-exclusion, sometimes referred to as "cool-off", (e.g.: 24 hours, one week, etc) the operator must ensure that:
    a. as soon as reasonably practicable following receipt of a self-exclusion order, no new bets or deposits are accepted from that customer, until such time as the temporary self-exclusion has expired; and
    b. during the temporary self-exclusion period, the customer is not prevented from withdrawing any or all of their cleared account balance.

4.2.3 Involuntary Exclusion

1. Where operators exclude customers they must keep a record of the reason(s) for the exclusion (e.g. harassing help-desk staff, harassing other customers, etc).
2. Immediately upon activating the exclusion, no new bets or deposits are to be accepted from that customer, until such time as the exclusion has been revoked.
3. During the exclusion period, the customer must not be prevented from withdrawing any or all of their account balance, provided that the system acknowledges that the funds have cleared, and that the reason(s) for exclusion would not prohibit a withdraw (e.g. suspect of money laundering, suspect of cheating, etc).

4.2.4 Responsible Gaming Features

1. Customers must be provided with straight-forward and easily accessible methods to limit their gambling.
2. The self-limitation mechanisms must include at least one of the following options:
    a. spend limit over a specified time period (e.g. daily, weekly, etc);
    b. loss limit per time period – an overall maximum loss limitation over a specified period of time (e.g. daily, weekly, etc);
    c. deposit limit per time period – an overall maximum deposit limitation over a specified period of time (e.g. daily, weekly, etc);
    d. individual session duration limit– a limitation on the duration of each individual gambling session; or
    e. cumulative session duration limit per time period – a limitation on the length of time a customer may gamble within a specified time period.

3. As soon as practicable, following receipt of any self-limitation order, the operator must ensure that all specified limits are correctly implemented in the system.
4. Once established by a customer, if the limit is being reduced (tightened), the change shall happen no later than the next login, however, if the customer is increasing (loosening) their limit, the change should occur after the previous limit's period has ended.
5. Limits must not be compromised by external time events, such as leap-years and daylight savings adjustments.
6. Limits must not be compromised by internal status events, such as self-exclusion orders and self-exclusion revocations.
7. The IGS shall ensure that if the patron exceeds a deposit threshold, the IGS shall immediately prevent any wagering until the patron acknowledges the deposit threshold and is informed they have the ability to establish responsible gaming limits.
8. Operators shall monitor player behaviour to proactively identify problem gambling for possible intervention (Intervention could be subtle messages listing the range of responsible gambling options available to customers to more overt intervention as determined by the operator). Such behaviour could include:
    a. multiple account deposits within a short time period;
    b. abnormal amount of new funding methods being used for deposits;
    c. excessive time spent gambling;
    d. noticeable increase in gambling activity compared to normal account activity; or
    e. problems indicated in communications between the customer and operator.

4.2.5 Involuntary Limitation

1. Operators may set their own customer limits.
2. Customers must be informed of any such limits.
3. The lower of the two limits must always apply.

4.2.6 Complaints

1. Jurisdictions may have relevant generic legislation or regulations that address consumer complaints and disputes. This section is intended to provide useful guidance to those jurisdictions that do not have relevant requirements.
2. Operators must provide clear and easily accessible information to customers on their website about their complaints procedure including:
    a. how to make a complaint against the operator; and
    b. adjudication of complaints by the regulator or approved third party.
3. Operators must retain customer gambling transaction data so that it:
    a. complies with data retention requirements;
    b. enables complaints to be resolved; and
    c. retains information that may be required for investigations by the regulator, other third party adjudicators or other approved bodies.

More information on data logging can be found in section 10 and information security in section 9 of this document.

4.2.7 Last Log in Time Display

1. When a customer logs in to the IGS, the last time the customer logged in must be displayed to the customer without the customer's intervention.

4.2.8 Balance Display

1. Current account balance must be displayed in currency (as opposed to credits).

4.2.9 Customer Activity Statement

1. Customer activity statements must be easily available to the customer and must give sufficient information to enable them to review their previous gambling and account transactions.
2. Statements must include sufficient information to allow the customer to reconcile the statement against the customer's own records.
3. All customer account activity information retained by the operator must be available to the customer for a reasonable timeframe.

4.2.10 Transaction Logging

1. Adequate on-site transaction logging of customer accounts must occur in order to ensure that dispute resolution is transparent (for detailed guidelines, please refer to the data logging guidelines section of this document).
2. Adequate backups of customer account transactions must occur in order to ensure all customer account balances can be recovered in the event of a disaster rendering the IGS inoperable (for detailed guidelines, please refer to the data logging guidelines section of this document).

5. Generation of Random Outcomes

5.1 Overall Objective:

The objective of this guideline is to recommend random number generator (RNG) controls are in place to ensure the integrity of gambling is not compromised.

5.2 Good Practice Guideline:

5.2.1 General

"Game outcomes" include, for example, the selection of symbols, ordering of cards, position of dice, determination of the result of a virtual race and any other events determined by reference to the output of an RNG.

1. Any RNG output used for determining game outcomes must be demonstrated to:
    a. be statistically independent;
    b. be uniformly distributed (within statistically expected bounds) over their range;
    c. pass various recognised statistical tests intended to demonstrate the absence of patterns; and
    d. be unpredictable without knowledge of the algorithm, its implementation, and the current seed value (all of which must be secure).
2. Any forms of seeding and re-seeding must not introduce predictability.
3. The range of the RNG must be sufficient to support the games that utilise its output.
4. Scaling of raw RNG outputs into specific number ranges for use in games must not introduce any bias, pattern or predictability.
5. It must be demonstrated that the method used to convert RNG output into game outcomes ("mapping") creates the expected distribution of outcome probabilities for the game.
6. Game outcomes must not be influenced, affected or controlled by anything other than RNG outputs used in accordance with the rules of the game. *Note: this does not prohibit metamorphic games or jackpots determined by means other than individual game outcomes from being considered on a case-by-case basis.*
7. RNG outputs must be used to generate game outcomes in the order in which they are received, in accordance with the rules of the game. Valid RNG outputs and game outcomes must not be manually or automatically discarded.
8. Security of generated numbers must be maintained through to their usage (e.g. numbers are not transmitted unencrypted between RNG server and game server). RNG output and game symbols should be used immediately and should not be unnecessarily stored in memory before use.
9. When random numbers, scaled or otherwise, are received, e.g. following a game requesting a sequence of random numbers, they are to be used in the order in which they are received. For example, they may not be discarded due to adaptive behaviour.
10. Numbers or sequences of numbers are not to be discarded, unless they fall outside the expected range of numbers required by the virtual event – such an occurrence should result in an error being logged and investigated.
11. Where required the game or system should monitor the game output on a defined

periodic or volume basis. The purpose of monitoring is early detection of abnormal behaviour enabling timely appropriate remedial action. Any abnormalities (e.g. the actual RTP for the period falling outside the expected range) should result in an error being logged and escalated for investigation.

5.2.2 Mechanical RNGs

1. For games that use the laws of physics to generate game outcomes ("mechanical RNGs") the mechanical RNG must also meet the following guideline:
    a. components must be constructed of materials that will not degrade before their scheduled replacement lifecycle;
    b. the properties of the items used must not be altered; and
    c. customers must not have the ability to interact with, come into physical contact with, or manipulate the components.

5.2.3 Software RNGs

1. Where software algorithms are used to generate random numbers the method of reseeding must be appropriate for the usage of the random numbers and ensure the software operates in a random way. For example, reseeding must take place before the RNG output pattern repeats.

5.2.4 RNG Failure

1. In the event of an RNG failure, games that rely upon that RNG must be made unavailable for gambling until the failure is rectified or the RNG replaced.
2. Systems must be in place to quickly identify any failure of the RNG (for example, if a short sequence is repeated, the output is outside the RNG's range, or if the output is a constant flow of the same value).

6 Game Guidelines

6.1 Overall Objective:

The objective of this guideline is to ensure that a game is conducted in a way that is fair and open to the player and in accordance with the rules provided to the player.

6.2 Good Practice Guidelines:

6.2.1 Information about the Rules of the Game

1. For each game, an explanation of the applicable rules must be easily available to the customer before they commit to gamble.
2. The availability of game rule information must be checked regularly; where the information is not available the game must not be made available for gambling.
3. The published game information must be sufficient to explain all of the applicable rules and how to participate.
4. As applicable, the game information must include the following *minimum* information:
    a. the name of the game;
    b. the applicable rules, including clear descriptions of what constitutes a winning outcome;
    c. any restrictions on play or betting, such as any play duration limits, maximum win values, etc;
    d. the number of decks or frequency of shuffles in a virtual card game;
    e. whether there are contributions to jackpots (“progressives”) and the way in which the jackpot operates, for example, whether the jackpot is won by achieving a particular outcome;
    f. instructions on how to interact with the game; and
    g. any rules pertaining to metamorphosis of games, for example, the number and type of tokens that need to be collected in order to qualify for a feature or bonus round and the rules and behaviour of the bonus round where they differ from the main game.
5. For multi-state or metamorphic games, as the game progresses, clear information sufficient to inform the customer about the current state of the game must be displayed on screen in text and/or artwork. For example:
    a. where a game builds up a collection of tokens (symbols, etc) the current number collected must be displayed; and
    b. where different rules apply an indication of the rules that are currently relevant, such as “bonus round” or other feature labels.
6. The rules of the game must not be unfair or misleading.
7. Game rules must not be changed during a session unless adequate advance notification is given to customer. (where customers have incomplete games, etc).
8. Game rules must not be changed between a customer making a bet and the result of the bet being generated and calculated. For jackpots, parameters must not be altered once customer(s) have contributed to the jackpot.
9. All information presented on the website 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).

6.2.2 Information about Prizes and the Chances of Winning

1. For each game, information about the likelihood of winning must be easily available to the customer before they commit to gamble. Information must include:
    a. a description of the way the game works and the way in which winners are determined and prizes allocated, for example, for peer to peer games where the likelihood of winning is influenced by the relative skill of the participants or for Bingo where the likelihood of winning is not known at the outset because it is dependent on the number of participants, a description of the way in which prizes are won or allocated is sufficient; and
    b. the theoretical return to player (RTP%) percentage which may be appropriate for a slot machine style games or other games of chance. Where games involve some element of skill the published RTP must be based on the theoretical RTP% generated by a strategy that is reasonably achievable by a customer.
2. Where games include jackpot or progressive jackpot amounts, the published information must disclose whether this is included in the overall RTP% for the game.
3. For each game, information about the potential prizes and/or payouts (including the means by which these are calculated) must be easily available. This must include, where applicable:
    a. paytables, or the odds paid for particular outcomes;
    b. for peer-to-peer games, where the prize is determined based on the actions of the participants, a description of the way the game works and the rake or commission charged;
    c. for lotteries and other types of events where the potential amount or prize paid out may not be known before the customer commits to gamble, describing the way in which the prize amount is determined will be sufficient; and
    d. displays of jackpot amounts that change over time ("progressives") must be regularly updated and as soon as possible after the jackpot has been reset following a win.

6.2.3 Play for Fun Games

1. Play-for-fun games must accurately represent the for-money version of the game; in particular they must not be designed to mislead the customer about the likelihood of winning in the for-money version of the game, by for example, using mappings or different probabilities that produce different outcome likelihoods.

6.2.4 Game Displays

1. The name of the game must be displayed on game screens.
2. The game must display the unit and total stake for the customer's gamble including conversions to other currencies or tokens.
3. The information displayed about the game result must be sufficient for the customer to determine whether they have lost or won and the value of any winnings.
4. Game results must be displayed for a reasonable period of time, that is, sufficient time for the customer to be able understand the result of the game in the context of

their gamble.

6.2.5 Game Fairness

1. Games must operate and interact with the customer strictly in accordance with the published rules.
2. Games must not be designed in such a way as to mislead the customer about the likelihood of winning, by for example, substituting one losing outcome with another that represents a “near-miss”, in order to encourage a customer to believe that they came close to winning and continue gambling.
3. Games must not be designed to give the customer the perception that skill influences the outcome of a game when it does not (i.e. where the outcome is entirely random).
4. Where a game is represented or implied to include a simulation of a real-life physical device, the behaviour of the simulation must replicate the expected behaviour of the real-life physical device. For example:
    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 (e.g.: the probability of obtaining a 6 on a simulated die throw must be equal to 1 in 6);
    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 a real-life physical device that has no memory of previous events, the behaviour of the simulation must be independent of (i.e.: not correlated with) the previous behaviour.
5. If a cap is established on any jackpot, all additional contributions once that cap is reached must be credited to the next jackpot.
6. If the artwork contains game instructions specifying a maximum win, then it must be possible to win this amount from a single game (including features or other game options).
7. All customers contributing to a jackpot must be eligible to win that jackpot.

6.2.6 No Adaptive Behaviour by Games

1. Games must not be “adaptive” or “compensated”, that is, the probability of any particular outcome occurring must be the same every time the game is played, except as provided for in the (fair) rules of the game.
2. The rules of the game must not provide for manipulations of return to customer percentage based on previous turnover or money paid out, or to maintain a constant return to customer percentage.
3. Restricting adaptive behaviour prohibits automatic or manual interventions that change the probabilities of game outcomes occurring during play. Restricting adaptive behaviour is not intended to prevent games from offering bonus or special features that implement a different set of rules, if they are based on the occurrence of random events.

6.2.7 No Forced Game Play

1. The customer must not be forced to play a game simply by selecting it.
2. A mechanism must be implemented to prevent repeated gamble instructions, (for

example, where a customer repeatedly presses “play” while waiting for a game result) to be executed.
3. Edges of the “hot” area of buttons must be clearly defined in the artwork to prevent clicking near buttons from triggering a gamble.

6.2.8 Games in Multiple Languages

1. The following principles must be followed where games are provided in different language versions:
    a. all game information must be provided in the language specified for that version;
    b. the game instructions (and restrictions) must carry the same meaning across all language versions so that no one version is advantaged or disadvantaged; and
    c. where a customer may elect to play in multiple different language versions of a game they must have the same likelihood of winning regardless of which language version they choose to play.

6.2.9 Autoplay

1. The customer must retain control of the gambling where autoplay functionality is provided. The autoplay functionality must:
    a. require the customer to choose the stake, the number of auto-play gambles or the total amount to be gambled;
    b. enable the customer to stop the auto-play regardless of how many auto-play gambles they initially chose or how many remain; and
    c. Not override any of the display requirements (e.g. the result of each gamble must be displayed for a reasonable length of time before the next gamble commences.

6.2.10 Game Play

1. Customers must be provided with a means to review the last game, 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. the display associated with the final outcome of the game;
    c. total customer cash / credits at start and end of play;
    d. amount gambled including any multipliers (e.g.: number of lines played, and cash/credits bet per line);
    e. total cash/credits won for the prize resulting from the last play (including progressive jackpots);
    f. any customer choices involved in the game outcome; and
    g. results of any intermediate game phases, such as gambles or feature games.

6.2.11 Game Disable

1. It must be possible for the operator to disable any game or game session without any unfair impact on the customer.
2. The operator must provide full audit trails when disabling a game that is currently in

play.

6.2.12 Incomplete Games

1. Where a game can have multiple states, or stages, (multi-state), the system must provide a method for the customer to return to the incomplete game to complete it.
2. The operator must provide a mechanism for a customer to complete an incomplete game before a customer is permitted to participate in any other game. Incomplete games may occur as a result of:
    a. loss of communications between operator and end customer device;
    b. operator restart;
    c. game disabled by operator;
    d. end customer device restart; and
    e. abnormal termination of gambling application on end customer device.
3. Gambles associated with a partially complete game that can be continued must be held by the operator until the game completes. Customer accounts must reflect any funds held in incomplete games.
4. The operator must ensure customer fairness, to the extent possible, in the event of a communication loss to one or more end customer devices during a multi-customer game.
5. Game rules must cater for situations where the operator loses connectivity with the customer.

6.2.13 Multi-Customer Games

1. Multi-customer games (e.g.: Poker) with outcomes that can be affected through collusion between customers must contain functionality and enabling technology such as clear rules, compensating controls and other technology to minimise the risk of cheating (some of the controls to detect and prevent collusion will be operational controls outside the scope of game software).
2. Multi-customer games with outcomes that can be affected through the use of automated electronic devices or ancillary computer systems must have warnings in the game rules so that customers can make an informed decision whether or not to participate.

6.2.14 Peer to Peer Gaming

1. Where operators use programs to participate in gambling on their behalf in peer-to-peer gambling (e.g. “robots”), information must be displayed, which clearly informs customers that the operator uses this kind of software.
2. Where peer-to-peer(s) customers may be gambling against programs deployed by other customers to play on their behalf, information must be made easily available that describes that this is possible.
3. This information must warn customers of the risks of gambling against robots and of using robots themselves, that is, that the predictability of robots may be exploited by other customers.
4. If it is against the operator’s terms and conditions to use robots, information must be made easily available on how to report suspected robot use.
5. Customers must be informed where performance characteristics of networks or end-user devices may have, or may appear to have, an effect on the game, such as the

display of progressive jackpot values.

6.2.15 Monitoring Game Output

Where required the game or system should monitor the game output on a defined periodic or volume basis. The purpose of monitoring is early detection of abnormal behaviour enabling timely appropriate remedial action. Any abnormalities (e.g. the actual RTP for the period falling outside the expected range) should result in an error being logged and escalated for investigation.

7 Jackpot guidelines

7.1 Overall objective:

The objective of this requirement is to identify controls that an operator should implement to ensure that game jackpots operate correctly. Jackpots are normally prizes awarded outside of a normal games operation and additional controls are needed to ensure customer jackpot entitlements are transparent and correctly awarded to players.

7.2 Good Practice Guideline:

7.2.1 Partial Jackpot Redirection

Diversion Pool schemes, where a portion of the jackpot contributions are redirected to another pool so that, when the jackpot is won, that pool is added to the restart level of the next jackpot, must be demonstrably fair. The following guidelines apply to such schemes:

1. A jackpot redirection scheme must not have a mathematical expectation of the diversion pool of infinity.
2. Diversion pools must not be capped (unless clearly stated in the rules).

7.2.2 Multiple Jackpot Winners

The operator must address the possibility of a jackpot being won (or appearing to be won) by one or more customers at approximately the same time. The rules of the game must include resolution of this possibility.

7.2.3 Jackpot Financial Liability

The rules of the game must provide for any planned or unplanned termination / discontinuation of a jackpot. In the event a jackpot is decommissioned, the operator must ensure outstanding jackpot pool amounts are transferred to another game available for play within a reasonable amount of time (for example 30 days). The transferred amount shall be added to a progressive game with a similar player base as the original progressive.

7.2.4 Jackpot Integrity Measures

The operator shall ensure an adequate method is available to reconcile all progressives offered to ensure the progressive amount displayed to the patron is the correct amount. The data utilized for the progressive reconciliation shall be stored in a secure manner to prevent unauthorized modifications. In addition, the operator must store and maintain the following records at a minimum:

1. Total amount contributed/won (normally equal) for each previous jackpot, including separate figures for any diverted amounts.
2. Grand total amount contributed/won (normally equal) for all previous jackpots combined.
3. Total amount contributed for current jackpot, including separate figures for any diverted amounts.

7.2.5 Jackpot Recovery

In order to enable the recovery of the current value of the jackpot amount in the case of an operator failure:

1. The current value of the jackpot amount must be stored in a redundant manner, or
2. The current value of the jackpot amount must be able to be accurately calculated from other available records that are not stored in the same system as the jackpot amount.

7.2.6 Linked Progressive Games

An operator my offer two or more linked games on the same progressive jackpot with different denominations and/or minimum wagers required to win the progressive, provided that the probability of winning the progressive jackpot is directly proportional to the minimum wager required to win that jackpot.

8 System Disclosure Guidelines

8.1 Overall Objective:

The objective of this guideline is to specify the information that may be required by the regulator or body authorised by the regulator to assess the suitability of the eGambling system or some of its components.

The issue of independent testing of gambling systems is primarily a compliance issue and jurisdictions will have their own approaches in this area. However, this section sets out the information and systems that operators should have in place so that regulators, inspectors or test houses can have access to relevant information.

8.2 Good Practice Guideline:

8.2.1 General Statement

Where required, operators must make available all results of in-house testing (including quality assurance) and system overview diagrams.

8.2.2 Source Code

For new or modified systems, RNG's or games the source code shall be commented in an informative and useful manner and able to be compiled. The following source code information must be made available:

1. File / module / function name(s).
2. Brief description of file / module / function purpose(s).
3. Edit History, including who modified it, when and why.

8.2.3 Documentation

For the base system (ie. the underlying website platform) the following documentation must be available:

1. A list of all gambling products and individual games hosted / offered on the base website.
2. An all-inclusive functional description of the base website (including website home page and all website peripheral pages).
3. Detailed functional descriptions of the following processes:
    a. Customer Account Registration;
    b. Customer Account Login (Username & Password);
    c. Customer Interface to Customer Account;
    d. Operator Interface to Customer Account;
    e. Operator Accounting and Financial Reporting Capabilities;
    f. Customer Protection / Responsible Gaming Features;
    g. Fraud Detection System;
    h. Operator Payment Systems & Financial Institution Interfacing;

i. Customer Location & Identity Verification Software; and
j. Customer Account Deactivation.

For the games that run on the base system the following documentation must be available:

1. Game name.
2. Game version number(s).
3. Paytable version number(s).
4. Detailed game rules, including all options and bonus features.
5. Detailed breakdown of all paytables, payouts and mapped symbols present in the game.
6. A formal mathematical treatise of the derivation of the theoretical Percentage Return to Player (%RTP) of the game.

For RNG's the following documentation must be available:

1. A list of all games connected to the RNG (including the associated mathematical Degrees of Freedom (DOFs) for each game).
2. For hardware-based RNGs:
    a. type of hardware device used;
    b. technical specifications for hardware device;
    c. methods of connecting hardware device to operator software; and
    d. details of all RNG / game implementation, including methods of scaling and mapping.
3. For software-based RNGs:
    a. type of mathematical algorithm used;
    b. full details, in technical terms, of random number generation process and mathematical algorithm theory;
    c. details of the mathematical algorithm's period;
    d. details of the mathematical algorithm's range;
    e. details of the methods for seeding (and re-seeding);
    f. details of the methods for background cycling / activity; and
    g. details of all RNG / game implementation, including methods of scaling and mapping.

9 Security Guidelines

9.1 Overall Objective:

The objective of the security guidelines is to ensure the protection of the systems against threats and secure information stored in the systems. A number of significant safety issues are safeguarded by ensuring the integrity of and access to the systems. Through the protection of sensitive information, concerns regarding confidentiality are met not only with regards to the operator, but also with regards to players and third parties. For the purposes of this section, the term “users” are in reference to operator/platform provider’s user accounts.

Controls should be implemented that are consistent with current information security principles such as ISO 27001 or equivalent in relation to confidentiality, integrity and availability. Operators that comply with ISO 27001 or equivalent are likely to comply with many of these guidelines but for jurisdictions that do not currently specify guidelines the following is suitable.

9.2 Good practice Guideline:

9.2.1 General Principles

1. There are three broad categories of threats to operator’s systems, these include, but are not limited to:
    a. *Hardware Failure* – including power loss to the whole system or other disasters, hard drive failure, overheating causing shut down;
    b. *External Threats* – from people unknown who attack the system from the outside, including DDOS attacks, Hackers, Crackers ,”Social Engineering” attacks, Viruses, Worms;
    c. *Internal Threats* – from staff or other individuals with system access that cause damage, or loss of data through errors, ignorance of procedures, malicious intent.
2. To minimise threats to operator’s systems they must have in place security policies, procedures, and mechanisms to ensure that:
    a. sensitive customer data remains confidential and is protected from theft and misuse;
    b. customer account details are available to authorised people only;
    c. the integrity of gambling and account transactions can be assured and there is an audit trail of modifications to accounts and gambling transactions;
    d. customer transactions are not lost through events such as systems failures, or unauthorised modification by entities internal or external to the operator; and
    e. the software that determines the results of games must be protected from unauthorised modification.

9.2.2 Critical Systems

As a minimum the following systems must be adequately protected:

1. Systems that record, store, process, share, transmit or retrieve sensitive customer information, e.g. credit/debit card details, authentication information.

2. Systems that generate, transmit, or process random numbers used to determine the outcome of events.
3. Systems that store the results or state of events.
4. All points of access, either physical or electronic to any and all of the above systems (other systems that are able to communicate directly with core critical systems).
5. Communication networks that transmit sensitive customer information.

9.2.3 Detailed Security Guidelines

9.2.3.1 Security policy and training

1. Operators must have an up-to-date security policy that is regularly reviewed by management.
2. Staff with direct access to critical systems must receive security training appropriate to their role.

9.2.3.2 Third party Security Assessment

1. Operators must ensure that a suitably qualified third party assesses the security of their systems annually and after any significant changes that are likely to affect the security of systems (such as change of hosting facilities, or new access media).
2. An annual penetration test and quarterly vulnerability scans, conducted by a third party, is strongly recommended for systems connected to the Internet.

9.2.3.3 Other Third Party Agreements

1. Agreements with third parties providing hosting and/or other services to the gambling system must contain a provision for implementation of appropriate security measures.
2. The operator must have policies and procedures for managing third parties and monitoring adherence to security requirements.

9.2.3.4 Physical Protection of Equipment

1. Hardware used for operating the systems must be protected by physical access control. The level of access control can be adjusted based on the criticality of the systems.
2. Equipment holding data backups must be stored securely.
3. Production and test/development facilities must be logically and/or physically separated.
4. Equipment used to store sensitive data must have data securely removed before disposal.

9.2.3.5 Backup and Redundancy

1. Adequate provision of data backups and system redundancy must be implemented to protect customers from potential financial loss due to loss of data. The systems and associated procedures must be tested regularly.

9.2.3.6 Network Security

1. Systems must be implemented in such a way that devices in the same broadcast domain shall not allow any alternate network paths to bypass the firewall.
2. Firewalls must be dedicated to firewall operations and shall only contain administrative accounts and firewall related applications.
3. Appropriate network segregation must be implemented.
4. Electronic transactions between the operators and customers, and operators and third parties passing over public networks must be protected from unauthorised message modification, disclosure, duplication or replay.

9.2.3.7 Access Control

1. Operators must maintain an up to date access control policy so access to systems is controlled and only those users with specific authorisation have access. The granting and revocation of system access must be done in a timely and controlled manner.
2. Access control restrictions on network functions must be enforced and user access shall only be possible through this access control. The system shall prevent unauthorised internal and external access to network functions.
3. All users shall have a unique identifier/user ID for their personal use only and systems shall enforce suitable authentication techniques to ensure confirmation of the identity of each user at log in.
4. The system shall enforce the use of strong passwords in relation to user access to the systems as well as timed log-outs or screen savers for inactive access points.
5. Users must be required to follow good practice in the selection and use of passwords which shall be changed regularly.
6. Audit logs must be kept secure and protected from unauthorised access or modification.

9.2.3 Sensitive Data and Encryption

1. Operators must have and implement appropriate policies and procedures for the use of encryption and the management of cryptographic keys.
2. Sensitive data such as credit and debit card details and passwords must be protected from unauthorised viewing by implementing encryption.
3. Any sensitive or confidential information maintained by the operator must be stored in areas of the system that are secured from unauthorised access, both external and internal and encrypted.

9.2.3.9 Monitoring

1. The systems shall maintain audit logs, which records:
    a. staff member's user activities;
    b. exceptions; and
    c. information security events.
2. Faults must be logged, analysed and appropriate action taken.

9.2.3.10 Time Synchronisation

1. All relevant system clocks must on a suitable interval undergo time synchronisation through an authoritative time server.

9.2.3.11 Protection of Critical Systems

1. Critical systems must be protected from the unauthorised execution of mobile code. Mobile code is executable code that moves from computer to computer, including both legitimate code and malicious code such as computer viruses.
2. Adequate audit logs for critical systems must be maintained to enable investigations to determine who did what and when, for example, amending customer balances, changing game rules or pay-tables, or administrator or root level access to critical systems.
3. Applications must implement appropriate data handling methods, including validation of input and rejection of deliberately or unintentionally corrupt data.
4. In the event the system is breached, a mechanism shall be in place to notify regulators in an expeditious manner.

10 Data Logging Guidelines

10.1 Overall Objective:

The objective of this requirement is to identify key information that should be logged and retained by an operator to ensure that critical historical information and transactions are available for review if required. The operator must be capable of retaining and backing up all relevant information as well as providing the regulator with the ability to export the below logs upon request without the operator's assistance (if required by the jurisdiction). There may be local requirements for the length of time such records are required to be kept.

10.2 Good Practice Guidelines:

10.2.1 Customer Account Information

1. The operator must maintain and back up the following customer account information:
    a. customer identity details (including customer identity verification results);
    b. account details (including changes to these details) and current balance;
    c. any self-imposed customer protection measures (including self-exclusion and self-imposed limits);
    d. details of any previous accounts, including reasons for deactivation;
    e. deposit / withdraw history; and
    f. gambling history (i.e.: games played, amounts bet, amounts won, jackpots won, etc).
2. The operator must be capable of producing the following customer account information:
    a. active customer accounts;
    b. inactive customer accounts (including reasons for deactivation);
    c. accounts for which the customer has currently (or previously) imposed a customer protection self-exclusion;
    d. accounts for which the customer has currently (or previously) been excluded from the site by the Operator (i.e.: involuntary exclusion);
    e. accounts for which the customer's funds have currently (or previously) been inactive for a period of time exceeding 90 days; and
    f. accounts for which one or more of the customer's deposits and/or withdraws have exceeded an Operator-configurable 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.

10.2.2 Gambling Session Information

1. The operator must maintain and back up the following gambling session information:
    a. unique customer ID;
    b. gambling session start and end time; and
    c. gambling information for session (i.e.: games played, amounts bet, amounts won, jackpots won, etc).

2. The operator must be capable of reporting the following gambling session information:
    a. current active gambling sessions; and
    b. interrupted sessions.

10.2.3 Game Information

1. The operator must maintain and back up the following game information:
    a. unique customer ID;
    b. unique game identifier;
    c. game start time, according to operator;
    d. customer account balance at start of game;
    e. amount wagered;
    f. contributions to jackpot pools (if any);
    g. current game status (e.g.: in progress, complete, etc…) (note: the operator must maintain records of any game that fails to complete, and the reason why the game failed to complete);
    h. game result / outcome;
    i. jackpot wins (if any);
    j. game end time, according to operator;
    k. amount won; and
    l. customer account balance at end of game.
2. The operator must be capable of reporting the following information on active games:
    a. game name;
    b. game type;
    c. version number; and
    d. pay table details.

10.2.4 Significant Event Information

1. The operator must maintain and backup a log of all significant events on the system: including:
    a. game enabled/disabled;
    b. changes made by the Operator to game parameters;
    c. changes made by the Operator to jackpot parameters;
    d. new jackpots created;
    e. jackpot wins;
    f. jackpot shutdowns;
    g. switch to Disaster Recovery (DR) systems;
    h. irrecoverable loss of customer-related data; and
    i. significant periods of system unavailability.
2. Where an operator uses external computer systems (ie an external RNG or suite of games) it must be able to maintain a log of significant events for those systems.

11 Shut Down and Recovery

11.1 Overall Objective:

The objective of this requirement is to ensure that operators' systems maintain data and gambling session integrity following an unexpected event or planned system shutdown.

11.2 Good practice guidelines:

1. The operator must be able to perform a controlled shut down in the event of a power failure, and not restart automatically on power up.
2. In the event of a critical hardware / software failure, the operator 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 (no time limit is specified).
3. The operator must have disaster recovery capability sufficient to ensure customer entitlements are protected and there is a full audit trail up to the point of the disaster.
4. The operator's systems must be able to recover from unexpected restarts of its central computers or any of its other components.
5. The operator hardware platform and Operating System (OS) must be proven to be reliable.
6. The operator must have a mechanism whereby all gambling offered on the operating system can be disabled, as a whole, by the operator – with full consideration to the associated requirements listed above.

12 Advertising and Marketing

12.1 Overall Objective:

The objective of this guideline is to identify socially responsible measures for advertising and marketing. Some jurisdictions may have legislation for advertising and marketing of gambling however where a jurisdiction does not have such measures the following are applicable. Relevant legislation takes precedent over this guideline.

12.2 Good Practice Guidelines:

An Advertising and Marketing Policy must be put in place to address the following guidelines:

1. Advertising and marketing must be truthful.
2. Advertising and marketing must not bring the operator or the regulator into disrepute.
3. Advertising and marketing must not target minors (under the age of majority). Media selection, content and placement must reflect this.
4. Advertising and marketing must not use individuals who are, or appear to be, minors (under the age of majority) to promote gambling.
5. Advertising and marketing must not present winning as the most probable outcome, nor misrepresent a person's chances of winning a prize.
6. Advertising and marketing must not encourage excessive participation or challenge or dare people to participate.
7. Advertising and marketing must not encourage people to play beyond their means.
8. Advertising and marketing must not imply the certainty of financial reward or alleviation of personal and financial difficulties.
9. Advertising and marketing must not encourage play as a means of recovering past gambling or financial losses.
10. Advertising and marketing must not suggest that skill can influence the outcome, or imply that the chances of winning increase the longer one plays (outside of the factual impact of customer skill in conjunction with the rules of game play).
11. Advertising and marketing must not imply or convey a message that one's status, general abilities or social success can be attributable to gambling.
12. Where advertising and marketing describes prize amounts, it must describe prize amounts accurately, indicating (where necessary) if prizes are in the form of an annuity.
13. Winning must not be shown out of context with the reality of the Percentage Return to patron (%RTP) and must not promote any unrealistic expectation of winning.
14. Operators must ensure that they do not use customer information to market products irresponsibly.
15. Operators must be required to discontinue as expeditiously as possible the use of a particular advertisement, promotion or program upon receipt of regulatory notice that the use of the particular advertisement, promotion or program could adversely impact the public or the integrity of gaming.
16. Marketing material should include a reputable responsible gaming service and include the responsible gaming service's phone number.
17. The use of third parties for marketing purposes requires the primary operator to be responsible and ensure all required regulations are upheld including any restriction on marketing to excluded customers.

12.3 Bonus Guidelines:

1. Where bonus marketing is allowed by jurisdiction, operators may only offer bonuses that are responsible.
2. The bonus terms must be correct, formulated correctly and relevant.
3. Individual terms must not give rise to misunderstandings, ambiguity and misinterpretation.
4. Terms should not contain unnecessary information.
5. As a rule, all bonus terms must be disclosed in a clear and lucid manner within the immediate context (first presentation) of the bonus offer.
6. Depending on the marketing channel (media type) it is not always possible to show all bonus terms at the first presentation of the bonus. In such situations the bonus offer must be described in a clear, loyal and balanced manner with regard to the terms, including benefits and restrictions. Essential terms should however, always be shown at the first presentation of the bonus offer. The following terms could be considered essential:
    a. the bonus only applies to a limited group (e.g. new customers);
    b. deposit requirements;
    c. wager requirements including information of games, which may not be covered by the bonus offer or if bets must be placed using a specific minimum odds; and
    d. time limits.
7. When using media types with limited space (e.g. AdWords or small banner ads on third party websites) it can be necessary to refer to another media (e.g. the operator's website) for additional information. In these situations it should always be mentioned that terms apply and a link leading directly (one click) to the relevant terms and the bonus offer in its entirety must be provided.

13 Anti-Money Laundering guidelines

13.1 Overall Objective:

The objective of this requirement is to identify controls that an operator should implement to minimise the potential for money laundering activities. This includes methods for detecting potential money laundering and reporting suspicious activity to the appropriate bodies.

Many worldwide jurisdictions are subject to Financial Action Task Force (FATF) requirements and may have supporting FATF compliant regulations. Where such regulations are in place a regulator will need to ensure any anti-money laundering requirements comply with the appropriate local regulations as well as international compliance requirements.

13.2 Good Practice Guidelines:

13.2.1 General Anti-Money Laundering Controls and Objectives

1. In support of anti-money laundering efforts world-wide, the operator must ensure that documented technical procedures and policies are put in place in order to satisfy the following objectives:
    a. that it be possible to effect account closures in order to halt suspected money-laundering;
    b. that it be possible to impose general or risk-based deposit limits on customers in order to reduce the overall exposure to money-laundering. Such limits must not be invoked in response to suspected money-laundering activity in order to avoid alerting the suspect to a potential investigation;
    c. that customer accounts be monitored for opening and closing in short time frames;
    d. that customer accounts be monitored for deposits and withdrawals without associated game play;
    e. that cheques and Electronic Fund Transfers (EFTs) be reviewed and returned to customers marked “Account Closure” or “Over-contribution”, and be identified separately from a win;
    f. that all suspicious activity reports be reported to the appropriate body in compliance with anti-money laundering regulations implemented within the jurisdiction;
    g. aggregate transactions over a defined period of time may require further customer due diligence checks and may be reportable to the relevant organisation if they exceed the threshold prescribed by that jurisdiction; and
    h. in calculating amounts paid to or received from a customer, take into account all payments used by the customer or operator.
2. Payments from a customer’s account must be paid directly to an account with a financial institution in the registered name of the customer, or made payable to the customer and forwarded to the customer’s registered address. Restricted accounts should only be permitted for a limited time period specified by the regulator.
3. A customer must not be permitted to deposit funds to a gambling account from one

bank account[1] and subsequently withdraw to a different bank account without appropriate controls to keep track of the movement of funds[2].

4. A customer must not be permitted to move money into another customer's account, except as permitted in the rules of peer-to-peer gambling. Where it is permitted, the movement of money to other customer accounts must be monitored and supervised by the anti-money laundering regime.
5. Where the customer's account is to be closed, any money left in the account must be remitted to the customer using the registered name and address, except where criminal activity is being investigated, in which case such account must be frozen.
6. All changes made to customer's contact details must be recorded, including the old (replaced) details, and retained for a period stipulated by the anti-money laundering regulations in the jurisdiction.
7. Staff must be trained in anti-money laundering, and this training is to be kept up to date by regular re-training.
8. A responsible staff member will be appointed as the Anti-Money Laundering Officer, and will be responsible for all areas of anti-money laundering by the operator including ensuring the reporting of SARs.

[1] In the context of internet gambling a reference to a bank account could also be a reference to other types of money transfer into gambling accounts, for example from an e-wallet.

[2] This measure is primarily aimed at preventing financial gain from the use of stolen bank cards directly or indirectly via chip dumping

Glossary of Terms

Term	Description
%RTP	Percentage Return to Customer. The %RTP is the expected percentage of wagers that a specific game will return to the customer in the long run. The %RTP can be calculated via either a theoretical or simulated approach. The method used for calculation depends on the game type.
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.
Base Website	'Base Website' refers to operator software that drives the features that are common to all of the games, such as customer account administration, website home page, website peripheral pages (e.g.: "Legal Disclaimer", "About Us", "FAQs", etc…), and accounting and financial reporting capabilities. Any software that is not directly related to any of the games hosted / offered on the base website, and is composed of visual or auditory information that is displayed to either the customer or the Operator, is considered to be base website software.
Chip dumping	A practice in peer-to-peer gaming (for example poker) where one customer deliberately loses to another customer in order to transfer money to that customer.
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).
Dormant Account	A customer account that has no transactions initiated by the customer for 12 months.
EFT	Electronic Funds Transfer
eGambling	Gambling via remote means such as the internet, interactive television or mobile telephone
FAQ	Frequently Asked Question
FATF	Financial Action Task Force
Game	'Game' refers to operator software that is specific to each individual game that is hosted / offered on the base website. Each game is to be treated as a separate and distinct entity.
ID	Identification
operator	Interactive gambling System
ISO	International Standards Organisation
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).
Metamorphic Game	A game where free games, feature games or prizes (other than jackpots) are triggered by the cumulative result of a series of plays. (i.e. tokens are awarded during plays and are accumulated by players).
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 $^{52}P_{10} = 5.74 \times 10^{16}$. 20 balls from 80 (e.g.: Keno) requires $^{80}C_{20} = 3.54 \times 10^{18}$ possible outcomes.

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 2^{32} possible outcomes (4.29×10^{9}). If one considers a 64-bit output, one can achieve 1.8×10^{19} different RNG outcomes.
Reseeding	Reseeding is when the RNG algorithm is restarted (given new initial seed values).
RNG	Random Number Generator. Refers to operator hardware and / or software that determines random outcomes for use by all of the games hosted / offered on the base website.
SARS	Suspicious Activity Reporting
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 RNGs 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).
Whitelabel	An arrangement whereby a gambling operator hosts and provides gambling on behalf of one or more companies.