CEN

WORKSHOP

AGREEMENT

CWA 16259

January 2011

ICS 35.240.99; 97.200.99

English version

Responsible Remote Gambling Measures

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No.:CWA 16259:2011 D/E/F

Contents

Foreword

The CEN Workshop offers a mechanism whereby stakeholders can submit their standardisation and specification requirements and develop a result by consensus, validated in an open process.

In a CEN Workshop all the decision-making powers rest with the interested parties themselves, the members of the Workshop. These include all stakeholders (for example industry representatives, service providers, administrators, users) and can come from any part of the globe. They are responsible for the funding and direction of the Workshop and for the approval of the deliverables.

The main activity of a CEN Workshop is the development and publication of the CEN Workshop Agreement (CWA). The CWA is a voluntary standard applicable internationally and does not have the force of regulation.

This CWA sets out the Control Measures required to achieve the promotion of responsible remote gambling.

The CEN Workshop commenced in May 2010 and held its plenary meeting on 6 September 2010.

Participant comments and a public consultation process took place between 25 July and 25 November 2010.

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN-CENELEC Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

A list of the individuals and organizations which supported the technical consensus represented by the CEN Workshop Agreement is available to purchasers from the CEN-CENELEC Management Centre. The CEN Workshop involved 27 participants from the remote gambling sector, including representatives of trade associations, licensing authorities, experts on gaming behaviour, associations of players, software providers and operators. In addition, three parties were involved in the development as an observer, namely the European Commission, Gamcare UK and the French National Standards Body AFNOR. The secretariat was held by the Dutch National Standards Body NEN.

Khalid Ali	ESSA
Andrew Beveridge	eCOGRA Limited
Birgit Bosch	Interwetten
Gerhard Bühringer	TU Dresden

Kristoffer Cassel	Unibet
Oliver Chubb	International Federation of Poker
George Debrincat	Malta Remote Gaming Council
Nicolas Gibbon/ Tim Philips	BetFair
Marie Cecile Grisard	PMU
Sue Harley	Ladbrokes
Jörg Häfeli	Hochschule Luzern
Maarten Haijer	EGBA
Clive Hawkswood	RGA
Joachim Haeusler	Bwin
Helmut Kafka	Automatenverband Austria
Michael Levi	Cardiff University
Sigrid Ligne	EGBA
Lisa Lombardi	Mangas Gaming
Melody Morgan-Busher	Rapporteur to Malta Standards Authority
Thomas Murphy	William Hill Org LTD
Tex Rees	eCOGRA Limited
Ynze Remmers	G4
Peter Reynolds	Party Gaming
Howard Shaffer	Harvard Medical School -The Cambridge Health Alliance Division on Addictions

Leon Thomas	Gibraltar Betting Gaming Association
Enric Tomas	Blueprint
Sarah Winterton	KW Communications

This CEN Workshop Agreement is publicly available as a reference document from the CEN National Members of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

Comments or suggestions from the users of the CEN Workshop Agreement are welcome and should be addressed to the CEN-CENELEC Management Centre.

Introduction

The objective of the CEN Workshop on 'Responsible Remote Gambling Measures' is to develop Control Measures that are:

1. capable of adequately protecting customers and ensuring that the remote gambling operators, software suppliers and associated service providers behave responsibly; and
2. provide policy makers with easy access to a set of measures that are readily and consistently understood and can be used to address the challenges of creating a safe and secure remote gabling environment.

Some aspects of remote gambling in the EU have been harmonised by specific EU directives, including the Third Money Laundering Directive, the Directive on Data Protection, the Distance Selling Directive, the Unfair Commercial Practices Directive, the Unfair Contract Terms Directive and the 8th Company Directive.

However, these directives do not cover all aspects of remote gambling and as a result, multiple different regulations, standards, codes and rules govern the European remote gambling market. In the absence of pan-European regulation, a further objective of this Workshop is to develop evidence based (to the extent possible) self-regulatory control measures as an effective complement to existing legislative requirements in order to develop and maintain - cross border - a safe and secure environment for customers throughout the EU.

Application

The requirements of this CWA are generic and are intended to be applicable to trade associations, licensing authorities, operators, software providers and associated service providers in the field of remote gambling.

This document does not in itself impose any obligation upon anyone to follow it. However, such an obligation may be imposed, for example, by legislation or by a contract. In order to be able to claim compliance with this document, the user needs to be able to identify the requirements he/she is obliged to satisfy. The user also needs to be able to distinguish these requirements from other provisions where there is a certain freedom of choice.

Contents of the informative Annex should not in any way be construed as being Control Measures.

1 Scope

This CWA specifies the Responsible Remote Gambling Measures for operators, software providers, associated service providers and other relevant industry stakeholders.

The Workshop only concerns remote gaming and betting, and the scope does not include land-based gambling activities. Remote gambling is defined as gaming and betting activities accessed by the customers via the use of the internet, telephone, television and other electronic devices used for facilitating communication.

The Control Measures contained within this CWA are not intended to replace existing legislation, but rather guide and facilitate future regulatory efforts.

2 Terms and Definitions

For the purposes of this document the following terms and definitions apply:

Term	Definition
“account”	record kept by the operator, which shall at all times be accessible to the customer, which shows the customer’s credit against the operator, including all wagers placed and all prizes won by the customer and any other debits or credits as may be permitted by the applicable terms and conditions
“affiliate”	third party website administrator providing marketing for an operator for which the affiliate in turn receives financial gain
“AML”	anti-money laundering
“AMPRO”	Anti-Money Laundering Reporting Officer
“bonus”	provision of additional economic benefits to a customer as encouragement for further customer activity, not necessarily linked to the customer’s transaction history
“cash”	operator cash in hand and on demand deposits
“cash equivalents”	short-term, highly liquid investments (including payment processor retention reserves) that are readily convertible to known amounts of cash and which are subject to an insignificant risk of changes in value
“CFT”	combating the financing of terrorism
“clearing inactive accounts”	process whereby an operator transfers funds from an inactive account, to be separately identifiable in the operator’s financial records, and made available to the customer according to the published terms and conditions
“complaint”	matter of dissatisfaction expressed by a customer which is referred to the operator
“compliance personnel”	persons authorised to act on behalf of an operator or software provider, in a capacity of ensuring compliance with applicable Control Measures, laws and regulations
“Control Measures”	measures contained in this document
“cooling-off”	process by which a customer voluntarily requests their own account be temporarily locked in order to prevent them from participating in further gambling. The cooling-off period may be anywhere from 24 hours to less than six months. For the avoidance of doubt, it is not the period of time a customer is required to wait after terminating a self-exclusion period
“combating the financing of terrorism”	combating obscure financial transactions intended to support terrorism
“cryptographic controls”	controls to hide or obscure the contents of information transfer or stored data, including encryption and hash functions
“customer”	person who is over the legal age of majority as defined by the relevant Regulatory Authority, and participates in remote gambling

Term	Definition
“deposit”	funding paid by the customer into their account
“director”	member of the board of directors of an operator or software provider
“dispute”	complaint submitted by a customer which has not been resolved by the operator and is consequently escalated to a third party mediator or arbitrator
“employees”	persons actively employed by an operator or software provider and engaged with its remote gambling operation
“fees”	costs levied to a customer as a result of a funding transaction (deposit or withdrawal) from their account, or other customer initiated actions that are subject to fees as covered by the published terms and conditions in force
“financial reconciliation”	matching of transactions with an economic value and noting those transactions where a corresponding match does not exist, for future investigation
“free play”	participation in games where no deposit was required from the customer and no actual monetary value is attributable to the customer
“gambling software”	application from which the customer accesses the games, account information and payment facilities
“gambling”	all types of games involving wagering or betting a stake with monetary value in games in which participants may win, in full or in part, a monetary prize based, totally or partially, on chance or uncertainty of an outcome
“game pay tables”	illustration, in tabular format, of the game outcome and associated payout
“inactive customer account”	account is considered inactive when there is no customer initiated activity or contact for pre-defined period of time
“jurisdiction”	practical authority granted to a formally constituted legal body to deal with and make pronouncements on legal matters and, by implication, to administer justice within a defined area of responsibility
“money laundering”	process(es) by which criminals conceal or attempt to conceal the origin of the proceeds of their or others’ criminal activities
“officer”	person who has been authorised to act on behalf of an operator or software provider, in a capacity of authority
“operator”	company conducting remote gambling activities
“payment requests”	request submitted by a customer to have funds paid out to him from his account
“payout percentage”	expected percentage of wagers a specific game will return to the customer in the long run. The payout percentage can also be calculated via either a theoretical or simulated approach
“payout”	economic value gained by the customer occurring from a favourable outcome of a game
“prize”	credits with an economic value presented to a customer in recognition of the occurrence of a pre-defined event, in favour of the customer

Term	Definition
“products”	various types of remote gambling offerings, including, but not limited to, casino, poker, bingo and sportsbook
“promotion”	provision of additional economic benefits to a customer as encouragement for further customer activity
“promotional material”	distribution of information to customers relating to offers and incentives for the customers to gamble at the operator
“random number generator” or “RNG”	computational or physical device designed to generate a sequence of numbers or symbols that lack any discernible pattern
“real money”	participation in gambling using funds and promotions attributable to the customer
“registration”	process of a customer providing the required information and taking the appropriate steps in order to open an account.
“Regulatory Authority”	local, regional or national authority giving explicit permission to operate one or various forms of gambling.
“rules”	any terms and conditions applicable to a participant of a game and details of the expected action and consequential result of a game
“self-exclusion”	process by which a customer voluntarily requests their own account be locked for a minimum period of six months in order to prevent them from further gambling with that operator during the exclusion period
“software providers”	company which develops and manages the remote gambling software
“stake”	economic value which the customer, or any third party on his behalf, has to commit in order for the customer to participate in a game and which he can lose, wholly or in part, depending on the result of the game
“system-wide regression test”	any type of software testing that seeks to uncover software errors by partially retesting a modified program. The intent of regression testing is to provide a general assurance that no additional errors were introduced in the process of fixing other problems
“theoretical statistical return percentage”	expected payout percentage from a game to a customer using optimal strategy
“timeout receipts”	deposits made by a customer where the payment processor experienced a communication error while the transaction was pending. The customer’s deposit has been deducted from their bank account but does not reflect on the recipient account until manual rectification has taken place
“uncontested funds”	funds in an account over which the operator has no claim
“underage individuals”	any person who is not over the legal of age majority as defined by the relevant Regulatory Authority
“users”	operators, software providers and relevant service providers supporting and subscribing to these Control Measures
“verification”	process of obtaining evidence, often identification documentation, substantiating an individual’s claims of identity
“virus”	a software program capable of reproducing itself and usually capable of

Term	Definition
	causing great harm to files or other programs on the same computer
“winnings”	monetary and non-monetary rewards in favour of the customer, arising from remote gambling activity
“wins”	see “payout”
“withdrawal”	funding withdrawn by a customer from their account

3 Responsible Remote Gambling Control Measures

This CWA is intended to develop measures that are capable of adequately protecting customers and ensuring that the remote gambling operators, software suppliers and associated service providers behave responsibly.

To ensure the proper protection of the customer on as many levels of gambling as possible, the CWA has nine 'Control Objectives'. These Control Objectives are the statements of the desired result or purpose to be achieved by the effective implementation of the Control Measures.

1. The protection of vulnerable customers

Users are committed to promoting socially responsible gambling, and working with customers, employees and relevant industry stakeholders to help combat problem gambling. Users should ensure that proper controls are established, implemented and enforced, and that gambling takes place in a responsible environment.

2. The prevention of underage gambling

Users should seek to implement all reasonable measures that prevent underage individuals from accessing gambling products. Users should ensure these measures address appropriate age verification, and with help from industry stakeholders and governments, work to maximise the coverage, quality and effectiveness of near real-time verification.

3. Combating fraudulent and criminal behaviour

Customers should be protected from fraud or criminal behaviour, and strict security measures and gambling supervision should be implemented and enforced to prevent fraudulent activity. Any transactions suspected of being potentially connected to money laundering or other criminal activity should be reported in compliance with the Third Money Laundering Directive (Directive 2005/60/EC)[1].

4. Protection of customer privacy and safeguarding of information

Users should ensure that the privacy and confidentiality of all customer information submitted at any point in time is maintained and protected from unauthorised or unnecessary disclosure in compliance with the Directive on Data Protection (Directive 95/46/EC) and the e-Privacy Directive (Directive 2009/136/EC) as applicable.

5. Prompt and accurate customer payments

Users should ensure prompt and accurate processing of winnings and payment requests, subject to appropriate and necessary checks and verification, and compliance with the Distance Selling Directive (Directive 97/7/EC) where applicable.

---

[1] EU directives referred to in the Control Objectives are relevant to remote gambling at 25 November 2010, and do not necessarily constitute an exhaustive list.

6. Fair gaming

Users are committed to ensuring that gaming products are subjected to continuous and rigorous independent assessment to ensure products continue to operate in a fair and random manner, and in accordance with published rules in compliance with the Unfair Commercial Practices Directive (Directive 2005/29/EC).

7. Responsible marketing

Users should endeavour to employ well balanced advertising and marketing campaigns in line with responsible gambling good practices and in compliance with the Unfair Commercial Practices Directive (Directive 2005/29/EC) and Distance Selling Directive (Directive 97/7/EC).

8. Commitment to customer satisfaction and support

Users are committed to providing customers with an enjoyable gaming experience with access to 24/7 support, where they can be assured of timely attention to complaints and resolution of disputes. Where applicable, users should ensure compliance with the Distance Selling Directive (Directive 97/7/EC).

9. Secure, safe and reliable operating environment

Users should operate gambling products within an internal control environment that is in line with good practice and in compliance with the 8th Company Directive (Directive 2006/43/EC) regarding statutory audits. The internal control environment must support a secure, safe and reliable environment through adequate governance, monitoring and continuity provisions.

The Control Measures[2] are as follows:

1. The protection of vulnerable customers

Links and information

1.01 The homepage of the operator websites should contain a clear link to the website of at least one organisation trained to assist problem gamblers, and a responsible gambling page containing the following:

- A brief statement of the operator's commitment to responsible gambling.
- A warning that gambling could be harmful.
- Advice on responsible gambling and where available a link to sources of help, including helpline numbers.

[2] Remote gambling may involve various different products, including casino, poker, bingo and sportsbetting. It is important to note that each Control Measure is not necessarily applicable to all products.

- An accepted and simple self-assessment process to determine risk potential.
- A list of the customer protection measures that are available on the site and details of how to access to these measures.
- Promotional material should not be displayed on this page.

1.02 Messages of an operator's support for the provision of problem gambling treatment, research or educational initiatives should not be misleading.

1.03 Downloaded gambling software should contain a clear reminder to the customer about responsible gambling and a link to the responsible gambling page.

1.04 Direct communication with the customer should carry a responsible gambling message, where practicable.

1.05 A clearly visible clock should be available for use by the customer at all times.

1.06 The denomination of each credit should be clearly displayed on the games screen and the currency unit should be clearly stated where multiple currency game play is available.

1.07 Customers should be provided with remote access to their account balance and account history dating back for a minimum period of sixty days, and offline access dating back for a minimum period of six months, including all deposits, withdrawals, wagers, wins, losses, fees and bonuses.

1.08 Free play games websites should provide links to the same age restriction, responsible gambling, and customer protection information as the real money sites, but need not be subject to the same verification process.

1.09 Information concerning age limits, responsible gambling, and customer protection should be provided in each language offered by the website.

Deposit limits

1.10 Customers should be able to request the setting of their own deposit limits.

1.11 There should be a clear link from the deposit page to the facility to set deposit limits and/or to the Responsible Gambling page.

1.12 The operator should enable the customer to set and review their deposit limit without undue delay through the website and/or through contact with customer services. A request to decrease a deposit limit should be implemented immediately. However, if a customer wants to increase a deposit limit previously set, a minimum waiting period of 24 hours should apply.

Cooling-off and self-exclusion

1.13 Operators should offer customers a cooling-off period from gambling activity, and reasonable endeavours should be made to prevent marketing to customers during their cooling-off period.

1.14 Operators should offer self-exclusion for a minimum of six months. The customer should, in addition, be able to request a longer self-exclusion period within operator defined increments.

1.15 Once the customer has selected the self-exclusion option, the following is required:

- The account should be locked and any funds in the account paid out, subject to appropriate and necessary checks and verifications.

- All reasonable endeavours should be made to prevent marketing to these customers.
- The customer should be provided with contact information for an organisation trained to assist problem gamblers, and encouraged to contact this organisation.

1.16 Cooling-off and self-exclusion procedures and conditions should be clearly communicated on the responsible gambling page.

1.17 A third party making an application for a customer's self-exclusion should be properly identified. Taking into consideration relevant local legal and regulatory requirements, the appropriate manager should give due consideration to the appropriate course of action.

1.18 Training should be provided to customer service employees on the issues of problem gambling and to ensure the prompt and efficient handling of correspondence relating to self-exclusion and cooling-off. Refresher courses should be undertaken as and when needed.

General

1.19 A customer should not be given credit (other than through the provision of a promotion or bonus) nor allowed a negative balance unless the Regulatory Authority permits such practice, and adequate measures have been taken to establish the financial standing of the customer and the customer has clearly consented to honour consequential debts.

1.20 A designated senior management employee should be appointed by each operator to assume responsibility for the implementation and monitoring of responsible gambling practices.

1.21 Relevant third party and business partner contractual terms and conditions should provide the operator the right to terminate the contract where that third party's conduct conflicts with the operator's responsible gambling program.

2. The prevention of underage gambling

Links and information

2.01 The homepage of the operator's websites should prominently display an age restriction determined by the Regulatory Authority, which links through to a clear message about play by underage individuals.

2.02 The operator's responsible gambling page should provide a link to a recognised filtering programme to assist customers/parents in preventing underage individuals from using gambling sites.

2.03 The operator's website terms and conditions should state that no underage individual is permitted to participate in remote gambling activities.

Registration and verification

2.04 The registration process should include a clear message regarding play by underage individuals.

2.05 Customer registration should require the customer to provide the following minimum information: name, age, address and unique username and password details.

2.06 Age and customer verification should be conducted in accordance with a formal documented process, and should include operator and third party verification checks, where feasible and available.

2.07 Operators should work with reputable verification service providers to improve coverage and quality of verification services available.

Free play sites

2.08 Free play sites should not award cash or cash equivalents unless the customers have been successfully age verified.

2.09 If registration is required prior to potential customers being allowed to “Play for Free”, the operator’s registration process should include confirmation of age.

Dealing with identified underage individuals

2.10 Operators should have a clear documented policy which is applicable in the event that an underage individual is identified.

2.11 Operators should immediately lock the account of any underage individual or person suspected of being an underage individual found to have accessed its services.

2.12 The operator should have in place an appropriate system for refunding the value of all deposits should a person, subsequent to registration, be identified as an underage individual.

General

2.13 Best endeavours by the operators should be made to prevent advertising that is targeted towards underage individuals, and should not portray any underage individuals in any gambling adverts or promotional material.

2.14 Training should be provided to all employees involved in the operator’s age verification process, including training on the process to follow in the event that a need for additional verification is identified.

3. Combating fraudulent and criminal behaviour

Responsibility and ownership

3.01 Operators should implement an AML and CFT policy approved and supported by senior management which will provide reasonable security measures to prevent transactions which are potentially connected to money laundering and the financing of terrorism.

3.02 A designated senior management employee should be appointed by each operator to assume responsibility for the implementation and monitoring of AML and CFT systems.

3.03 AML and CFT control requirements between operators and service providers should be clearly defined.

3.04 Training and guidance should be provided to employees on the operator’s policy to ensure the prompt identification, escalation and reporting of fraud and AML and CFT suspicions.

Account funding and transfers

3.05 No physical cash or non-electronic methods of payment should be used to fund an account, except where such funds are deposited in a licensed gambling establishment, which adheres to the relevant AML laws that are applicable in the relevant jurisdiction.

3.06 Transfers of funds between accounts should be conducted through a formal documented process in compliance with the operator’s AML and CFT policy.

3.07 The operator's terms and conditions should state the controls applicable over funds transferred between customers.

Detecting and reporting of criminal and suspicious behaviour

3.08 AML and CFT policies and procedures should cater for the identification, escalation and reporting of unusual or suspicious activities, including investigating material or unusual deposits, withdrawals and accounts where little or no gambling activity takes place.

3.09 The operator's AML and CFT practices should include the provision of suspicious transaction reports to the relevant national financial intelligence unit and international institutions.

3.10 No deposits or payouts should be made to an account if there is reason to suspect money laundering or terrorist activity unless authorised by the AMLRO. Where the deposit or payout exceeds €2,000 (whether in a single transaction or a series of transactions which appear to be linked), no payment may be made until the customer has been positively identified.

3.11 A legal disclaimer should be displayed on the operator's web site stating that any criminal or suspicious activities may be reported.

3.12 All employees should be made aware of their personal obligations to detect and report criminal and suspicious behaviour. All employees must be aware of the dangers of 'tipping-off' and the procedures to be followed to ensure it does not happen.

Record retention

3.13 Records of customer financial transactions should be retained in accordance with the retention requirements of the operator's licensing jurisdiction.

3.14 All information regarding changes to customer details should be logged and the validity of requests for significant changes (e.g. changes to customers' names and banking details) should be substantiated.

3.15 The operator should remit funds to the customer only to the same payment mechanism from which the funds originated, except where changes to the payment mechanism are substantiated, and where such funds are withdrawn in a licensed gambling establishment, which adheres to the relevant AML laws that are applicable in the relevant jurisdiction.

3.16 Customer verification documents should be retained in accordance with the retention requirements of the operator's licensing jurisdiction.

4. Protection of customer privacy and safeguarding of information

Policies and procedures

4.01 The operator's privacy policy should state the minimum information that is required to be collected, the purpose for information collection, the conditions under which information may be disclosed and the controls in place to prevent the unauthorised or unnecessary disclosure of the information.

4.02 Multiple language websites should display the operator's privacy policy in the relevant languages.

4.03 Terms and conditions that require acceptance from customers during registration should clearly state the operator's privacy policy. Customer consent of the terms and conditions is required prior to successful registration.

Safeguarding of information

4.04 Customer credit card numbers stored on the system should be secured from unauthorised use.

4.05 The operator should take all reasonable steps to ensure that any information supplied by customers is kept up to date and that customers are provided access to their personal information.

4.06 Director, officer and employee contracts should contain a “confidentiality” clause prohibiting the unauthorised or unnecessary disclosure of customer information.

5. Prompt and accurate customer payments

Registration, information and payment process

5.01 The operator’s website terms and conditions should state that only customers legally permitted by their respective jurisdiction can participate in gambling activities.

5.02 Payments to and from customers should be conducted according to a formal documented process.

5.03 The detection and correction of timeout receipts should be conducted in accordance with a formal documented process.

5.04 Operators should ensure prompt and accurate processing of payments subject to appropriate and necessary checks and verifications.

5.05 All information regarding receipts and payments should be logged and retained by the applicable parties in accordance with the retention requirements of the operator’s licensing jurisdiction.

5.06 Financial reconciliations performed for payments and receipts should be reviewed and approved.

5.07 Account related queries should be promptly addressed.

Locking of accounts

5.08 The locking of accounts should be conducted through a formal documented process.

5.09 Any uncontested funds left in an account, previously de-activated by the operator, should be remitted to the account holder, upon request and subject to published terms and conditions.

Sufficiency of operator funds

5.10 The operator’s liability for customer balances, pending cash-ins and guaranteed prizes should be separately identifiable at any point in time, and operators should demonstrate sufficient cash and cash equivalents to pay these balances.

Inactive accounts

5.11 If the operator adopts a policy of clearing inactive accounts, then customers should be informed prior to clearing of the account, and this policy should be clearly stated in the operator’s terms and conditions.

6. Fair gaming

Policies and procedures

6.01 Operators should implement a product testing policy, approved and supported by its senior management, which will provide for the testing of all products for fairness and randomness.

6.02 The policy should make provision for the internal and external testing of product fairness and randomness.

Payout percentage, randomness and other fairness testing

6.03 Testing of fairness and randomness of products should be conducted prior to, and subsequent to the live implementation of the games.

6.04 All major changes should be individually tested and a system-wide regression test should be completed at least annually.

6.05 Payout percentage reviews should be conducted on a regular basis to verify the final result and actual return to the customer against the theoretical statistical return percentage.

6.06 The financial data log files should be reconciled to movements on the accounts to ensure accuracy and completeness of data used in final result output-based payout percentage and RNG testing.

6.07 The theoretical statistical return percentage for a particular game type should be no less than that of the equivalent game in free play mode.

6.08 The results of games ought to be random, unless it is clearly disclosed that different game-rules apply.

6.09 The final result output obtained through the use of the RNG in games should be proven to be:

- Statistically independent.
- Uniformly distributed over their range.

6.10 "Near-miss" game results should not be falsely displayed by substituting one losing outcome with a different losing outcome.

6.11 Where a game simulates a physical device:

- The visual representation of the device ought to correspond to the features of the physical device.
- The probability of any event occurring should be as for the actual physical device except where deviations are clearly displayed to the customers.

6.12 Where the game simulates multiple physical devices that would be expected to be independent of one another, each simulated device should be independent of the other simulated device.

6.13 Where the game simulates physical devices that have no memory of previous events, the behaviour of the simulations should be independent of the behaviour of previous simulations.

Game rules and other customer information

6.14 The design and operation of games should be strictly in accordance with the specified game rules, and should not deviate from those rules. This should be tested either internally or externally on an annual basis.

6.15 Game rules should be date stamped and made available to the customer at all times.

6.16 The game pay tables should be available to the customer during games of chance.

6.17 Changes to game rules and game pay tables should not be retrospective in their effect.

6.18 Multiple language websites should provide game rules in the relevant languages.

Anti-collusion and anti-deception measures

6.19 Preventative and detective controls or technology should be in place to ensure that the prospect of cheating through collusion (external exchange of information between different customers) is prevented.

6.20 Under their terms and conditions, poker rooms should not permit the use of robots by customers with a view to providing them with an advantage over other customers, and should have procedures in place to monitor the rooms for robots and, upon detection stopping their use.

6.21 For sports betting there should be procedures for identifying suspicious betting transactions and patterns which might identify a threat to the sport's integrity or an offence of cheating. Where a threat is identified there should be a procedure for notifying the relevant sporting body or Regulatory Authority in line with applicable data protection requirements.

Betting risk management

6.22 Effective risk control mechanisms should be in place for managing events offered, bet sizes and prices, taking into consideration available cash and cash equivalents.

7. Responsible marketing

Advertising content

7.01 Advertisements should contain factually correct information and should not be false or misleading, particularly with regard to customer winnings.

7.02 Advertisements should not entice underage individuals to gamble, and should not be displayed in media that is clearly targeted at underage individuals.

7.03 Customers should not be encouraged to chase their losses or re-invest their winnings and at no time should it be suggested that gambling is a means of solving financial difficulties.

7.04 Advertisements and promotional content should be within the spirit of responsible gambling.

7.05 Terms and conditions applicable to promotional activities should be clearly displayed, date and time stamped, and should not be unreasonably altered subsequent to the wagering activity.

7.06 Direct advertisements and promotional communication should carry an age restriction warning where practical.

Unauthorised marketing activity

7.07 Email, SMS and bonus advertisements should have an unsubscribe, or opt out, facility.

7.08 The operator should not abuse its relationship with the customer by any unauthorised activity on the customer's computer system.

Third party marketing activities

7.09 Operators should ensure that an affiliate and/or third party performing advertisements on their behalf is aware of and is willing to take appropriate steps to abide by the Control Measures.

7.10 If the operator becomes aware of an affiliate and/or third party behaving in a manner that contravenes these Control Measures, the operator should take reasonable steps to ensure that the affiliate ceases that behaviour or that the affiliate and/or third party contract is terminated.

8. Commitment to customer satisfaction and support

Operator dispute resolution

8.01 Contact information for complaints and dispute resolution should be readily accessible on the operator websites.

8.02 Customers should be able to log complaints and disputes on a 24/7 basis.

8.03 Where possible websites should aim to provide assistance and guidance to all customers on complaints and disputes in the same language as the content of the site.

8.04 The resolution and escalation of customer complaints should be conducted in accordance with a formal documented process.

8.05 Operators should keep records of all customer correspondence relating to a complaint and dispute for an appropriate period of time.

Third party dispute resolution

8.06 An independent third party should be available for mediation or resolution of disputes.

8.07 The third party should be required to keep records of all customer correspondence relating to a dispute for an appropriate period of time.

9. Secure, safe and reliable operating environment

Responsibility and ownership

9.01 Operators should appoint appropriate compliance personnel, who will assume responsibility for compliance with the controls specified within the Control Measures.

9.02 The appointed compliance personnel should:

- Ensure that training and awareness programmes, specified within the Control Measures, are conducted on an annual basis or more frequently if required within the operator organisation.

- Ensure that processes, policies and procedures required for compliance are established, implemented and maintained.
- Have the responsibility and authority to report on compliance with the Control Measures to senior management.

Contractual, legal and regulatory requirements

9.03 Operators should keep financial transaction records in accordance with the retention requirements of their licensing jurisdiction.

9.04 Operator websites should display the name of the operator and the address of its registered office.

9.05 Operator websites should prominently display date stamped contractual terms and conditions applicable to gambling activities, which should be available to print or download at any time.

Accounting and record keeping

9.06 Operators should keep records in a manner that will allow the timely preparation and audit of financial statements and accounting records.

9.07 Operators should commit to an annual audit of financial statements and accounting records performed by a reputable external audit firm.

Information and security environment

9.08 Security policies and procedures should be documented and communicated to relevant employees, and reviewed at least annually or in the event of material changes.

9.09 Security policies and procedures should be implemented and monitored. Risk-based internal and external security reviews should be conducted at least annually or in the event of material changes.

9.10 Physical security perimeters should be in place to restrict access to authorised personnel to areas that contain information and information processing facilities and to reduce the risk of environmental threats and hazards to equipment.

9.11 Relevant third party and business partner contractual terms and conditions should cover all appropriate security requirements.

9.12 Virus scanners and/or detection programs should be installed on all pertinent information systems. These programs should be updated regularly to scan for new strains of viruses.

9.13 Controls should be in place to manage changes to information processing facilities and systems in order to reduce the risk of security or system failures.

9.14 All customers should be verified with an account identifier/password pair, or by any other means that provide equal or greater security (e.g. digital certificates), prior to being permitted to participate in gambling activities.

9.15 All system users should have their identity verified with an account identifier/password pair, or by any other means that provide equal or greater security, prior to being permitted to access the system. All system user actions should be logged.

9.16 All customer deposit, withdrawal or adjustment transactions should be subject to strict security control and should be recorded in a system audit log.

9.17 Information involved in online transactions should be protected to prevent incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

9.18 A policy on the use of cryptographic controls for protection of information should be developed and implemented.

Business continuity and disaster recovery

9.19 Backup and recovery procedures should be in place to ensure appropriate data and information (e.g. logs and financial information) are backed up on a regular basis and can be restored in the event of a disaster.

9.20 Backup and disaster recovery responsibilities between software providers and operators should be clearly defined.

9.21 All information required for completing an incomplete game should be recoverable by the system.

9.22 All transactions involving customer funds should be recoverable by the system in the event of a failure or malfunction.

9.23 If an operator has reason to believe or to suspect that an interruption has been caused, or a transaction affected by illegal activity, the operator may withhold payment to the relevant accounts pending further investigation.

Software development and maintenance

9.24 A development methodology for software and applications should be defined, documented and implemented.

9.25 All documentation relating to software and application development should be available and retained for the duration of its lifecycle.

9.26 Change control procedures should be implemented in line with the change management policy and should cater for the following:

- Approval procedures for changes to software.
- A policy addressing emergency change procedures.
- Procedures for testing and migration of changes.
- Segregation of duties between the developers, quality assurance team, the migration team and users.
- Procedures to ensure that technical and user documentation is updated as a result of a change.
- Procedures to ensure that security control requirements are specified for new information systems, or enhancements to existing information systems.

9.27 The development and test environments ought to be isolated physically and logically from the live operational systems.

4 Annex A (Informative) – Non-Exhaustive List of Existing Responsible Gambling Regulations, Measures and Codes

- United Kingdom Gambling Commission Codes of Practice (see link)
- Isle of Man Online Gambling Regulations (see link)
- Malta Lotteries and Gaming Authority Remote Gaming Regulations (see link)
- Maltese Standard MSA1600:2008 “Remote Gaming – Operators Management System – Requirements”.
- Gibraltar Code of Practice for the Gambling Industry (see link)
- Swedish Presidency Progress Report ´Legal framework for gambling and betting in the Member States of the European Union´, doc 16571/09 (see link)
- EGBA Standards (see link)
- RGA Social Responsibility Code (see link)
- eCOGRA’s Generally Accepted Practices (eGAP) (see link)
- European Lotteries
    - Responsible Gaming Standards (see link)
    - Code of Conduct on Sports betting (see link)
- IAGR eGambling Guidelines (see link)
- Interactive Gaming Council
    - Code of Conduct (see link)
    - Responsible Gambling Guidelines (see link)
    - Advertising Code of Practice (see link)
- Ehrenkodex VEWU
- ESSA Code of Conduct (see link)
- Global Gambling Guidance Group (G4), e-Gambling Code of Practice (see link)