2008-01-15 03:28:00

G005_ADMINISTRATIVE_SYSTEMS

Administrative systems, policies, and procedures

Guidelines

1. Preliminary

1.1 Authority

This document is issued by the Financial Services regulatory Commission (the Commission) pursuant to r 105(e) of the Antigua & Barbuda Interactive Gaming and Interactive Wagering Regulations (the Regulations).

1.2 Confidentiality

This document, all related documents, and methodologies embodied in this document and related documents ("*the documents*") are the property of the Financial Services Regulatory Commission. Unauthorised copying and distribution of *the documents*, by any means, on any media is prohibited.

This document, its themes, and ideas are strictly confidential and may not be used in any manner other than its expressed purpose, without the written permission of the author. The documents are authorised for use by licence holders.

The documents are copyright.

1.3 Disclaimer

The guidelines provided in this document are current at the time of writing. The Commission may in its absolute discretion amend these guidelines, or any definitions or interpretations pursuant to this or related documents at anytime.

Each licence holder should ensure it has the current version of each document.

1.4 Queries

All queries relating to this document should be made, in writing, to:

Director of Gaming
Financial Services Regulatory Commission
First Caribbean Financial Centre
Old Parham Road
St John's
Antigua and Barbuda

e-mail : director@antiguagaming.gov.ag

1.5 References

G	**001**	***Accounting systems, chart of accounts***
G	**002**	***Accounts held at financial institutions***
G	**003**	***Financial reconciliation & financial adequacy***
G	**004**	***Organisational chart***
G	**005**	***Administrative systems, policies & procedures***
G	**006**	***Information systems***
G	**007**	***Change and configuration management***
G	**008**	***Business continuity & disaster recovery***
G	**009**	***Operational systems, terms and conditions, and rules of games***
G	**010**	***Physical & environmental security***
G	**011**	***Systems***
G	**012**	***Responsible gaming & wagering***
G	**013**	***Restriction of underage gaming & wagering***
G	**014**	***Anti-money laundering***
G	**015**	***URLs & domains***
G	**016**	***Risk management - overview***
G	**017**	***Risk management - compliance (preliminary)***
G	**018**	***Gaming equipment***
G	**019**	***Continuous improvement - compliance programme***
G	**020**	***Advertising***
G	**021**	***Approved certifying organisation***
RP	**001**	***Monitoring***

CS	***Certification Standards***
RP	***Rules and procedures***
S	***Specifications***
SG	***Submission Guidelines***
G	***Guidelines***

G 005

1.6 Table of contents

2. Guidelines

These guidelines do not override other lawful requirements.

2.1 Policies

2.1.1 Scope of policies

REGULATORY OBJECTIVE

Licence holders shall provide management direction and support for business, security, and compliance in accordance with business, regulatory, and legal requirements.

2.1.1.1 Policy documents

1. All policies shall be documented. The documents shall be suitable, adequate, and effective.
2. There shall be policy documents relating to information security and compliance.
3. The policy documents shall be approved by management.
4. The policy documents shall be published.
5. The policy documents shall be communicated to all employees and relevant external parties.

2.1.1.2 Review of policy documents

1. The policy documents shall be reviewed at planned intervals.
2. The policy documents shall be reviewed if significant changes occur.

2.2 Procedures

The licence holder shall have formal, documented procedures comprising an internal control system (ICS). The ICS should provide details of the following:

a. each class of account required to operate the IGS in a production environment (e.g. System Administrator, Operator, Hotline, Network support);

b. the configured access control list. (e.g. for each job function such as Customer Service Representative, Casino Manager, Finance Manager, etc.);

c. the physical location of each component of the central IGS, including the location of staff;

d. recurrent IT procedures, including:

- shift change procedures;
- end-of-day procedures;
- weekly procedures;
- monthly procedures

There should be a philosophy throughout the ICS that one single person undertaking impugned activities cannot cause a security breach or non-compliance which will not be detected. In so doing all of the routine procedures will require substantial monitoring and review of staff activity and financial and gaming reconciliations.

2.3 Organisation of information security & compliance

2.3.1 Licence holder's organisation

REGULATORY OBJECTIVE

Licence holders shall ensure information security and compliance is managed within the organisation.

2.3.1.1 Management commitment to information security

1. Management shall actively support security and compliance within the organisation through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security and compliance responsibilities.

2.3.1.2 Information security coordination

1. Information security and compliance activities shall be coordinated by representatives from different parts of the organisation with relevant roles and job functions.

2.3.1.3 Allocation of information security responsibilities

1. All information security and compliance responsibilities shall be clearly defined.

2.3.1.4 Authorisation process for information processing facilities

1. A management authorisation process for new information processing facilities shall be defined and implemented.

2.3.1.5 Confidentiality agreements

1. Requirements for confidentiality or non-disclosure agreements reflecting the licence holder's needs for the protection of information shall be identified and regularly reviewed.

2.3.1.6 Contact with authorities

1. Appropriate contacts with relevant authorities shall be maintained.
2. Relevant authorities shall include as a minimum: Financial Services Regulatory Commission (FSRC), Office of National Drug & Money Laundering Control Policy (ONDCP), the Royal Police Force, Power and Water Authority (PAWA), and relevant Internet service provider(s).

2.3.1.7 Contact with special interest groups

1. Appropriate contacts with special interest groups or other specialist security fora and professional associations should be maintained.

2.3.1.8 Independent review of information security

1. The licence holder's approach to managing information security and compliance and their implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur.

NOTE: Licence Holders should not rely on r 189 alone to implement this control.

2. The reviewing entity should be truly independent of the licence holder.

2.3.2 External parties

REGULATORY OBJECTIVE

Each licence holder shall maintain the security and compliance of the licence holder's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

2.3.2.1 Identification of risks related to external parties

1. The risks to the licence holder's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.
2. Risk identification and management should be documented and formally approved by appropriate management.

2.3.2.2 Addressing security when dealing with customers

1. All identified security requirements shall be addressed before giving customers access to the licence holder's information or assets.

NOTE: Access to information means "all information" and includes but is not limited to communication with help desks, e-mail and telephone, etc.

2.3.2.3 Addressing security in third party agreements

1. Agreements with third parties involving accessing, processing, communicating or managing the licence holder's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.

NOTE: Payment processors and other financial institutions are third parties which the FSRC consider captured by this guideline. Aggregators and affiliates may be third parties which are captured by this guideline – depending on the nature of the information accessible by those third parties.

2.4 Asset management

2.4.1 Responsibility for assets

REGULATORY OBJECTIVE

Licence holders shall achieve and maintain appropriate protection of organisational assets.

2.4.1.1 Inventory of assets

1. All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.

NOTE: For the purpose of this guideline assets include policies, procedures, software components, hardware components, human resources, etc – all assets to the licence holder achieving its business and regulatory objectives.

2.4.1.2 Ownership of assets

1. All information and assets associated with information processing facilities shall be "owned" by a designated part of the licence holder's organisation.

NOTE: Where components of the business of interactive gaming and interactive wagering, including but not limited to gaming management, payment processing and/or management, are outsourced or provided by a third party. The licence holder shall continue to assign an "internal owner" responsible for the integrity, confidentiality, availability, and accountability of all such information and information processing.

2.4.1.3 Acceptable use of assets

1. Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.

2.4.2 Information classification

REGULATORY OBJECTIVE

Licence holders shall ensure that information receives an appropriate level of protection.

2.4.2.1 Classification guidelines

1. Information shall be classified in terms of its value, legal requirements, sensitivity, and criticality to the licence holder and its compliance requirements.

2.4.2.2 Information labelling and handling

1. An appropriate set of procedures for information labelling and handling should be developed and implemented in accordance with the classification scheme adopted by the organisation.

2.5 Human resource security

2.5.1 Prior to employment

REGULATORY OBJECTIVE

Licence holders shall ensure that employees, contractors, and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

2.5.1.1 Roles and responsibilities

1. Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the licence holder's policies (including but not limited to information security and compliance).
2. All licence holder information is and remains into perpetuity licence holder property. Where possible all information processing machines relating to licence holder business should be and remain licence holder property.

NOTE: Employees and persons with management control (or equivalent) should utilise licence holder machines for licence holder and related business. Those machines should be used for licence holder business only. those machines and all data on those machines shall belong to the licence holder and be subject to full disclosure.

3. All communications and logs of communications in anyway related to licence holder business are and shall remain the property of the licence holder.

NOTE: Licence holder should have corporate e-mails and maintain a complete log of all e-mails. The use of peer-to-peer communications between remote users (i.e. Yahoo Messenger, MSN Messenger, Skype, etc) should be managed and logs maintained.

2.5.1.2 Screening

1. Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.
2. All persons identified as having material control, influence or benefit over or from the licence holders operations should complete a "key person" application and be included in the asset of associates.

2.5.1.3 Terms and conditions of employment

1. As part of their contractual obligation, employees, contractors, and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their, the licence holder's responsibilities for information security and compliance.

2.5.2 During employment

REGULATORY OBJECTIVE

Licence holders shall ensure that all employees, contractors and third party users are aware of information security and compliance threats and concerns, their responsibilities and liabilities, and are equipped to support organisational security policy in the course of their normal work, and to reduce the risk of human error.

2.5.2.1 Management responsibilities

1. Management shall require employees, contractors, and third party users to apply security in accordance with established policies and procedures of the organisation.

2.5.2.2 Information security awareness, education, and training

1. All employees of the licence holder and where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function.

2.5.2.3 Disciplinary process

1. There shall be a formal disciplinary process for employees who have committed a security breach.

2.5.3 Termination or change of employment

REGULATORY OBJECTIVE

Licence holders shall ensure that employees, contractors, and third party users exit the organisation or change employment in an orderly and controlled manner.

2.5.3.1 Termination responsibilities

1. Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.

2.5.3.2 Return of assets

1. All employees, contractors, and third party users shall return all of the licence holder's assets in their possession upon termination of their employment, contract, or agreement.

2.5.3.3 Removal of access rights

1. The access rights of all employees, contractors, and third party users to information and information processing facilities shall be removed upon termination of their employment, contract, or agreement, or adjusted upon change.

2.6 Registers

The licence holder shall establish and maintain registers.

- contracts & agreements
- financial accounts
- URLs associated with licence holder business
- payment gateway providers
- associates
- gaming equipment
- games
- events
- excluded customers

- customers
- customer bet limits
- assets

Registers shall be bought up-to-date at the end of each calendar month.

NOTE: Where an entity establishes a relationship worthy of inclusion into a register and the relationship is ceased at the end of month update time, then that entity shall be recorded in the register, with a commencement and cessation date and reason for brevity.

2.7 Compliance

2.7.1 Compliance with legal requirements

REGULATORY OBJECTIVE

Licence holders shall avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

2.7.1.1 Identification of applicable legislation, regulations, and directions

1. All relevant statutory, regulatory, and contractual requirements and the licence holder's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system.

2.7.1.2 Intellectual property rights

1. Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products – within the laws of Antigua and Barbuda.

2.7.1.3 Protection of organisational records

1. Important records shall be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

2.7.1.4 Data protection and privacy of personal information

1. Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

2.7.1.5 Prevention of misuse of information processing controls

1. Users shall be deterred from using information processing facilities for unauthorised purposes.

2.7.1.6 Regulation of cryptographic controls

1. Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.

2. Where any records required under the Regulations are encrypted then the encryption/decryption keys and pass codes shall be stored in Escrow with an organisation approved by the Commission.

3. Where corporate communications, or a users communications via corporate systems (i.e. e-mail) is encrypted then the information owner shall have access to the encryption and decryption keys and pass phrases to enable management to monitor and control information transfers.

2.7.2 Compliance with policies, standards, and technical compliance

REGULATORY OBJECTIVE

Licence holders shall ensure compliance of systems with organisational and regulatory policies and standards.

2.7.2.1 Compliance with policies and standards

1. Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

2.7.2.2 Technical compliance checking

1. Information systems shall be regularly checked for compliance with security implementation standards.

2.7.3 Information systems auditing considerations

REGULATORY OBJECTIVE

Licence holders shall maximise the effectiveness of and minimise interference to and from the information systems audit processes.

2.7.3.1 Information systems audit controls

1. Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimise the risk of disruptions to business processes.

2.7.3.2 Protection of information systems audit tools

1. Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.

2. All functions relating to the provision of information to the Commission, including but not limited to the Commission's approved monitoring programme, shall be strictly controlled to ensure the integrityt of that information.

End of document