Financial Services Regulatory Commission
Directorate of Offshore Gaming

2008-01-18 12:37:00

G006_INFORMATION_SYSTEMS

Information systems including logical access control

Guidelines

G 006

1. Preliminary

1.1 Authority

This document is issued by the Financial Services Regulatory Commission (the Commission) pursuant to r 105(f) 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

A.1 References & related documents

The Financial Services Regulatory Commission utilised many documents and international standards when compiling the suite of guidelines.

The current list of related guidelines is available from the Commission's website at http://www.antiguagaming.gov.ag.

Licence holders and other interested parties should acquaint themselves with the contemporary documents before relying on them.

1.5 Table of contents

2. Guidelines

These guidelines do not override other lawful requirements.

2.1 Access control

2.1.1 Business requirements for access control

REGULATORY OBJECTIVE

Licence holders shall control access to information and information processing functionality and facilities.

2.1.1.1 Access control policy

1. An access control policy shall be established, documented, and reviewed based on business, security, and compliance requirements for access.

2.1.2 User access management

REGULATORY OBJECTIVE

Licence holders shall ensure authorised user access and prevent unauthorised access to information systems.

2.1.2.1 User registration

1. There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.
2. Registered user accounts shall be reviewed for applicability at specified periods.

2.1.2.2 Privilege management

1. Privileges shall be defined for specific business purposes.
2. The allocation and use of privileges shall be restricted and controlled.
3. Privileges and privilege allocation shall be reviewed for applicability at specified periods.

2.1.2.3 User password management

1. The allocation and establishment of passwords shall be controlled through a formal management process.

2.1.2.4 Review of user access rights

1. Management shall review users' rights at regular intervals using a formal process.

2.1.3 User responsibility

REGULATORY OBJECTIVE

Licence holders shall prevent:

- **unauthorised users access to, and**
- **compromise or theft of**

information and information processing facilities.

2.1.3.1 Password use

1. Users shall be required to follow good security practices in the selection and use of passwords.

NOTE: The Commission anticipates this guideline will be enforced by information processing facilities.

2.1.3.2 Unattended user equipment

1. Users shall ensure that unattended equipment has appropriate protection.

2.1.3.3 Clear desk and clear screen policy

1. A clear desk policy for papers and removable storage media shall be adopted for appropriate office and work areas.
2. A clear screen policy shall be adopted for appropriate office and work areas

2.1.4 Network access control

REGULATORY OBJECTIVE

Licence holders shall prevent unauthorised access to networked services.

2.1.4.1 Policy on use of network services

1. Users shall only be provided with access to the services that they have been specifically authorised to use.

2.1.4.2 User authentication for external connections

1. Appropriate authentication methods shall be used to control access by remote users.

2.1.4.3 Equipment identification in networks

1. Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.

2.1.4.4 Remote diagnostic and configuration port protection

1. Physical and logical access to diagnostic and configuration ports shall be controlled.

2.1.4.5 Segregation in networks

1. Groups of information services, users, and information systems shall be segregated on networks.

2.1.4.6 Network connection control

1. For shared networks, especially those extending beyond the licence holder's boundaries, the capability of users to connect to the network shall be restricted in line with the access control policy and requirements of the business applications (see *2.1 Access control*).

2.1.4.7 Network routing control

1. Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

2.1.5 Operating system access control

REGULATORY OBJECTIVE

Licence holders shall prevent unauthorised access to operating systems.

2.1.5.1 Secure log-on procedures

1. Access to operating systems shall be controlled by a secure log-on procedure.
2. Access to operating systems shall be restricted in accordance with the formally identified need to access (see *2.1 Access control*).

2.1.5.2 User identification and authentication

1. All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.

2.1.5.3 Password management system

1. Systems for managing passwords shall be interactive (shall not require a human intermediary) and shall ensure quality passwords.

2.1.5.4 Use of system utilities

1. The use of utility programs that might be capable of overriding system and application controls or amending data shall be restricted and tightly controlled.

NOTE: The Commission anticipates operating system minimisation techniques shall be utilised throughout the licence holder's business.

2.1.5.5 Session time-out

1. Inactive sessions should shut down after a defined period of inactivity.

2.1.5.6 Limitation of connection time

1. Restrictions on connection times should be used to provide additional security for applications, which would represent a high-risk if used in an unauthorised manner.

2.1.6 Application and information access control

REGULATORY OBJECTIVE

Licence holders shall prevent unauthorised access to information held in application systems.

2.1.6.1 Information access restrictions

1. Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.

2.1.6.2 Sensitive system isolation

1. Sensitive systems shall have a dedicated (isolated) computing environment.

NOTE: The Commission anticipates isolation shall be achieved by physical and logical means.

2.1.7 Mobile computing and tele-working

REGULATORY OBJECTIVE

Licence holders shall ensure information security and compliance when using mobile computing and teleworking facilities.

2.1.7.1 Mobile computing and communications

1. A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.

2.1.7.2 Teleworking

1. A policy, operational plans, and procedures shall be developed and implemented for teleworking activities.

NOTE: Where teleworkers connect to licence holder systems then a risk assessment considering the extension of the secure perimeter must be undertaken and appropriate controls identified and implemented.

End of document