2008-01-18 12:49:00

G010_PHYSICAL_ENVIRONMENTAL_SECURITY

Physical & environmental security

Guidelines

G 010

1 Administration

1.1 Authority

This document is issued by the Financial Services Regulatory Commission (the Commission). The document provides guidance as to controls which might be incorporated into control systems required by Regulation 105 of the Antigua & Barbuda Interactive Gaming and Interactive Wagering 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 these 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 & 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.

1.6 Table of contents

1.7 Definitions

Term	Meaning
NLZ	No-Lone-Zone is an area in which people are not permitted to be left alone.
server	A server is a computer used to run programs that provide services to multiple users connected to it via a network.
server room	A space containing servers and any associated communications equipment.

G 010

2 Preliminary

2.1 Purpose

The purpose of this document is to provide guidance as to control systems which might be applied to meet the requirements of r 105(j):

> **105.** A control system submission must be in a form approved by the Commission and describe and explain the licence holder's proposed control system and in particular must include: …
>
> (j) physical and environmental security and physical access control; …

2.2 Introduction

The guidance provided here suggests controls, which a licence holder might include in its physical and environmental security, and physical access control policies, procedures, and practices. The Commission consider these controls are appropriate for the purpose of managing compliance and risk associated with physical and environmental security.

These guidelines do not circumvent any legislation, regulation, or statutory direction with which the licence holder is bound to comply.

3 Control guidance

3.1 Fundamentals

Policy objective

Control systems should be derived through formal, structured processes.

3.1.1 Risk management

1. The licence holder shall ensure that a site specific physical security threats and vulnerabilities are included in its risk management process.

NOTE: "Theft" by otherwise authorised persons should be considered as a threat in the risk management process.

Information assets to be included in the risk management process include (but are not limited to) all assets, which enable the licence holder's information and information processing facilities, such as: uninterruptible power supplies, generators, Internet access, air conditioning units, etc

2. The sensitivity of licence holder information and information processing facilities should be identified.

NOTE: Some publicly available information may not be confidential. Yet the integrity and/or availability of that information might be essential. Therefore, the sensitivity with regard to confidentiality, integrity, and availability should be considered.

3.2 Secure areas

Policy objective

To prevent unauthorised physical access, damage, and interference to the licence holder's premises and information.

3.2.1 Physical security perimeters

1. Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.

2. The security perimeters should be consistent with a defence-in-depth design (i.e. a more restrictive area separated containing more sensitive information and information processing facilities should be separated from general users).

3. All licence holder information and information processing facilities should be encompassed by a security perimeter.

3.2.2 Physical entry controls

1. Secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.

2. All access should be recorded in a secure log.

3. The access log cited in guideline 3.2.2 - 2 shall be capable of facilitating evacuation and to support investigations – containing records of persons currently and previously in the licence holder premises. An appropriate key person (as defined by the Interactive Gaming and Interactive Wagering Regulations) shall be responsible for maintaining the log, which should be kept for twelve (12) months.

4. Secure areas should detect attempts at unauthorised access.

5. Attempts at unauthorised access should be logged and a remedial plan, which identifies person(s) attempting unauthorised access and reduces attempts at unauthorised access, implemented.

6. Authorised persons must not permit unknown or unauthorised persons to pass through doors, gates, and other entrances to restricted areas at the same time when authorised persons go through these entrances.

7. Workers must not attempt to enter restricted areas in the licence holder's buildings for which they have not received access authorisation.

8. In the event that a person with authorised access privileges is terminating his or her relationship with the licence holder, all physical security access codes known by the person must be deactivated or changed.

9. A list of managers who are authorised to grant access to the licence holder's premises must be kept up-to-date. This list must also be periodically reviewed by the higher-level managers who delegated authority to these managers. All such managers shall be key persons as defined by the Interactive Gaming and Interactive Wagering Regulations.

10. Every department head should receive, on a monthly basis, a listing of all persons in their area who currently have valid identification badges. Department heads must authorise the list of approved access or amend it accordingly.

11. All visitors should show picture identification and sign-in prior to gaining access to restricted areas controlled by the licence holder.

3.2.3 Intrusion detection systems

1. All licence holder premises shall include a system for intrusion detection & alarm.

2. Any alarm pursuant to guideline 3.2.3 - 1 should have a formal response plan.

3.2.4 Securing offices, rooms, and facilities

1. Physical security for offices, rooms, and facilities shall be designed and applied.

2. Areas segregated by perimeters should have dry floor to ceiling walls, such that person(s) may not breach access controls via a sub-floor or ceiling compartment.

3. Each server room should have standard operating procedures (SOPs). The following topics may be included in the SOPs:

a. a summary of the relevant risk assessment;

b. roles and responsibilities of individual staff with access to the server room;

c. the administration, operation, and maintenance of the Electronic Access Control System (EACS) and/or Security Alarm System (SAS);

d. key management, the enrolment and culling of users and issuing of pin codes;

e. staff clearances, security awareness training, and regular briefings;

f. inspection of the generated audit trails, logs, and surveillance tapes;

g. end of day checks and lockup; and

h. reporting of security incidents and breaches.

3.2.5 Protecting against external and environmental threats

1. Physical protection against damage from hurricane, fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.

2. Multi-user computers and communications facilities (including server rooms) should be located above the ground floor in buildings.

3. Kitchen facilities should be located away from (including not directly above or below) multi-user systems or server rooms.

4. Rest room facilities should not be located directly above these systems.

5. Multi-user computer systems (including server rooms) should not be located adjacent to a building's exterior wall.

6. There should be no signs indicating the location of computer or communications centres.

3.2.6 Working in secure areas

1. Physical protection and guidelines for working in secure areas shall be designed and applied.

2. Where access to information or information processing facilities is controlled by physical segregation, then consideration should be given to whether some physically segregated areas should be in a No-Lone-Zone (NLZ) – this would be areas where it is considered that "two person integrity" is a suitable control to protect the information or information processing facilities within that zone.

3. Areas designated as NLZs shall be appropriately signed, and access should be secured, monitored, and logged.

4. Workstations with access to sensitive information or information processing functionality should be placed in a manner that screens and keyboards may not be viewed by unauthorised persons.

5. Whenever in licence holder buildings or facilities, all persons should wear an identification badge on their outer garments so that the information on the badge is clearly visible.

6. Licence holder' staff who have forgotten their identification badge should obtain a temporary badge.

7. All authorised persons should challenge persons not wearing an identification badge in accordance with guideline 3.2.6 - 5.

3.2.7 Public access, delivery, and reception areas

1. Access points such as delivery and loading areas and other points where unauthorised persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.

2. Visitor or other third party access to the licence holder's premises, computer facilities, and other work areas containing sensitive information should be controlled by guards, receptionists, or other staff.

3. Visitors to the licence holder's offices must be escorted at all times by an authorised employee, consultant, or contractor. This means that an escort is required as soon as a visitor enters a controlled area, and until this same visitor goes outside the controlled area. Visitors requiring an escort include but are not limited to business partners, former employees, worker family members, equipment repair contractors, and package delivery company staff.

4. A secured intermediate holding area must be used for computer supplies, equipment, and other deliveries. Delivery personnel must not be able to directly access rooms containing multi-user computer facilities (including server rooms).

3.3 Equipment security

Policy objective

To prevent loss, damage, theft or compromise of assets and interruption to the licence holder's activities.

3.3.1 Equipment citing & protection

1. Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.

2. Removable media (e.g. back-up tapes, hard rives, memory sticks, floppy disks, CDs, DVDs, etc) should be stored in accordance with the sensitivity of the information contained therein (including after hours storage).

NOTE: Encryption provides logical security. Thus where information is appropriately encrypted it may be less sensitive with regard to the need for physical security.

3. Physical access to servers must be restricted to authorised persons.

4. Servers shall be separate from other user equipment i.e. in a purpose built server room and/or appropriate cabinets or racks.

5. Where the equipment perimeter is achieved by a cabinet or rack the equipment must be secured by a commercially secure cabinet. Cabinets and racks used in this way must be within an authorised access only perimeter.

6. Where equipment of different sensitivity and value to the licence holder is co-mingled in a server room, then the equipment should be compartmentalised within the server room in different racks. Racks shall be secured according to the most sensitive of equipment contained within the rack, and access to the rack shall be afforded to persons(s) authorised to access the most sensitive of equipment within the rack.

7. Information stored on media that is not permanently fastened within equipment (e.g. CD and DVD towers, backup tapes, RAID arrays, etc) be contained in a rack, container, or cabinet in accordance with the requirements for the storage for hardcopy material of equal sensitivity. Where the sensitivity of information contained on such media is not known then it should be taken to be at the most sensitive classification within the licence holder's organisation.

8. When media (per guideline 3.3.1 - 7) is installed for operation in a server room then it should be secured in equipment, which is further secured in a locked commercial grade rack or cabinet.

9. Workstations and network infrastructure should be wholly contained within an area of the appropriate security for the information or information processing functionality accessible from the workstation or network infrastructure.

10. Equipment and racks containing sensitive information or sensitive information processing functionality may be secured with tamper evident seals.

11. The use of tamper evident seals pursuant to guideline 3.3.1 - 10 should be recorded in a register, including:

a. issue and usage details of the seals and associated tools;

b. serial number of seals used;

c. the location or system each seal is used on;

d. details of authorised breaking of the seal.

12. The licence holder should have a contractual arrangement with the provider to ensure that seals described in guidelines 3.3.1 - 10 & 11 are identifiable and unique to the licence holder.

3.3.2 Supporting utilities

1. Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

3.3.3 Cabling security

1. Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

3.3.4 Equipment maintenance

1. Equipment shall be correctly maintained to ensure its continued availability and integrity.

2. All licence holder computer and communications equipment should have a unique computer-readable identifier attached to it such that physical inventories can be efficiently and regularly conducted.

3. All licence holder computer and communications equipment should have an identification number permanently etched onto the equipment.

4. Microcomputer equipment (PCs, LAN servers, etc.) should not be moved or relocated without the prior approval of the involved department manager. The department manager shall be a key person as defined by the Interactive Gaming and Interactive Wagering Regulations.

3.3.5 Security of equipment off-premises

1. Security shall be applied to off-site equipment taking into account the different risks of working outside the licence holder's premises.

2. Laptop computers should be secured with a commercial grade locking device to an immovable object, whether on-site or off-site.

3. Laptop computers shall not be left unattended in motor vehicles.

4. All management or employees who must keep sensitive licence holder information at their homes in order to do their work should receive lockable furniture for the proper storage of this information. At the time of separation from the licence holder, both the furniture and sensitive information stored therein must be immediately returned to the licence holder.

3.3.6 Secure disposal or re-use of equipment

1. All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use in a separate area of the licence holder's business.

3.3.7 Removal of property

1. Equipment, information, or software should not be taken off-site without prior authorisation. Such authorisation should be in writing by the appropriately qualified person, who is a Key Person as defined by the Interactive Gaming and Interactive Wagering Regulations.

2. All briefcases, suitcases, handbags, and other luggage may be opened for inspection by licence holder management or building guards to check when people leave licence holder premises.

3.4 Physical security incidents

3.4.1 Incident management

1. Licence holders should have: policies, plans, and procedures that address the management of physical security incidents.

2. Licence holders should ensure all staff report all physical security incidents – actual or suspected – to the appropriate manager. The appropriate manager shall be a key person pursuant to the Interactive Gaming and Interactive Wagering Regulations. Incidents include, but are not limited to:

a. unauthorised access to areas within a permitter;

b. unauthorised access to equipment and cabling;

c. detection of any unauthorised equipment; and

d. failures in security mechanisms, which may have allowed unauthorised access.

3.4.2 Emergency situations

1. Emergency policies, plans, and procedures should include the securing of sensitive information and sensitive information processing facilities.

NOTE: Health and safety considerations must be the first priority at all times.

3.5 Buildings

3.5.1 Construction standard

1. Buildings shall be built to a standard which is expected to withstand Category 5 Hurricanes – as certified by a suitable qualified and independent person.

2. Buildings should be fire resistant.

3. Buildings and secure areas should have minimal points of entry.

4. Fire exits should have one-way crash bars, and trip an appropriately loud audible alarm when opened.

5. Buildings should have appropriate lightning protection, which is tested on a periodic basis.

6. Buildings shall be certified by an appropriate engineer to cope with the proposed floor loading of all equipment, cabinets, and personnel.

NOTE: Uninterruptible power supplies (UPSs), densely populated server rooms, and fire resistant safes and cabinets can cause high floor loadings.

7. Buildings shall be designed to enable the efficient delivery of large assets (e.g. UPSs, safes, fire resistant cabinets).

3.6 Server rooms

1. Server rooms should not:

a. have a window on the external of the building;

b. have glass access or security walls; and

c. be susceptible to water intrusion in the event of roof loss during a hurricane;

2. Server rooms should have:

a. real floor to real ceiling secure perimeters, which would provide evidence of unauthorised access;

b. secure entry;

c. access logging and surveillance;

d. intrusion detection and alarms;

e. appropriate fire prevention, detection, and suppression controls;

f. redundant services (electricity and air conditioning); and

g. electro-static discharge safeguards.

3. Firewalls surrounding server rooms should be non-combustible and resistant to fire for at least one hour. All openings to these walls (doors, ventilation ducts, etc.) should be self-closing and likewise rated to at least one hour.

4. Server rooms should be equipped with hurricane resistant, riot doors, fire doors, and other doors resistant to forcible entry.

5. Secure areas should be equipped with doors that automatically close immediately after they have been opened, and which set off an audible alarm when they have been kept open beyond a certain period of time.

End of document