

THE PRELIMINARY TEXT OF THE PROPOSED RULE DEVELOPMENT IS:

61D-14.074 Security Requirements, Data Transfer, System Access, and Audit controls ~~Firewalls~~.

(1) Except as provided in this section, all computer application program communication for the facility based monitoring system (FBMS) is to be restricted to the slot machine licensee's facility. The slot machine licensee shall only provide the minimum necessary connectivity for the functioning of computer applications programs permitted under Chapter 551, Florida Statutes and Chapter 61D-14, Florida Administrative Code.

(2) For purposes of this rule the term data transfer shall mean the process permitted under the rules to transfer computer data from and to one or more sites external to the slot machine licensee's facility through communication networks authorized under this rule. Data transfer shall:

(a) Not be authorized that in any way to write to or alter any records of the FBMS, accounting or revenue records

(b) Be authorized to update computer data, under the control of programs tested and certified by a licensed independent laboratory, maintained in the facility player tracking system for non-revenue purposes only at the slot machine licensed facility.

(3) Data transfer authorized under this rule is limited to the operation of a player tracking system, an Electronic Funds Transfer system, a patron slot machine gaming account system as defined in Rules 61D-14.076, 61D-14.077, and 61D-14.078, and accounting and FBMS reporting programs that execute and deliver the reports produced from the FBMS.

(4) Each licensee's FBMS shall be physically isolated from all other shared communication medium.

(a) Computer applications, programs and any applicable updates or modifications to those programs permitted by rule that must provide data transfers to external resources in order to function, shall be certified by an independent testing laboratory licensed by the state and approved by the division in writing prior to implementation.

1. The slot machine licensees shall provide all software, system and subsystem specifications, and complete specifications of each type of transaction intended to pass outside of the slot machine licensee's facility for laboratory certification and validation.

2. An independent testing laboratory licensed by the state must provide certification of review of all records provided and certify to the division in writing that the data being transferred by the program outside the slot machine licensee's facility is permitted and consistent with all applicable statutory requirements and rules. The laboratory shall provide its written certification to the division no less than ten work days prior to the proposed date of live system execution of that software capability.

3. The slot machine licensee may implement the certified software capability upon receipt of certification from the independent testing laboratory licensed by the state.

4. The slot machine licensee shall conduct random evaluations of at least 10% of all transactions for all records and logs regarding material transactions provided as a result of the data transfers.

a. Slot machine licensees shall provide the division a data record [i.e., data "dump"] of all transaction history/logs for up to 365 days prior to a designated evaluation date upon request. The data record shall be provided in electronic file format that clearly reflects the date of each record and is completely searchable on all data elements.

b. The slot machine licensee shall randomly compare the information retained in the data record of all transaction history/logs for content and compliance with requirements of all applicable statutes and rules.

c. Should the division or the slot machine licensee determine that any unauthorized transactions have occurred, the licensee shall immediately cease all data transfers that pass outside of the licensee's facility.

(I) In those case where the slot machine licensee detects unauthorized transactions have occurred, the licensee shall immediately notify the division in writing.

(II) Resumption of processing external to the licensee's facility shall occur only after the division issues written approval.

5. The licensee must, upon notification of an unauthorized transaction, immediately obtain a complete audit of the software and process by a independent testing laboratory licensed by the state.

6. The independent testing laboratory licensed by the state shall ascertain what error conditions exist and certify their correction and resolution of any future unauthorized transactions prior to the licensee receiving formal authority to resume data transfer activity originally granted under this rule.

(b) The slot machine licensee shall provide documentation of the applications communication requirements such as protocol, port, source and destination internet protocol (IP) address to a independent testing laboratory licensed by the state for certification.

(c) The connectivity provided by the licensee for data transfers must be configured to only permit approved application communication as defined in the application communication documentation provided.

(d) The data transfer program shall maintain an audit log and abort the data transfer process and generate an error event if the audit log becomes full. An audit log shall contain the following information:

1. All changes to configuration of the data transfer program; and

2. The source and destination IP addresses, port numbers, and media access control (MAC) addresses of all successful and unsuccessful transmission attempts when communicating data transfers outside of the slot machine licensee's facility.

(5) For purposes of establishing data transfer access to the FBMS, the slot machine licensee shall :

(a) Submit the identification of the remote location to which it proposes to provide data transfers to the division for approval no less than 10 days prior to the first intended data transfer.

(b) Certify to the division in writing that all data transfers shall be conducted over encrypted data lines secured from access from all unauthorized sources. that meet current National Institute of Standards and Technology (NIST) guidelines as of the date of the certification (TBD)

(c) Certify to the division that authentication to access the player tracking system shall be, at a minimum, two factor authentication that meet current NIST guidelines as of the date of the certification (TBD)

(d) Provide a written procedure within its internal controls to assure that each access authorization granted to an employee is disabled when that employee is transferred from those duties authorizing access to the player tracking system.

(e) Not grant access to any individual who does not possess a current and valid slot machine occupational license issued by the state.

(f) Provide certification quarterly to the division that:

1. All data transfers conducted over data lines are secure from access from all unauthorized sources by means of encryption that meets that meet current NIST guidelines as of the date of the certification (TBD)

2. Authentication used for access to the player tracking system is, at a minimum, two-factor authentication that meet current NIST guidelines as of the date of the certification (TBD)

; and

3. Each access authorization granted to an employee granted access to the player tracking system has been deleted upon the employee's transfer from those duties authorizing remote access to the player tracking system or licensensure expiration.

(6) A slot machine licensee shall provide in its system of internal controls a method of providing read only remote access to the facility based monitoring system for a business or person licensed as a business occupational licensee pursuant to Section 551.107(2)(a)(3), F.S., and authorized division personnel.

(7) The slot machine licensee's written internal controls providing for remote access shall provide for the following:

(a) Designation of an officer required to sign for acknowledgement of internal controls in subsection 61D-14.058(4), F.A.C., who shall be responsible for determining the need for remote access to the facility based monitoring system;

(b) The device or method through which remote access is given shall be taken offline when remote access to the player tracking system is not required;

(c) Limited access to any device or method used to establish remote access including:

1. A list of remote locations authorized for access to the facility based player tracking system.

2. A list of persons licensed pursuant to Section 551.107(2)(a), F.S., and division personnel, authorized to access the facility based player tracking system from an authorized remote location; and

3. A log with separate entries for each person and the dates and times when the remote access is enabled, disabled or modified.

(d) Maintenance of a log of each time remote access is provided, enabled, disabled or modified with a separate entry for each of the following:

1. The specific reason for which remote access was provided to another person or entity;

2. The name and occupational license number of the employee who authorized remote access to be provided to another person or entity;

3. The name and occupational license number of the employee of the slot machine licensee who established a remote access connection to the person or entity, if such employee is different from the employee provided in subparagraph (d)2.;

4. The name and occupational license number of the person and entity with whom remote access is established. If remote access is provided to an employee of a business occupational licensee, the name and occupational license number of both the employee and the business entity shall be entered on the log;

5. The date and time that remote access is established; and

6. The date and time that remote access is terminated.

(e) A written report to be provided to the division in no less than 24 hours after the remote access has been completed which shall include:

1. The reason that remote access was provided, enabled, disabled or modified;
2. The name of the employee of the slot machine licensee that authorized the remote access;
3. The name of the slot machine employee who established the remote access on behalf of the slot machine licensee;

4. The name of the person and entity with whom remote access was established;

5. The date and time remote access was established and concluded; and

6. A narrative report that shall describe:

a. Each component of the facility based monitoring system that was accessed; and

b. Whether the remote access was successful in resolving the issue described in subparagraph (d)1.

(f) Whenever unauthorized system access (remote or local) is suspected or actually occurs, a written report shall be provided to the division within 24 hours. The report shall notify the division when a password or similar device required for direct or remote access, use or maintenance of the facility based monitoring system employed by the licensed facility is or is suspected of being compromised. That written report shall include at a minimum the following:

1. Name of the facility;

2. Name and telephone number of corporate or administrative officer responsible for the operational integrity and systems security of the facility based monitoring system;

3. Name and position title of each individual to whom the compromised password was provided and the date (approximate when exact is not available) the password was provided and purpose for which the password was provided these individuals;

4. Last recorded date of authorized remote access to facility based monitoring system;

5. Date and approximate time it was discovered the password was compromised or lost;

6. Name, position and telephone number of individual who discovered or suspected the compromise of the password;

7. A brief explanation of the circumstances surrounding the use and discovery of the compromise; and

8. List of immediate corrective measures to protect the integrity of the facility based monitor system.

(8) Minimum waiver procedure to permit limited, non-accounting software and code maintenance prior to final independent testing laboratory certification.

(a) The slot machine licensee's shall include procedures within its written internal controls for requesting limited non-accounting software and code maintenance to the facility based monitoring system.

(b) The internal controls shall specify:

1. Waivers shall be submitted to the division and shall include the signature of the senior manager responsible for the licensed slot machine gaming facility. The waiver request addressed and delivered to the division must state:

a. That the software work requested pursuant to the specific waiver does not effect any accounting or metered records of any description.

b. The reason for the waiver request, why the maintenance access can not be accomodated in the next independent licenced laboratory certification; and

c. Explain the impact to continued operations if the waiver is not approved.

2. Requests shall be submitted no less than 72 hours prior to anticipated work on the effected code or software

3. The senior facility manager shall certify that a complete record of the software modification shall be recorded and provided an independent testing laboratory for certification within 24 hours of completion of the software modification in the facility based management system.

(c) The slot machine licensee shall contract with and submit all records to a independent testing laboratory and bear all expenses associated with that testing.

1. The licensee shall retain all software records prusuant to all software update for one year after that software update is replaced with software modifidation programs certified by an independent testing laboratory.

2. The slot machine licensee shall also submit a complete copy of all records for additional independent laboratory testing upon written request of the division.

(d) The division shall respond to the slot machine licensee's written waiver request within 72 hours of receiving that request. If the waiver request is disapproved, no software modifications shall be permitted. If the waiver request is approved, the facility must

1. Provide written notification of the start of the modifiction to the division at or before the time work is to comence;

2. follow all procedures listed in paragraph (3) and (4) above; and

3. Provide written notification of the completion of the modification to the division at the time work is complete and no later than 6 hours after completion.

~~(1) The firewall application shall maintain an audit log and disable all communications and generate an error event if the audit log becomes full. An audit log shall contain the following information:~~

- ~~(a) All changes to configuration of the firewall;~~
- ~~(b) All successful and unsuccessful connection attempts through the firewall; and~~
- ~~(c) The source and destination IP addresses, port numbers and MAC addresses.~~

~~(2) Except as provided in this section, the facility based monitoring system shall not allow for remote access and all access to the facility based monitoring system shall be conducted from within the slot machine licensee's facility. A slot machine licensee shall provide in its system of internal controls a method of providing limited remote access to the facility based monitoring system for a business or person licensed as a business occupational license pursuant to Section 551.107(2)(a)3., F.S., for performance of maintenance or diagnostics of the facility based monitoring system that cannot be performed by the slot machine licensee's on site personnel. The system of internal controls for such remote access shall provide for the following:~~

~~(a) Designation of an officer required to sign for acknowledgement of internal controls in subsection 61D-14.058(4), F.A.C., who shall be responsible for determining the need for remote access to the facility based monitoring system;~~

~~(b) The device or method through which remote access is given shall be taken offline when remote access is not required;~~

~~(c) Limited access to any device or method used to establish remote access including:~~

- ~~1. A list of persons authorized to modify or enable such a device or method used to establish remote access; and~~
- ~~2. Storage of any such device or method in a secure location that is not readily accessible to any person other than those listed under subparagraph (c)1.; and~~
- ~~3. A log with separate entries for each person and the dates and times when the remote access is enabled, disabled or modified.~~

~~(d) Maintenance of a log of each time remote access is provided, enabled, disabled or modified with a separate entry for each of the following:~~

- ~~1. The specific reason for which remote access was provided to another person or entity;~~
- ~~2. The name and occupational license number of the employee who authorized remote access to be provided to another person or entity;~~
- ~~3. The name and occupational license number of the employee of the slot machine licensee who established a remote access connection to the person or entity, if such employee is different from the employee provided in subparagraph (d)2.;~~
- ~~4. The name and occupational license number of the person and entity with whom remote access is established. If remote access is provided to an employee of a business occupational licensee, the name and occupational license number of both the employee and the business entity shall be entered on the log;~~
- ~~5. The date and time that remote access is established; and~~
- ~~6. The date and time that remote access is terminated.~~

~~(e) A written report to be provided to the division in no less than 24 hours after the remote access has been completed which shall include:~~

- ~~1. The reason that remote access was provided, enabled, disabled or modified;~~
- ~~2. The name of the employee of the slot machine licensee that authorized the remote access;~~
- ~~3. The name of the slot machine employee who established the remote access on behalf of the slot machine licensee;~~
- ~~4. The name of the person and entity with whom remote access was established;~~
- ~~5. The date and time remote access was established and concluded; and~~
- ~~6. A narrative report that shall describe:
 - ~~a. Each component of the facility based monitoring system that was accessed; and~~
 - ~~b. Whether the remote access was successful in resolving the issue described in subparagraph (d)1.~~~~

~~(9)(3) Automated ticket redemption machines are only to be used for the purpose of accepting, validating and providing payment for tickets inserted, or converting bills into smaller denominations. Automated ticket redemption machines shall not incorporate other functions. Automated ticket redemption machines shall use a communication protocol that shall not permit the automated ticket redemption machine to write directly to the system database and~~

only process payments based on commands from the system. Automated ticket redemption machines shall meet the slot machine hardware requirements for security and player safety, as set forth in Rules 61D-14.022-.044, F.A.C.

~~(10)~~(4) Automated ticket redemption machines shall be capable of detecting and displaying the following error conditions:

- (a) Power loss or power reset;
- (b) Interpretation of communication with the automated ticket redemption machine;
- (c) Cash dispenser empty or timed out;
- (d) RAM error;
- (e) Low RAM battery;
- (f) Ticket in jam;
- (g) Door open;
- (h) Bill acceptor stacker full;
- (i) Bill acceptor door open;
- (j) Bill stacker door open or bill stacker removed; and
- (k) Printer errors.

~~(11)~~(5) The error conditions referenced in subsection ~~(7)~~(4) shall illuminate the tower light alarm. The automated ticket redemption machine shall be able to recover to its prior operating condition.

~~(12)~~(6) Error conditions listed in paragraphs ~~(7)~~(4)(a)-(g) and (k) shall require a slot machine attendant to intervene and clear the error from the automated ticket redemption machine prior to the resumption of operation.

~~(13)~~(7) There shall be a maximum ticket value of \$500 that can be paid by an automated ticket redemption machine, per individual ticket.

~~(14)~~(8) The automated ticket redemption machine shall maintain the following meters:

(a) A "total in" meter that accumulates the total value of tickets or vouchers accepted by the automated ticket redemption machine; and

(b) A "total out" meter(s) for payments issued by the machine.

(c) Separate "out meters" shall report the value of all bills dispensed by denomination.

~~(15)~~(9) A log shall be maintained in critical memory or on a paper log housed within the individual automated ticket redemption machine that consists of the following:

(a) An event log which shall record the following information about the ticket redeemed:

- 1. Date/time of redemption;
- 2. Amount of ticket; and
- 3. At least last 4-digits of validation number; and

(b) The automated ticket redemption machine shall maintain the most recent 35 events in the event log.

~~(16)~~(10) Tickets may only be accepted by the automated ticket redemption machine when:

(a) All communication links are intact;

(b) Tickets inserted into an automated ticket redemption machine shall be rejected in the event of a communication failure; and

(c) Payment shall only be made when the ticket is collected and physically housed within the bill stacker.

~~(17)~~(11) A business occupational licensee who provides maintenance or diagnostic services under this section for a slot machine licensee by remote access shall maintain a log each time remote access is provided by a slot machine licensee with a separate entry for each of the following:

(a) The specific slot machine licensee;

(b) The name and occupational license number of the employee of the slot machine licensee who requested remote access;

(c) The name and occupational license number of the employee of the slot machine licensee who established a remote access connection to the business occupational license, if such employee is different from the employee provided in paragraph ~~(17)~~(11)(b);

(d) The name and occupational license number of the employee of the business occupational license who provides services to the slot machine licensee by remote access;

(e) The date and time that remote access is established; and

(f) The date and time that remote access is terminated.

~~(18)~~(12) A written report shall be provided by a business occupational licensee that performs maintenance or diagnostic services under subsection ~~(17)~~(11) to the division at the division's office located at the slot machine licensee's facility to whom services were provided by remote access. The report shall be postmarked for no less than

24 hours after the remote access has been completed which shall include:

- (a) The reason that remote access was provided;
- (b) The name of the employee of the slot machine licensee that authorized the access;
- (c) The name of the slot machine employee who established the remote access on behalf of the slot machine licensee;
- (d) The name of the person and entity with whom remote access was established;
- (e) The date and time remote access was established and concluded; and
- (f) A narrative report that shall describe:
 - 1. Each component of the facility based monitoring system that was accessed; and
 - 2. Whether the remote access was successful in resolving the issue described in subparagraph (2)(d)1.

Specific Authority 551.103(1), 551.122 FS.

Law Implemented 551.103(1)(d), (g), (i) FS.

History – New 8-13-06, Amended