Rule 3772-10-15 | Information technology controls.

(A) The casino operator's information technology ("IT") department ~~shall be~~is responsible for the quality, reliability, accuracy, security, and integrity of all gaming-related computer systems, regardless of the system's location.

~~(A) IT department personnel shall be prohibited from having a signatory ability on gaming-related documents affecting gross casino revenue and initiating general or subsidiary ledger entries.~~

~~(B) Each casino operator's internal control system shall contain provisions for information technology, which include, but are not limited to:~~

~~(1) Procedures for the control and installation of gaming-related system software. A software control log evidencing all authorized changes to software shall be maintained and reviewed for accuracy and completion by a member of the IT department, as designated by the casino operator's internal controls;~~

~~(2) Procedures for the examination of gaming-related system software to detect changes, whether authorized or not. The examination shall occur at least monthly and shall be logged and reviewed for accuracy and completion by a member of the IT department, as designated by the casino operator's internal controls;~~

(B) ~~A description of the secured~~ Each casino operator must provide hardware and software, approved by the executive director, for the exclusive use of the commission to facilitate access to the casino operator's gaming-related systems from commission offices.

(C) Each casino operator must provide the commission with a comprehensive list of all gaming-related computer systems in a format approved by the executive director. Each casino operator must provide updates to the list as changes occur.

~~(B)~~(D) The area where the gaming-related system servers and core components are located~~, including the physical security measures implemented to prevent unauthorized access and loss of data integrity. Non-IT department personnel shall be prohibited from having unrestricted~~ must be secured and access ~~to gaming-related system servers.~~ restricted to appropriate personnel. Access to the secured area ~~shall~~must be logged. The log ~~shall~~must be reviewed for accuracy and completion by a member of the IT department~~, as designated in the casino operators internal controls,~~ at least monthly. At a minimum, the log ~~shall~~must include the following information:

(1) Date and time the secured area was entered;

(2) Date and time the secured area was exited;

(3) Reason for access;

(4) First and last name of individual entering the area; and

(5) License number of individual entering the area, if applicable~~;~~.

~~(C)~~(E) ~~A description of the logical~~Logical access and security measures must be implemented on all gaming-related systems to segregate incompatible functions, prohibit unauthorized access, and prevent loss of data integrity. The measures ~~shall~~must include~~, but are not limited to~~:

(1) Creation and maintenance of gaming-related system user accounts~~. Accounts shall~~, which must be reviewed for appropriate access levels at least quarterly. The review ~~shall~~must be documented and checked for accuracy and completion by a member of the IT department~~, as designated in the casino operator's internal controls~~; and

(2) Gaming-related system user accounts must be authenticated prior to being given access. ~~A description of the~~Appropriate authentication ~~mechanism~~mechanisms (passwords, biometrics, etc.) and ~~the associated~~ security policies ~~shall~~must be ~~included~~used.

~~(D)~~(F) ~~Procedures for back~~Gaming-related system data must be backed-up and ~~recovery of gaming-related system data.~~recoverable. The back-up and recovery process ~~shall be logged and reviewed for completion and accuracy by a member of the IT department, as designated in the casino operator's internal controls;~~must be logged.

~~(E)~~(G) ~~Procedures for monitoring and reviewing gaming~~Gaming-related system security event logs ~~for~~ must be monitored and reviewed for suspicious activity and abnormal operation. ~~Completion of the procedures shall be logged.~~ The ~~log shall be reviewed for accuracy and completion by a member of the IT department, as designated in the casino operator's internal controls~~commission must be notified upon confirmation of any activity or abnormal operation that results in unauthorized access to, or loss of, gaming-related system data;

~~(F)~~(H) ~~Procedures for allowing remote~~Remote access to gaming-related systems~~. The procedures shall include~~ may be allowed, but ~~are not limited to~~must adhere to the following guidelines:

(1) ~~The process for establishing a~~A unique gaming-related system user account must be established for each vendor requesting remote access;

(2) ~~A description of the~~A dedicated and secure communication mechanism must be used to provide remote access~~, including applicable security and encryption parameters~~;

(3) ~~Steps taken to activate remote access capability for each~~Each instance of remote access must be activated by the casino operator's IT department;

(4) ~~Steps taken to deactivate remote~~Remote access ~~capability~~must be deactivated by the casino operator's IT department at the conclusion of each instance of remote access; and

(5) ~~Logging of each~~Each instance of remote access must be logged. At a minimum, the log ~~shall~~must include the following information:

a) Date and time remote access capability was activated;

b) Date and time remote access capability was deactivated;

c) System accessed, including manufacturer and version number;

d) First and last name of the individual or unique service request tracking number assigned by the licensed gaming-related vendor remotely accessing the system;

e) First name, last name, and license number of the IT department member who activated the remote access capability;

f) First name, last name, and license number of the IT department member who deactivated the remote access capability; and

g) The reason for remote access, including a description of the actions taken during the remote access session.

~~(G) Licensed gaming-related vendors shall maintain a log of each remote access session established with a gaming-related system. At a minimum, the log shall include:~~

~~(1) Date and time the remote access session started;~~

~~(2) Date and time the remote access session ended;~~

~~(3) Name of the casino the session was established with;~~

~~(4) System accessed, including manufacturer and version number;~~

~~(5) First and last name of the individual or unique service request tracking number assigned by the licensed gaming-related vendor remotely accessing the system; and~~

~~(6) The reason for remote access, including a description of the actions taken during the remote access session.~~

(I) Each casino operator's internal controls must contain provisions for IT, which include, but are not limited to:

(1) Procedures for the control and installation of gaming-related system software. A software control log evidencing all authorized changes to software must be maintained and reviewed for accuracy and completion by a member of the IT department; and

(2) Procedures for the examination of gaming-related system software to detect changes, whether authorized or not. The examination must occur at least monthly and must be logged and reviewed for accuracy and completion by a member of the IT department.