Ohio Administrative Code

Rule 3772-10-15 Information technology controls.

Effective: October 1, 2016

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

(B) 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.

(C) 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;

(3) A description of the secured 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 access to gaming-related system servers. Access to the secured area shall be logged. The log shall 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 include the following information:

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

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

(c) Reason for access;

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

(e) License number of individual entering the area, if applicable;

(4) A description of the logical access and security measures implemented to segregate incompatible functions, prohibit unauthorized access, and prevent loss of data integrity. The measures shall include, but are not limited to:

(a) Creation and maintenance of gaming-related system user accounts. Accounts shall be reviewed for appropriate access levels at least quarterly. The review shall 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

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

(5) Procedures for back-up and recovery of gaming-related system data. 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;

(6) Procedures for monitoring and reviewing gaming-related system security event logs 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;

(7) Procedures for allowing remote access to gaming-related systems. The procedures shall include,

but are not limited to:

(a) The process for establishing a unique gaming-related system user account for each vendor requesting remote access;

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

(c) Steps taken to activate remote access capability for each instance of remote access;

(d) Steps taken to deactivate remote access capability at the conclusion of each instance of remote access; and

(e) Logging of each instance of remote access. At a minimum, the log shall include the following information:

(i) Date and time remote access capability was activated;

(ii) Date and time remote access capability was deactivated;

(iii) System accessed, including manufacturer and version number;

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

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

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

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

(D) 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.