# Ohio Administrative Code

## Rule 3772-10-15 Information technology controls.

Effective: February 28, 2022

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

(B) 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 operators 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.

(D) The area where the gaming-related system servers and core components are located must be secured and access restricted to appropriate personnel. Access to the secured area must be logged. The log must be reviewed for accuracy and completion by a member of the IT department at least monthly. At a minimum, the log 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.

(E) 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 must include:

(1) Creation and maintenance of gaming-related system user accounts, which must be reviewed for appropriate access levels at least quarterly. The review must be documented and checked for accuracy and completion by a member of the IT department; and

(2) Gaming-related system user accounts must be authenticated prior to being given access. Appropriate authentication mechanisms (passwords, biometrics, etc.) and security policies must be used.

(F) Gaming-related system data must be backed-up and recoverable. The back-up and recovery process must be logged.

(G) Gaming-related system security event logs must be monitored and reviewed for suspicious activity and abnormal operation. The 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.

(H) Remote access to gaming-related systems may be allowed, but must adhere to the following guidelines:

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

(2) A dedicated and secure communication mechanism must be used to provide remote access;

(3) Each instance of remote access must be activated by the casino operators IT department;

(4) Remote access must be deactivated by the casino operators IT department at the conclusion of each instance of remote access; and

(5) Each instance of remote access must be logged. At a minimum, the log 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.

(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.