

3772-10-15 Information technology standardscontrols.

~~(A) Each casino operator licensee or casino operator applicant's internal control system shall include internal controls for information technology standards.~~

~~(BA) The casino operator's licensee's management information systemsinformation technology ("MISIT") department shall be responsible for the quality, reliability, and accuracy, security, and integrity of all gaming-relatedgaming-relatedslot computer systems used by the casino operator licensee, regardless of where whether data, software, or systems areof the system's are located within or outside the casino facility. The MIS department shall be responsible also for the security and physical integrity of, and the accountability and maintenance of, the following:~~

~~(1) Access codes and other security controls used to ensure limited access to computer software and the system-wide reliability of data;~~

~~(2) Computer tapes, disks, or other electronic storage media containing data relevant to the casino operator licensee's operations;~~

~~(3) Computer hardware, communications equipment, and software used in the conduct of the casino operator licensee's operations; and~~

~~(4) The computerized slot monitoring system utilized by the casino operator licensee.~~

~~(C) The technology standards shall include general controls for gaming hardware and software, including:~~

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

~~(AC) Each casino operator's licensee or casino operator applicant's internal control system shall include contain internal controlsprovisions for information technology standards, 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 departmentby a member of the IT department, as designated in the casino operator's internal controls,;~~

~~by the MIS department;~~

~~(2) The creation of a software control log by the MIS department evidencing all authorized changes to software;~~

~~(3) The review and comparison of the report and log required by the internal audit department for any deviations and investigation;~~

~~(42) Methods for detecting~~ Procedures for the examination of ~~gaming-related~~ 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~~ by a member of the IT department, as designated in the casino operator's internal controls,; and

~~(5) Methods for generating reports from all computer systems.~~

~~(D) These general controls shall include all of the following requirements:~~

~~(34) A description of the secured area where the gaming-related~~ 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~~ 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 operator's 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;~~

~~The casino operator licensee's management shall ensure that physical and logical security measures are implemented, maintained, and adhered to by personnel to prevent unauthorized access that could cause errors or compromise data or processing integrity;~~

~~(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~~ 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~~ by a member of the IT department, as designated in the casino operator's internal controls,; and

~~(b) Gaming-related~~ 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~~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~~by a member of the IT department, as designated in the casino operator's internal controls.;

(6) Procedures for monitoring and reviewing ~~gaming related~~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~~by a member of the IT department, as designated in the casino operator's internal controls.; and

(7) Procedures for allowing remote access to ~~gaming related~~gaming-related systems. The procedures shall include, but are not limited to:

(a) The process for establishing a unique ~~gaming related~~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:

(1) Date and Time remote access capability was activated;

(2) Date and Time remote access capability was deactivated;

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

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

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

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

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

(D) Licensed ~~gaming-related~~ gaming-related vendors shall maintain a log of each remote access session established with a ~~gaming-related~~ 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~~ 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.

~~(2) The casino operator licensee's management shall ensure that all new gaming vendor hardware and software agreements and contracts contain language requiring the vendor to adhere to internal control standards applicable to the goods and services the vendor is providing;~~

~~(3) Physical security measures shall exist over computers, computer terminals, data lines, and storage media to prevent unauthorized access and loss of integrity of data and processing; and~~

~~(4) The requirements in paragraph (C)(1) of this rule shall apply to each applicable department within the casino facility. Only authorized personnel shall have access to the following:~~

~~(a) Systems software and application programs;~~

~~(b) Computer data;~~

~~(c) Computer communications facilities;~~

~~(d) The computer system; and~~

~~(e) Information transmissions.~~

~~(E) The main computers for each gaming application shall be located in a secured area with access restricted to authorized persons, including vendors. Non-MIS department personnel shall be precluded from having unrestricted access to the secured computer areas.~~

~~(F) Access to computer operations shall be restricted to authorized personnel.~~

~~(G) Incompatible functions shall be adequately segregated and monitored to prevent lapses in general information technology procedures that could allow errors to go undetected or fraud to be concealed.~~

~~(H) The computer systems, including application software, shall be secured through the use of passwords or other means approved by the commission, if applicable. MIS department personnel shall assign and control the access to system functions.~~

~~(I) Passwords shall be controlled.~~

~~(J) Data backup and recovery procedures shall be established and followed.~~

~~(K) Information technology system documentation shall be maintained, including descriptions of hardware and software, including current version numbers of approved software and licensee manuals.~~

~~(L) MIS department personnel shall meet the following requirements:~~

~~(1) Be precluded from unauthorized access to the following:~~

~~(a) Computers and terminals located in gaming areas;~~

~~(b) Source documents; and~~

~~(c) Live data files, which shall not contain test data; and~~

~~(2) Be restricted from the following:~~

~~(a) Having unauthorized access to cash or other liquid assets; and~~

~~(b) Initiating general or subsidiary ledger entries.~~

~~(M) All program changes for in-house developed systems shall be documented and controlled in the manner established by the MIS department.~~

~~(N) The MIS department shall maintain computer security logs. If computer security logs are generated by the system, the logs shall be reviewed by MIS department personnel for evidence of unauthorized access or irregularities.~~

~~(O) The MIS department shall create controls for remotely accessing and logging changes to the casino's computer systems.~~

~~(P) If a casino operator licensee employs computer applications to replace or to supplement manual procedures, the computer application procedures implemented shall provide the same level of documentation or procedures, or both, that manual procedures approved by the commission require.~~

