112-104-25. Information technology standards. (a) Each facility manager's internal control system shall include internal controls for information technology standards. The internal controls shall be submitted to and approved by the commission according to K.A.R. 112-104-1. The management information systems (MIS) department shall be responsible for the quality, reliability, and accuracy of all EGM computer systems used by the facility manager regardless of whether data, software, or systems are located within or outside the gaming 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 systemwide reliability of data;

(2) computer tapes, disks, or other electronic storage media containing data relevant to the facility manager's operations;

(3) computer hardware, communications equipment, and software used in the conduct of the facility manager's operations; and

(4) the computerized EGM monitoring system utilized by the facility manager, which shall ensure that the following conditions are met:

(A) EGMs located on the gaming floor are connected to the facility manager's computerized EGM monitoring system and to the Kansas lottery's central computer system in accordance with the act;

(B) the security features of the computerized EGM monitoring system prohibit the deletion, creation, or modification of any data unless a permanent record is created that sets forth the original information, modifications to the original information, the identity of the employee making the modification, and, if applicable, the identity of each employee authorizing the modification;

(C) computerized jackpot payout systems utilized by the facility managers are configured to require that any modification of $100 or more to the original amount recorded on a computerized jackpot payout or system override is authorized by two cage department employees, one of whom is in a position of greater authority than the individual preparing the jackpot payout; and

(D) procedures and controls are in place that define and limit interaction between the EGM department, the cage department, and the accounting department and the computerized EGM monitoring system, including access to system menus, the establishment of EGM profile parameters, and the ability of each department to access, delete, create, or modify information contained in the EGM monitoring system.

(b) The internal controls specified in subsection (a) shall include general controls for gaming hardware and software. These general controls shall include all of the following requirements:

(1) The facility manager'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.

(2) The facility manager'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.

(4) The requirements in paragraph (b)(1) shall apply to each applicable department within the gaming 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.

(c) Each facility manager shall include the following in that facility manager's internal controls:

(1) The method for detecting authorized and unauthorized software changes;

(2) the generation of daily reports from all computer systems, which shall document any software changes;

(3) procedures for the control and installation of software by the MIS department;

(4) the creation of a software control log by the MIS department evidencing all authorized changes to software; and

(5) the review and comparison of the report and log required in paragraphs (c)(2) and (4) by the internal audit department for any deviations and investigation.

(d) 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.

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

(f) 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.

(g) 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.

(h) Passwords shall be controlled through both of the following requirements:

(1) Each user shall have that person's own individual password.

(2) Each password shall be changed at least quarterly with each change documented.

(i) MIS department personnel shall have backup and recovery procedures in place that include the following:

(1) Daily, monthly, and annual backup of data files;

(2) backup of all programs;

(3) secured off-site storage of all backup data files and programs or other adequate protection access to which shall be restricted to authorized MIS department personnel; and

(4) recovery procedures, which shall be tested on a sample basis at least semi-annually with documentation of results.

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

(k) 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.

(l) All program changes for in-house developed systems shall be documented as follows:

(1) Requests for new programs or program changes shall be reviewed by the MIS department supervisor. The approval to begin work on the program shall be documented.

(2) A written plan of implementation for new and modified programs shall be maintained and shall include the following:

(A) The date the program is to be placed into service;

(B) the nature of the change;

(C) a description of procedures required in order to bring the new or modified program into service, including the conversion or input of data and installation procedures; and

(D) an indication of who is to perform the procedures specified in paragraph (l)(2)(C).

(3) The testing of new and modified programs shall be performed and documented before implementation.

(4) A record of the final program or program changes, including evidence of user acceptance, the date in service, the name of the programmer, and the reason for changes, shall be documented and maintained.

(m) The facility manager 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 the following:

(1) Multiple attempts to log on. Alternatively, the system shall deny user access after three attempts to log on;

(2) unauthorized changes to live data files; and

(3) any other irregular transactions.

(n) The following requirements shall apply to accessing computer systems through remote dial-up or other methods as authorized by the commission:

(1) If remote dial-up to any associated equipment is allowed for software support, MIS department personnel shall maintain an access log that includes the following:

(A) The name of employee authorizing modem access;

(B) the name of authorized programmer or vendor representative;

(C) the reason for modem access;

(D) a description of work performed; and

(E) the date, time, and duration of access.

(2) The facility manager shall be required by the commission to maintain evidence of all changes being made during remote access sessions.

(o) Any facility manager may scan or directly store documents to an unalterable storage medium if all of the following requirements are met:

(1) The storage medium shall contain the exact image of the original document.

(2) All documents stored on the storage medium shall be maintained with a detailed index listing the department and date. This index shall be available upon request by the executive director.

(3) Upon request and adequate notice by the commission, hardware, including the terminal and printer, shall be made available in order to perform auditing procedures.

(4) Controls shall exist to ensure the accurate reproduction of records, including the printing of stored documents used for auditing purposes.

(5) The storage medium shall be retained for at least seven years.

(p) If a facility manager 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 provide. (Authorized by and implementing K.S.A. 2007 Supp. 74-8772; Sept. 26, 2008.)