112-110-3. Central computer system security. (a) Each CCS's database shall contain LFG data for at least the prior 24 months. Older data shall also be available from archives for at least seven years. The CCS's vendor shall provide archived data within 24 hours of a request for the data from the Kansas lottery or the commission.

(b) Each CCS shall be capable of the following:

(1) Receiving and retaining a record of events that affect security, including all door openings, stacker access, and signature failure;

(2) receiving and retaining a record of events that affect the LFG state, including power on, power off, and various faults and hardware failures;

(3) receiving and retaining a record of events that affect LFG integrity, including random access memory (RAM) corruption and RAM clear;

(4) receiving and retaining a record of events that affect the status of communication between all components including the LFG, including loss of communication;

(5) reporting of all events specified in this article;

(6) receiving and retaining a record of any other events as specified in writing by the Kansas lottery or the commission; and

(7) automatic reporting of faults that require a manual reactivation of the LFG. These faults shall include the following:

(A) Logic area cabinet access;

(B) LFG RAM reset;

(C) catastrophic software corruption;

(D) unrecoverable hardware faults; and

(E) a failed signature check.

(c)(1) A record of each of the events specified in subsection (b) shall be stored at the central point of the CCS on a hard drive in one or more files of an approved structure.

(2) The record of each stored event shall be marked by a date and time stamp.

(3) Each event shall be detected and recorded to the database and posted to a line printer or terminal monitor within 10 seconds of the occurrence.

(d) Each CCS shall meet the following security requirements:

(1) The ability to deny access to specific databases upon an access attempt, by employing passwords and other system security features. Levels of security and password assignment for all users shall be solely the function of the Kansas lottery;

(2) the ability to allow multiple security-access levels to control and restrict different classes of access to the system;

(3) password sign-on with two level codes comprising the personal identification code and a special password;

(4) system access accounts that are unique to the authorized personnel;

(5) the storage of passwords in an encrypted, nonreversible form;

(6) the requirement that each password be at least 10 characters in length and include at least one nonalphabetic character;

(7) password changes every 30 days;

(8) prevention of a password from being used if the password has been used as any of the previous 10 passwords;

(9) the requirement that the CCS lock a user's access upon three failed attempted log-ins and send a security alert to a line printer or terminal monitor;

(10) the requirement that connectivity to any gaming system from a remote, non-gaming terminal be approved by the executive director and reported to the Kansas lottery, in accordance with K.A.R. 112-107-31. Remote connections shall employ security mechanisms including modems with dial-back, modems with on-off keylocks, message encryption, logging of sessions, and firewall protection;

(11) the ability to provide a list of all registered users on the CCS, including each user's privilege level;

(12) the requirement that approved software and procedures for virus protection and detection, if appropriate, be used;

(13) the requirement that only programs, data files, and operating system files approved by the Kansas lottery and the commission reside on hard drive or in the memory of the CCS computers;

(14) the requirement that nonroutine access alerts and alarm events be logged and archived for future retrieval;

(15) the requirement that software signatures be calculated on all devices at all facilities and the signatures be validated by devices on the CCS network. These devices

shall include gaming equipment, location controllers, and cashier stations. These devices shall exclude non-gaming devices, including dumb terminals;

(16) audit trail functions that are designed to track system changes;

(17) time and date stamping of audit trail entries;

(18) capability of controlling data corruption that can be created by multiple log-ons;

(19) the requirement that the gaming software be maintained under an approved software change control system;

(20) the ability to send an alert to any terminal monitor and line printer for any security event that is generated at an LFG or in the system. The system shall allow the system administrator to determine which events should be posted. The events shall be filtered by location;

(21) equipment with a continuous power supply;

(22) the capability of on-line data redundancy if a hard disk peripheral fails during operation; and

(23) provision of a secure way through a graphic user interface for an auditor to make adjustments to the system. (Authorized by and implementing K.S.A. 2009 Supp. 74-8772; effective May 1, 2009; amended April 1, 2011.)