

112-104-34. Physical key controls; automated key controls. (a) "Sensitive keys" shall mean those unlocking devices designated by the Kansas lottery, a facility manager, or the commission as important to preserving the security of the facility manager's business. Each facility manager shall control the storage, duplication, custody, issuance, and return of sensitive keys. The sensitive key box may be stored in each facility manager's accounting department. At a minimum, the following keys shall be deemed sensitive keys:

- (1) The EGM belly glass key;
- (2) the tip box key, sometimes called a "toke box" key; and
- (3) the accounting or audit box key.

(b) Sensitive keys may be further designated as "critical." Critical keys shall mean those unlocking devices that shall be maintained in a dual-lock box. If a critical key is lost or becomes missing, all locks that the key fits shall be changed within 24 hours. At a minimum, the following keys shall be deemed critical keys:

- (1) The EGM central processing unit key;
- (2) the EGM main door key;
- (3) the EGM drop door key;
- (4) the bill validator door and box release key;
- (5) the bill validator contents key;
- (6) the jackpot or EGM reimpressionment kiosk keys;
- (7) the self-redemption or bill breaker kiosk keys;

- (8) the change cart key;
- (9) the key for each table game's drop box;
- (10) the key for the table game drop box release;
- (11) the keys for the bill validator and table drop storage cart;
- (12) the key for each table game's chip bank cover;
- (13) the key for each table game's chip tray;
- (14) the key for each progressive game's controller;
- (15) the key for each progressive game's reset switch;
- (16) the keys for the reserve chip storage;
- (17) the keys for the card and dice storage area;
- (18) the keys for the secondary chip storage area;
- (19) the access door key to any cage, EGM bank, or redemption booth;
- (20) the window key to any cage, EGM bank, or redemption booth;
- (21) the keys to the vault;
- (22) the keys to the soft count room; and
- (23) any key not listed in this subsection that controls access to any cash or chip

storage area.

(c) If a facility manager chooses to use rings to maintain its keys, each key on the ring shall be individually identified on a key access list.

(d) Each facility manager's internal control system shall include the following information:

- (1) The location of each sensitive key and critical key box;
- (2) each employee or contract job title that is authorized to access the sensitive key or critical key boxes;
- (3) the procedure for issuing and controlling the keys for the sensitive key or critical key boxes;
- (4) the sensitive key or critical key names, location, and persons authorized to sign out each sensitive key or critical key;
- (5) the location and custodian of each duplicate sensitive key; and
- (6) continuous surveillance coverage of each key box.

(e) If a facility manager chooses to use an automated key control system, the facility manager's internal control system shall include the following information:

- (1) A description of the automated system and its configuration, including how access is controlled;
- (2) the system's ability to provide scheduled and on-demand reports for a complete audit trail of all access, including the following:
 - (A) The identity of the key box;
 - (B) the identity of the employee;
 - (C) the identity of the keys;
 - (D) the date and time a key was removed;
 - (E) the date and time a key was returned;
 - (F) any unauthorized attempts to access the key box; and

(G) all entries, changes, or deletions in the system and the name of the employee performing the entry, change, or deletion;

(3) the employee position that is in charge of any automated key control system;

(4) each employee position that is authorized to enter, modify, and delete any keys;

(5) each employee position that is authorized to access the system;

(6) details about the alarms being used to signal for the following events:

(A) Overdue keys;

(B) open key box doors;

(C) unauthorized attempts to access; and

(D) any other unusual activities;

(7) any system override procedures; and

(8) a procedure for the notification of a commission security agent on duty if a partial or complete system failure occurs.

(f) Each individual authorized to access keys in the automated system shall have the authorization noted in the employee's personnel file.

(g) Each change to the list of authorized employees that have access to the automated keys shall be updated within 72 hours of the change. (Authorized by and implementing K.S.A. 2008 Supp. 74-8772; effective Oct. 16, 2009.)