MISSOURI GAMING COMMISSION

MINIMUM INTERNAL CONTROL STANDARDS
CHAPTER B – KEY CONTROLS

CONTENTS

§ 1   General

1.01   Sensitive keys are those keys that either management or the MGC considers sensitive to the Class B ~~L~~license's operation. All licensees must exercise strict control over storage, duplication, custody, issuance and return of sensitive keys. Sensitive keys shall not be removed from the premises. The Internal Control System (ICS) shall identify each sensitive key used by the Class B ~~L~~licensee. Sensitive keys shall be maintained in a dual locked sensitive key box and if lost, missing, or taken from the premises all locks the key fits must be immediately changed unless the ~~C~~commission, in its sole discretion, deems this is not necessary. If sensitive keys are maintained in an automated key box, the box shall require two keys, which shall be issued to individuals from different departments, to access the box when the box is accessed without using the automated system.

1.02   If key rings, which may have their own key ring number, are used, each key on the ring shall also be identified on the key access list individually.

1.03   The ~~Internal Control System~~ICS shall include:

(A)   ~~t~~The location of each sensitive key box;
(B)   ~~p~~Positions which have authorized access to the sensitive key box key(s) and how the keys to the sensitive key boxes are issued and controlled;
(C)   ~~s~~Sensitive key name, sensitive key identifier, location, custodian and job titles authorized to sign out each sensitive key;
(D)   ~~t~~The location and custodian of duplicate sensitive key boxes; and
(E)   ~~p~~Positions which have authorized access to the duplicate sensitive key box key(s) and how the keys to the duplicate sensitive key boxes are issued and controlled.

1.04   Each sensitive key box and duplicate key box shall have continuous surveillance coverage.

1.05   If an automated key control system is used, the ICS shall also include:

(A)   ~~a~~A general description of the automated system and its configuration including how access is controlled, which shall require a biometric scanner and alternative procedures for employees whose biometric feature cannot be scanned and for any period of time in which the biometric scanner ceases to function~~, e.g., hand reader, fingerprint, retina scan, password or PIN, etc.~~;
(B)   ~~s~~System capabilities to provide scheduled and on-demand reports for a complete audit trail of all access including the identity of the key box, identity of the employee, identity of the key(s), date and time out, date and time returned, as well as unauthorized attempts to access the key box and all entries, changes, or deletions in the system and the employee who did so;
(C)   ~~p~~Position in charge of any automated key control system;
(D)   ~~p~~Position(s) authorized to enter, modify, and delete which keys/which positions are authorized for access. Changes must be made within 72 hours of an employee

being suspended subject to termination by the Class B ~~L~~license or any change in job position or status that would result in a change in key access;

(E) ~~a~~Alarms for overdue keys, open doors, unauthorized attempts to access, and any other unusual activities;

(F) ~~s~~System override procedures that require the use of two keys issued to individuals in different departments to access the box and the use of a manual sensitive key log; and

(G) ~~i~~Immediate notification of an MGC agent in the event of system failure.

1.06 All keys and individuals authorized to access keys in the automated system shall be the same as those authorized on the key access list and access granted in the individual employee's job description.

§ 2   Procedures

2.01 Each sensitive key box custodian shall maintain a sensitive key access list noting authorized job titles that may access each sensitive key.

2.02 Whenever dual locks are required, two (2) different keys shall be required to access the controlled area. The two keys shall be issued to employees from two different departments and each key shall be independently signed out.

2.03 Keys which require issuance under ~~s~~Security or management escort shall be identified as such on the sensitive key access list and the key log entries shall indicate who originally escorted the key.

§ 3   Key Access List

3.01 A current and accurate key access list shall be maintained for each sensitive key box (excluding duplicate key boxes). The list shall be posted at the key box and a copy shall be given to the MGC boat supervisor.

(A) The list shall include the:
   (1) ~~k~~Key ring number, if applicable;
   (2) ~~k~~Key identifier/stamp on the key (must be unique for each key name);
   (3) ~~n~~Name of the key;
   (4) ~~l~~Location of the key;
   (5) ~~c~~Custodian of the key;
   (6) ~~q~~Quantity of the key(s); and
   (7) ~~j~~Job titles authorized to sign out the key and, if applicable, escort requirements and specific limitations.
(B) If any non-sensitive keys are maintained in the key box, they must be included on the sensitive key access list and denoted as non-sensitive on the list.

3.02 The custodian of duplicate keys shall maintain a duplicate sensitive key access list posted at each duplicate key box documenting:

(A)   ~~n~~Name of the key, which shall be identical to the key name on the sensitive key access list;

(B)   ~~t~~The key number;

(C)   ~~k~~Key identifier/stamp on the key (must be unique for each key name); and

(D)   ~~t~~The job titles authorized to sign out the key and, if applicable, escort requirements.

3.03   The ~~Internal Control System~~ ICS shall indicate which employees have the authority to make changes, deletions and/or additions to the sensitive key access lists and duplicate sensitive key access lists.

§ 4   Key Log

4.01   All sensitive keys shall be issued after proper completion of a sensitive key log, which shall include:

(A)   ~~d~~Date;

(B)   ~~k~~Key number or ring number;

(C)   ~~i~~Individual/automated key box issuing key;

(D)   ~~i~~Individual receiving key;

(E)   ~~t~~Time key signed out;

(F)   ~~t~~Time key signed in;

(G)   ~~i~~Individual returning key; and

(H)   ~~i~~Individual/automated key box receiving returned key.

4.02   The individual who signs out a sensitive key shall maintain custody of the key until the key is returned to the sensitive key box. Keys shall not be passed to other individuals, except keys utilized in the soft count room as noted below. In the event of an emergency (illness or injury rendering the individual incapable of returning the key) a supervisor may return the key with a notation on the Sensitive Key Log. If an automated key system is used and an emergency warrants the need for a supervisor to return a key for an individual, an explanation shall be documented as described in the ~~Internal Control System~~ICS. The only keys that may be passed are keys utilized within the soft count room, which may be issued to the count team lead and distributed to other count team members only while inside the locked count room.

4.03   Upon completion, sensitive key logs shall be forwarded at specified intervals to the Accounting department where they shall be reviewed and retained. If any discrepancies are found they shall be investigated and documented.

§ 5   Duplicate Keys

5.01   A duplicate key inventory log shall be maintained documenting the current issuance, receipt and inventory of all duplicate sensitive keys. The duplicate key inventory log shall include the following information:

(A)   ~~d~~Date and time;
(B)   ~~k~~Key name, which shall be identical to the key name on the sensitive key access list;
(C)   ~~k~~Key number;
(D)   ~~n~~Number of keys in beginning inventory;
(E)   ~~n~~Number of keys added or removed;
(F)   ~~n~~Number of keys in ending inventory;
(G)   ~~r~~Reason for adding or removing keys;
(H)   ~~s~~Signatures of the two individuals accessing the box; and
(I)   ~~s~~Signature of the individual receiving the key.

5.02   An inventory of duplicate sensitive keys shall be maintained in such quantity that there shall always be at least one duplicate sensitive key in inventory for each sensitive key, except for keys to bank bags. The duplicate sensitive keys shall be maintained in a duplicate sensitive key box.

§ 6   Broken, Lost or Missing Keys

6.01   The ~~Internal Control System~~ICS shall include procedures in the event a sensitive key is broken as to which employee shall receive and replace the broken key, disposition of the broken key and notification to the MGC boat agent on duty.

6.02   The ~~Internal Control System~~ICS shall include procedures to be followed when a sensitive key is lost, missing, or taken from the premises.

6.03   The ~~Internal Control System~~ICS shall include procedures for investigating and reporting missing sensitive keys. The MGC boat agent on duty shall be notified immediately of any missing or lost sensitive keys.

§ 7   Required Sensitive Keys

7.01   At a minimum, the following keys shall be considered sensitive keys:

(A)   EGD Central Processing Unit Key;
(B)   EGD Main Door Key (the key allowing access to the internal components of the EGD);
(C)   ~~k~~Keys allowing access to areas housing Critical IT Systems and equipment;
(D)   Toke Box Key;
(E)   Bill Validator Door and Box Release Key (shall have a Security escort for anyone other than count room employees);
(F)   Bill Validator Contents Key (shall have a Security escort for anyone other than count room employees);
(G)   EGD Belly Glass Key;
(H)   ~~Self~~-Redemption and/or ~~Bill Breaker~~Jackpot Kiosk Keys (~~D~~dual locks);
(I)   Wide Area Progressive Controller Compartment Key;

(J)   Table Game Drop Box Content Key (shall only be accessible to count room employees);
(K)   Table Game Drop Box Release Key;
(L)   BV and Table Drop Storage Cart Keys;
(M)   Table Games Chip Bank Cover Key;
(N)   Table Games Chip Tray Key;
(O)   Progressive Table Games Controller Key/Card/Fob (to adjust progressive jackpot meters or access CPSM game programs);
(P)   EGD Progressive Controller and Compartment Keys;
(Q)   Reserve Chip Storage Keys (Ddual locks);
(R)   Card and Dice Storage Area Keys (Ddual locks);
(S)   Secondary Chip Storage Keys (Ddual locks);
(T)   Access Door Key to any Sensitive or Controlled Area (e.g., cage, surveillance, Information Technology (IT) room(s), poller room, etc.);
(U)   Window Key (key to any cage or slot bank);
(V)   Vault Keys (Ddual locks);
(W)   Soft Count Room Keys (Ddual locks);
(X)   Accounting/Audit Box Key;
(Y)   Key to whiz machines;
(Z)   EGD Top Box Key;
(AA)   Poker Drop Box Contents Key;
(BB)   Bad Beat Drop Box Contents Key;
(CC)   Redemption Kiosk Logic Area Key;
(DD)   Jackpot Kiosk Logic Area Keys; and
(CCEE)   aAny keys not listed above controlling access to cash, cards, dice, or chip storage areas.

§ 8   Proximity Cards Used to Access Sensitive Areas

8.01   Proximity cards which are not maintained in a sensitive key box may be used in lieu of a sensitive key to access the following sensitive areas:

(A)   Information Technology (IT) room(s);
(B)   Areas housing Critical IT Systems;
(C)   Cage;
(D)   Card and Dice Inspection Room; and
(E)   Surveillance.;
(F)   EGD maintenance room; and
(G)   EGD storage room.

8.02   If a proximity card system is used to access sensitive areas, the cards shall be individually assigned. Any employee who is assigned a proximity card shall maintain possession of that card at all times and shall not allow his/ or her card to be used to allow unauthorized access to a sensitive area.

8.03   The system shall be capable of producing a report detailing the following information:

Effective TBD (Proposed).

    (A)   ~~c~~Card number;
    (B)   ~~n~~Name of employee to whom the card is assigned; and
    (C)   ~~s~~Sensitive areas which can be accessed by the card.

8.04   The system shall be capable of logging access to sensitive areas identifiable by card number and shall include the date and time. The system shall be able to provide reports for a complete audit trail of all access including:

    (A)   ~~t~~The identity of the proximity card;
    (B)   ~~i~~Identity of the employee to whom the card is assigned;
    (C)   ~~d~~Date and time;
    (D)   ~~u~~Unauthorized attempts to access sensitive areas; and
    (E)   ~~a~~All entries, changes, or deletions in the system and the employee who did so.

8.05   The ~~Internal Control System~~ICS shall specify the job position(s) in charge of the proximity card system and job positions authorized to make changes in the proximity card system. Changes must be made in the system within 72 hours of an employee being suspended by the Class B ~~L~~licensee or any change in job position or status that would result in a change in access to sensitive areas allowed by the proximity card.

8.06   The ~~Internal Control System~~ICS shall include procedures to be followed when a proximity card is lost, missing, or stolen. These procedures shall include immediately disabling the proximity card and immediately notifying the MGC agent on duty.

8.07   The ~~Internal Control System~~ICS shall include procedures to be followed in the event of proximity card system failure.