

SECTION 15
KEY AND ACCESS CONTROLS

15.1 Definitions

A. The definitions in this section shall apply to all sections of the part unless otherwise noted.

B. Definitions:

Access Badge / Card – a credential used to gain entry to an area having automated access control entry points.

Custody – directing and/or overseeing the use of a key and/or access badge/card.

Entry Access – is the ability to physically enter an area within a facility and classified as Highly Restricted, Restricted, or Unrestricted.

Entry Access – Highly Restricted – areas include but are not limited to:

1. Areas that contain equipment or control the HVAC systems or water supplies;
2. Areas that contain equipment or control the Safety and Security Systems;
3. Cage;
4. Chip Cage;
5. Chip Vault;

6. IT related areas, including areas where storage server racks are located;

7. Liquor storage;

8. Man Traps;

9. ~~Soft~~ Count room;

10. Surveillance; and,

11. Vault.

Entry Access – Restricted – areas include but are not limited to:

1. Back of House (area where employees and/or vendors have access and the public does not);
2. Players Club;
3. Point of Sale (POS) / cash drawers; and,
4. Warehouse/Storage areas (sensitive materials require locked cages with logs and camera coverage).

Entry Access – Unrestricted – areas are considered public access areas that do not require the use of a key or access badge/card to gain entry.

Keys – a metal instrument that when inserted into a lock and turned, operates the lock's mechanism. All keys within a facility shall be categorized as

SECTION 15
KEY AND ACCESS CONTROLS

Sensitive and Non-Sensitive with justification.

Keys / Locks / Access – Sensitive
– the following keys/locks/access shall be considered to be Sensitive and controlled in nature and shall include but not limited to:

1. Drop and Count:

- a. Casino instrument storage container release keys;
- b. Casino instrument storage container contents keys;
- c. ~~Soft~~ Count room; ~~and~~,
- d. Transport cart; ~~and~~,
- e. Storage racks used to secure casino instrument storage containers.

2. Electronic Gaming Systems:

- a. ~~Bill acceptor canister contents keys;~~
- b. ~~Bill acceptor canister release keys;~~
- a. Logic board / door keys;
- b. Machine data access/reset keys; and,
- c. Machine door/cabinet keys.

3. Table Games:

- a. Card room keys;
- b. Chip tray lid keys; ~~and~~
- c. ~~Drop box contents keys;~~
- d. ~~Drop box release keys; and,~~
- c. Pit storage cabinet keys.

4. Other:

- a. Accounting box;
- b. Electronic kiosks / Automated Teller Machines (ATM), ~~inclusive of kiosk currency cassettes;~~
- c. IT Server/computer rooms;
- d. Gaming related storage server racks;
- e. Key storage boxes / areas;
- f. Promotional devices (e.g. hoppers);
- g. Stationary and mobile POS/cash drawers;
- h. Surveillance; and,
- i. Vault / ~~main~~ cage areas.

5. Any keys not listed must be evaluated / categorized as approved by CNGC.

Lock – a fastening mechanism used to secure an area, door, etc.

SECTION 15
KEY AND ACCESS CONTROLS

operated/opened by a key and/or an access badge/card

Possession – maintaining and exercising physical control of a key and/or access badge/card.

15.2 General Standards

- A. Tier A casino operations shall be exempt from compliance with this section if the Cherokee Nation Gaming Commission (CNGC), or the operation as approved by the CNGC, establishes and the operation complies with procedures that maintain adequate key control and restricts access to sensitive areas.
- B. Tier B and C casino operations shall establish policies and procedures, subject to CNGC approval, that provide for proper key and access controls that meet the standards in this section.
- C. Key Controls shall provide for adequate segregation of duties and provide for adequate security of tribal assets.
- D. At no time shall any sensitive keys leave the gaming facility without the express written consent of the CNGC.
- E. Employees of the casino operation in custody of sensitive keys shall at no time have these keys leave their custody without the utilization of a

key log documenting the chain of custody for the sensitive keys in question.

- F. For sensitive keys locking mechanisms shall be unique for each type of key and property exclusive (e.g. locking mechanisms for ~~bill~~ ~~acceptor~~ ~~canister~~ [casino instrument storage container](#) release shall be exclusive to that purpose).
- G. Master keys for each property's sensitive keys / restricted areas shall be prohibited unless otherwise approved by the CNGC.

15.3 Key Inventory

- A. Inventory records shall be complete and shall indicate date keys are received into inventory and as applicable the date of removal or destruction as applicable.
- B. An inventory of all sensitive keys shall be maintained by the Security department and submitted to the CNGC, on a centralized standard form utilized by each property and approved by CNGC, which shall include the following:
 - 1. Assigned number (a separate number shall be assigned to each key);

SECTION 15
KEY AND ACCESS CONTROLS

2. Description (imprinted key number and designation and purpose);
 3. Location;
 4. Custodial department;
 5. Key Category (Sensitive and Non-Sensitive); and,
 6. Key Totals for each category.
- C. All duplicate keys shall be maintained in a manner that provides the same degree of control as the original. Duplicates shall not be made without prior written approval from management and the CNGC. Records shall be maintained for each key duplicated that indicate the number of keys made and destroyed.
- D. For the purchase/replacement of sensitive locks and/or keys, the purchase request must specify the need and be authorized by the operations management and Security supervisor with notice given to the CNGC.
- E. For on-site installation and repair, Security must accompany the vendor and Surveillance shall be notified.
- F. For off-site installation and repair, all locked items shall be inspected by an independent department before transport.

15.4 Manual Key and/or Access Control Logs

- A. Logs shall be maintained for sensitive keys and/or access to restricted areas as required and defined in this section.
- B. These logs shall be maintained by a designated custodial department/ key custodian and are the direct responsibility of the department manager.
- C. Logs must be maintained and available for review and/or inspection for at least one (1) year.
- D. Key logs shall be maintained for all highly restricted areas and sensitive keys as follows:
 1. Number and/or description of the key issued;
 2. Time and date the key was issued;
 3. Signature and employee number of the individual receiving the key;
 4. Signature and employee number of the individual issuing the key;
 5. Reason the key was issued;
 6. Time and date the key was returned;

SECTION 15
KEY AND ACCESS CONTROLS

7. Signature and employee number of the individual accepting the key at return; and,
 8. Signature and employee number of the individual returning the key.
- E. Manual access logs, where specific access is not granted as part of normal job duties, shall log entrance into highly-restricted areas. Such logs shall contain the following:
1. Area being accessed;
 2. Date/time of entry;
 3. Signature and employee number of employee entering highly-restricted area; and,
 4. Purpose of visit.

15.5 Computerized Key Security Systems

- A. Computerized key security systems which restrict access ~~to the gaming machine and table/card game drop and count~~ sensitive keys through the use of passwords, keys, or other means, other than a key custodian, must provide the same degree of control as indicated in the key control standards of this section. These standards shall be applicable to all tier levels. ~~of gaming.~~

- B. The following ~~additional gaming machine and table/card game~~ sensitive key control procedures shall apply:

1. Management personnel independent of the operational department (i.e., system administrator) shall assign and control user access to keys in the computerized key security systems to ensure that ~~the gaming machine and table / card game drop and count~~ sensitive keys are restricted to authorized employees.
2. In the event of an emergency or the key box is inoperable, access to the emergency manual key(s) used to access the box containing ~~the gaming machine and table/card game drop and count~~ sensitive keys, requires the physical involvement of at least three (3) persons from separate independent departments, including management, with the following documentation attested to by signatures of all participating employees signing out / in the emergency manual key(s):
 - a. The date and time; and,
 - b. The reason for the access.
3. The custody of the keys issued pursuant to Part 2 of this section requires the presence of

SECTION 15
KEY AND ACCESS CONTROLS

- two (2) persons from separate independent departments from the time of issuance until the time of their return.
4. Routine physical maintenance that requires accessing the emergency manual key(s) and does not involve the accessing of ~~gaming machine and table/card game drop and count~~ sensitive keys, only requires the presence of two (2) persons from separate departments with the following documentation attested to by signatures of all participating employees signing out/in the emergency manual key(s):
 - a. The date and time; and,
 - b. The reason for the access.
- C. Accounting / Audit personnel independent of the system administrator shall perform the following procedures:
1. Daily review the report generated by the computerized key security system indicating the transactions performed by the individual(s) that adds, deletes, and changes user's access within the system.
 2. Determine whether the transactions completed by the system administrator provide ~~an~~ adequate control over the access to ~~the gaming machine~~ ~~and table/card game drop and count~~ sensitive keys.
3. Determine whether any ~~gaming machine and table/card game drop and count~~ sensitive key(s) removed or returned to the key cabinet by the system administrator was properly authorized.
 4. For at least one (1) day each month, review the report generated by the computerized key security system indicating all transactions performed to determine whether any unusual ~~gaming machine and table/card game drop and count~~ sensitive key removals or key returns occurred.
 5. At least quarterly, review a sample of users that are assigned access to ~~the gaming machine and table/card game drop and count~~ sensitive keys to determine that their access to the assigned keys is adequate relative to their job position.
 6. All noted improper transactions or unusual occurrences are investigated with the results documented and submitted to the CNGC.
- D. Quarterly, an inventory ~~of all count room, drop box release, table/card game drop box release, storage rack, content keys, gaming machine door / access and reset /~~

SECTION 15
KEY AND ACCESS CONTROLS

~~override~~ / ~~panel~~ sensitive keys is performed and reconciled to records of keys made, issued, and destroyed.

- E. Investigations are performed for all keys unaccounted for, with the investigation being documented, and submitted to the CNGC.

15.6 Gaming Systems Keys

- A. For the installation of new gaming systems, standards set forth in Section ~~7.3(C)~~ 4(D) Gaming Systems – Machines of this document shall apply to this part.
- B. Storage server racks for gaming systems are required to be securely enclosed (covered backs with a lockable mechanism on the front panel).
- C. CNGC Agent(s) shall have sole custody of all keys to the logic board areas, or areas where programmable storage media are located.
- D. Upon verification of the proper locking mechanism of any gaming device, the following shall take place:
 - 1. Keys shall be logged by Security according to Key Inventory procedures in section 15.3;

- 2. Gaming device keys shall be separately stored from other keys to prevent unauthorized access; and,
- 3. Issuance of keys shall be determined based on the level of access and documented accordingly.

15.7 ~~Bill Acceptor Canister/Drop Box~~ Casino Instrument Storage Container Key Controls

- A. Procedures shall be developed and implemented to ensure that unauthorized access to ~~empty table/card game drop boxes~~ casino instrument storage containers shall not occur from the time the ~~boxes~~ containers leave the transport cart until they are placed ~~on the tables~~ in the appropriate asset.
- B. The involvement of at least two (2) persons, independent of the cage department, shall be required to access stored ~~empty table/card game drop boxes~~ casino instrument storage containers.
- C. ~~The~~ Casino instrument storage container release keys shall be separately keyed from the contents keys.
- D. For Tier A and B operations, at least two (2) count team members are required to be present at the time count room and other count keys are issued for the count. For

SECTION 15
KEY AND ACCESS CONTROLS

Tier C operations, at least three (3) (two (2) for table/card game drop box keys in operations with three (3) tables or fewer) count team members are required to be present at the time count room and other count keys are issued for the count.

- E. For Tier A and B operations, at least two (2) drop team members are required to be present at the time drop keys are issued and returned. For Tier C operations, at least three (3) (two (2) for table/card game drop box keys in operations with three (3) tables or fewer) drop team members are required to be present at the time drop keys are issued and returned.

15.8 ~~Bill Acceptor Canister/Drop Box~~ Casino Instrument Storage Container Release Keys

- A. The ~~bill acceptor canister~~ casino instrument storage container release keys shall be maintained by a department independent of the ~~gaming~~ operational department/revenue center.
- B. Only the person(s) authorized to remove ~~bill acceptor canisters from the gaming machines~~ casino instrument storage containers shall be allowed access to the release keys.
- C. Persons authorized to remove the ~~bill acceptor canisters~~ casino instrument storage containers shall be precluded from having

simultaneous access to the ~~bill acceptor canister~~ the contents keys and release keys.

- D. For situations requiring access to a ~~bill acceptor canister / drop box~~ casino instrument storage container at a time other than the scheduled drop, the date, time, and signature of the employee signing out/in the release key must be documented.
- E. ~~The table/card game drop box release keys shall be maintained by a department independent of the table/card games department.~~
- F. Only the person(s) authorized to remove ~~table/card game drop boxes from the tables~~ shall be allowed access to the ~~table/card game drop box~~ casino instrument storage containers may have access release keys; however, the count team members may have access to the release keys during the ~~soft~~ count in order to reset the ~~table/card game drop boxes~~ containers, if required.
- G. ~~Persons authorized to remove the table/card game drop boxes shall be precluded from having simultaneous access to the table/card game drop box contents keys.~~

15.9 ~~Bill Acceptor Canister/Drop Box~~ Casino Instrument Storage Container Transport Cart Keys

SECTION 15
KEY AND ACCESS CONTROLS

- A. Persons authorized to obtain ~~bill acceptor-canister~~ transport cart keys shall be precluded from having simultaneous access to ~~bill acceptor-canister~~ casino instrument storage container contents keys, with the exception of the count team.
- B. For Tier C operations, Security shall be required to accompany the ~~bill-acceptor-canisters~~ transport cart keys and observe each time ~~canisters~~ casino instrument storage containers are removed from or placed in storage racks.
- C. Persons authorized to obtain ~~table/card game drop-box~~ transport cart keys shall be precluded from having simultaneous access to ~~table/card game drop-box~~ casino instrument storage container contents keys, with the exception of the count team.
- D. For Tier C operations, a person independent of the ~~pit~~ department shall be required to accompany the ~~table/card game drop-box~~ storage rack keys and observe each time ~~table/card game drop-boxes~~ are removed from or placed in storage racks. **542.41(p)(1)**

**15.10 ~~Bill-Acceptor-Canisters/Drop-Box~~
Casino Instrument Storage
Container Contents Keys**

- A. The physical custody of the keys needed to access the contents of the stored, full ~~bill-acceptor canister/drop-box~~ casino instrument storage container contents, shall require the physical involvement of persons from two (2) separate departments, with the exception of the count team. Note: the key custodian checking out keys constitutes physical involvement.
- B. Issuance of the ~~bill-acceptor canister / drop-box~~ casino instrument storage container contents keys at other than scheduled count times shall require the involvement of at least two (2) persons for Tier A and Tier B and at least three (3) persons for Tier C operations from separate departments, one of whom must be a supervisor. The reason for issuance shall be documented with the signatures of all participants and observers. Two employees from separate departments are required to accompany the contents keys from the time the keys are issued until the time the keys are returned.
- C. Only the count team members shall be allowed access to ~~bill-acceptor canister / drop-box~~ casino instrument storage container contents keys during the count process.

SECTION 15
KEY AND ACCESS CONTROLS

15.11 Computerized Entry Access Control Systems

- A. The utilization of Computer Access Control Systems at any facility must be reviewed and approved by CNGC.
- B. Computerized entry access permissions must be controlled by one or more designated persons within Security Operations. A permissions matrix and/or procedures shall be established, as approved by the CNGC.
- C. The operation, as approved by the CNGC, shall establish procedures for reviewing access and reporting unauthorized access. Access control personnel shall review, at least quarterly, a sample of users that are assigned access to determine proper authorization and assurance.
- D. All noted unauthorized access shall be investigated with the results documented and submitted to the CNGC.
- E. Vendor access for the purpose of performing work shall require an escort for the duration of the work. The escort shall be a representative from the department relative to the work being performed (e.g. IT personnel for work being performed in data closets).
- F. Non-gaming facility personnel shall not be issued a sensitive key

- or given an access badge/card to access restricted areas without approval from CNGC or a permit or license issued by CNGC.
- G. Individuals / employees must maintain possession of the access badge / card issued to them.
- H. A lost or stolen access badge/card shall be reported to Security immediately and the access badge/card must be rendered inactive. Any found access badges/cards shall be returned to Security.
- I. All employees/vendors that are issued an access badge / card must scan the access badge / card prior to entering any area that utilizes a computerized access device regardless of their access permissions.
- J. Access badges / cards assigned to any employee must be rendered inactive if:
 - 1. The employee will be on leave for a period of two consecutive weeks or more;
 - 2. The employee is terminated or separates from the company; or,
 - 3. The employee is suspended.
- K. Actions under Part J of this section are governed as follows:

SECTION 15
KEY AND ACCESS CONTROLS

1. For J (1) and J (3), an employee may surrender his/her badge / card, which must be maintained by the employee's supervisor / manager or by Security. The badge/card may be re-issued upon the employee's return.
 2. If the badge / card is not surrendered, the employee's supervisor / manager shall notify the Access Control Administrator to deactivate the badge/card. The badge / card may be reactivated upon the employee's return.
 3. For any employee that is terminated or otherwise separates from employment, the employee's supervisor / manager or Employee Services shall notify the Access Control Administrator by no later than the end of the next business day.
- L. Non-gaming facility personnel must surrender any and all issued keys and/or access badges / cards and the Access Control Administrator shall deactivate access badges / cards upon their termination of services or employment.
- M. Access permissions must be evaluated and changed according to the approved policy / matrix immediately upon notification of a

change in employee status or position.

15.12 Password/Personal Identification Number (PIN) Integrity

Procedures shall be developed and implemented to ensure password / PIN integrity for access into casino ~~operating key control and access~~ systems, which shall include:

- A. Assignment of unique password/PIN for each user, ~~if applicable~~.
- B. Sharing of passwords / PINS is strictly prohibited.
- C. Passwords / PINS can only be issued and/or changed by ~~Information Technology~~ personnel independent of the operational department/revenue center being granted access.
- D. ~~Security~~ Access shall be reviewed by ~~Information Technology~~ personnel or department independent of the system administrator on a regular basis for terms or changes in access.