SECTION 10

KEY CONTROL

A. GENERAL

Keys to restricted areas are kept in two-keyed locked boxes. These locked boxes are securely attached in the cashier cage and clearly visible by surveillance. The cashier is the custodian of the two-keyed locked boxes and the restricted keys maintained within. The cashier is responsible for ensuring only authorized employees are allowed to check out restricted keys. This is achieved by verifying the employee's authority listed on the key authorization log or signature card. The cashier is also responsible to ensure restricted keys are returned in a timely manner and all keys are properly accounted for at the end of his/her shift. The cashier performs a review of the key logs at the end of each shift to ensure all restricted keys accessed throughout his/her shift, which are not currently in use (e.g., by the drop or count teams, on-shift employees, slot machine repair, BV repair, etc.) have been returned to the appropriate locked boxes. In the event the keys have not been returned, the cashier is to notify the gaming manager. Unless otherwise indicated in the ICMP, all restricted keys must be immediately returned to their applicable restricted key box once the licensee has completed the task for which the keys were originally checked out.

For the purposes of this section, premise is defined as the gross building area, as reflected on the casino's gaming map. Restricted gaming keys are not allowed off the premises; however, the slot door and kiosk door keys may be carried anywhere in conjunction with the individual's regular responsibilities while on duty. These keys are NOT allowed to be taken off premises when the individual is not on duty. If it is suspected there was unauthorized use of a restricted key, suspicion of criminal activity in regard to restricted keys, or if a restricted key is missing, the Division must be immediately notified. Additionally, the key control log must indicate any such activity.

For commonly owned casinos physically connected by a wall with an opening between the casinos, employees may go between the casinos with the restricted keys on his/her person in order to perform his/her job duties. This is allowed as long as the employee does not leave the building or go outside.

Locks requiring the use of restricted keys must be keyed differently in order to maintain an adequate control environment. Examples include:

1. The key used to access the slot machine door may not be the same as the key used to access the drop door.
2. The key used to release the slot machine bill validator (BV), (BV Release Key) may not be the same as the key used to release the kiosk stacker (Kiosk Stacker Release Key).
3. The key used to access the contents of the slot machine BV (BV Content Key) may not

be the same as the key used to access the contents of the kiosk stacker (Kiosk Stacker Content Key).

Restricted and non-restricted keys may not be keyed the same. For example, the BV Release Key may not be keyed the same as the Belly Glass Door Key. The intent is to ensure adequate segregation of access to restricted areas and funds. One person may not have the BV Release Key and the BV Content Key at the same time.

A minimum of two locked boxes for restricted keys are required to establish an adequate control environment. Locked box #1 (box 1) is referred to as the security locked box and locked box #2 (box 2) is referred to as the gaming manager locked box. Non-restricted gaming keys are not allowed to be kept in box 1 or box 2, unless specifically allowed by ICMP.

The Division recommends that general (non-restricted) gaming keys be maintained in a separate locked box #3 (box 3). Two locks are <u>not</u> required on box 3. If general, non-restricted gaming keys (e.g., pit podium key, table tray key, change bank key, etc.) are maintained in box 3, they may be checked out at the beginning of each shift, for the entire shift. The licensee must have procedures in place to ensure the accountability of the keys maintained in the non-restricted locked box.

Between shifts, restricted and non-restricted keys may be transferred to the individual responsible for the keys during the following shift by having that individual sign the key log. The cashier does not need to initial the log or physically transfer the key to the following shift individual. The control objective is to secure these keys when they are not being used, to prevent unauthorized access to or use of the keys and to document existing possession/responsibility for the keys.

Restricted keys must be inventoried at least twice a year. This includes **all** locked boxes containing restricted keys. The restricted key inventories may be accomplished in conjunction with the completion of the compliance checklists by the internal compliance officer. Evidence the inventory was performed must be documented and must include, at a minimum, the names, signatures and license numbers of the individuals performing the inventory count, the date the inventory was performed, and the results of the inventory. Any restricted keys missing or unaccounted for must be immediately reported to the Division. The Division will determine if it is necessary for all the associated locks to be replaced or re-keyed. An accurate detailed inventory listing is maintained in association with each restricted key box at all times.

To ensure an appropriate key control environment, a person may not have access to more than one key box. For example, if one employee is considered the gaming manager and is also acting as security, this person may not have both the gaming manager's key and security's key which are used to access boxes 1 and 2. The gaming manager's key and security's key used to access boxes 1 and 2 must be maintained by two different licensed individuals.

No keys are to remain inserted into the locks of boxes that provide access to restricted keys.

The cashier, gaming manager, and security must maintain control over their respective key at all times.

Licensees may utilize an Automated Key Tracking System (AKTS) to maintain their key control environment. An AKTS replaces the cashier's custodial functions in regard to the two-keyed locked boxes and the restricted keys that are maintained within. Licensees using an AKTS must achieve the same level of controls and safeguards as described for a manual key control environment.

Boxes 1 and 2 are securely attached to an area clearly visible by surveillance in the cashier cage. Locked boxes utilized for an AKTS must be securely attached to an area clearly visible by surveillance. Access to keys or areas accessed through the use of restricted keys is limited to only authorized individuals. Key authorization is granted through the use of key authorization logs or signature cards for a manual key control environment and utilization of an AKTS. The AKTS must accurately reflect the authorization reflected on the log or signature cards.

B. KEY CONTROL ENVIRONMENT

The following diagram represents the key control environment. The diagram reflects the restricted keys maintained in box 1 and box 2 and the licensed positions that control the access to the keys maintained in the boxes. The diagram also reflects which keys may be accessed by one person and which keys must be accessed by two people.

❶ = 1 person required to log into the AKTS to access the key.
❷ = 2 people required to log into the AKTS to access the key. Regardless of the key control environment (manual or AKTS) keys listed with ❷ next to them must always be accompanied by two (2) people; the person using the key to complete a procedure and a second person to escort the key and observe the procedure in which the key is being used. Unless otherwise indicated, the second person does not need to be the person who authorizes access to the key.

Where the diagram below reflects a ❶, one person is required to access a restricted key from the AKTS. This person does not need authorization by the gaming manager or a member of security each time the key is obtained. For example, the Slot Machine Door Key can be accessed by any authorized casino employee should his/her job function dictate the use of said key.

Where the diagram below reflects a ❷, two people are required to access a restricted key from the AKTS. One (1) of the two (2) people must either be the gaming manager or a member of security based on which box the key would be maintained in, if a manual key control environment was being utilized. For example, the Count Room Key is accessed using a member of security and another authorized licensed individual because this key would normally be kept in box 1 in a manual control environment; likewise, the Table Drop Box Content Key(s) is accessed using the gaming manager and another authorized licensed individual because this key would normally be kept in box 2 in a manual key control environment.

Locked Box #1			Locked Box #2		
		Keys to access locked box #1 First key – Cashier Second key – Security The following keys are kept in locked box #1:			Keys to access locked box #2 First key – Cashier Second key – Gaming Manager The following keys are kept in locked box #2:
❷		Table drop box rack key			
❷		Table drop box release key(s)	❷		Table drop box content key(s)
❶		Table multi-shift drop box shift change key			
❶		Card cabinet key			
❶		Dice cabinet key (primary & secondary storage)			
❶	*M	Security key to table games progressive controller	❶	*M	Gaming Manager key to table games progressive controller
❷		Slot Machine drop key	❶	*A	Slot Machine door key, may have meter keys on the same ring
❷		Bill validator rack key			
❷	*B	Bill validator release key	❷		Bill validator content key
❷		Emergency BV drop cabinet key			
❷		Kiosk stacker release key	❷		Kiosk stacker content key
❶	*C	Security Kiosk door key	❶	*C	Gaming Manager Kiosk door key
❶		Kiosk cassette release key			
❷		Kiosk stacker rack key			
❶		Handheld validation unit cabinet key			
❷	*D	Count room key	❶		Locked dispensing machine key
❶	*E	Owner/Operator/Designee vault key	❶	*E	Gaming Manager vault key
❶	*F	Calibration module key	❶	*F	Calibration module key
❶	*G	Security key to duplicate key locked box	❶	*G	Gaming Manager key to duplicate key locked box
❶	*H	Security duplicate key to the two keyed Drop Key Box	❶	*H	Gaming Manager duplicate key to the two keyed Drop Key Box
❶	*I	Security key to progressive controller	❶	*I	Gaming Manager key to progressive controller
❶	*J	Security key to BV release two keyed locked box	❶	*J	Duplicate of slot tech key to BV release two keyed locked box
			❶	*K	W-2G reset key
❶	*L	Security key to unused excess chips & tokens	❶	*L	Gaming Manager key to unused excess chips & tokens

*[A] The slot tech key rings containing the slot door keys, meter reset keys, and other non-restricted keys, can be maintained in a separate dual locked box (e.g., slot tech locked box) in addition to box 2. This separate box must be under surveillance and may be located in the slot supervisor's office, gaming manager's office, surveillance room, security office or similar secure area. Access to the box is restricted to the slot tech and gaming manager. Both individuals maintain control of his/her respective key and both must be present to access the box. Keys from the box are checked out and checked in on the key access log located near the box. The log is forwarded to accounting once a page is completed.

*[B] The licensee may have someone from security check out the BV Release Key for the entire shift. Two licensed individuals, one of which is security, must be present when the BV Release Key is used.

*[C] Access to the kiosk stacker requires a minimum of two individuals. An adequate key control environment must be established to ensure compliance with this requirement. For kiosks that require two door keys, one key must be maintained in box 1 and the other in box 2. The door keys may be checked out for the entire shift by two separate individuals. Both individuals must be present when the kiosk is accessed. The Kiosk Stacker Release Key may be checked out for the entire shift by one of the individuals maintaining one of the door keys. For kiosks that require one door key and one Kiosk Stacker Release Key, these keys may be checked out for the entire shift by two separate individuals. For kiosks that require only one door key the Kiosk Door Key is maintained in box 2. Whether the kiosk utilizes one or two door keys, at no time may one individual access the kiosk funds alone.

*[D] The Count Room Key must be immediately checked in once the licensee has completed the task for which the key was originally checked out. When accessing the count room for purposes other than drop and count, it is not required for a second person to escort the person receiving the key, provided there are no unsecured funds in the count room.

*[E] Access to the vault requires dual access (i.e., two individuals, each with a unique key or lock combination). One key or lock combination is kept in the possession of the owner/operator (or his/her designee) and the other in the possession of the gaming manager. Alternatively, the two keys to the vault may be kept in the two-keyed locked boxes, with one key in box 1, and the second key in box 2. If access to the vault includes a combination lock, the combination to the lock must be changed on a regular basis (at a minimum every 6 months) and immediately when there is a change in or termination of personnel who have knowledge of the combination.

*[F] If the licensee elects to secure the weigh scale with a lock and key, the key is maintained by the manufacturer or manufacturer's representative. Alternatively, the key may be maintained in either box 1 or box 2, with only the manufacturer or manufacturer's representative having authority to obtain the key. The manufacturer or manufacturer's representative must sign the key access log when checking the key out.

*[G] Dual locks are required for the duplicate key box. If the licensee does not have a vault, the

duplicate keys must be stored in a two-keyed locked box in the accounting office, in the security office, or in another secure area limiting access to authorized personnel only. One key to the locked box for the duplicate keys is maintained in box 1. The second key to the duplicate key box is maintained in box 2. The duplicate key box must be in a secure location and must be under surveillance coverage.

***H** The licensee may establish a Drop Key Box, which is a two-keyed locked box. The Drop Key Box must be under surveillance and must be secured to prevent unauthorized access. The objective is to preclude access to the Drop Key Box by one individual. Two separate licensed individuals must each maintain one key to the Drop Key Box. The drop/count team leader maintains one key to this box. A duplicate of the drop/count team leader's key is maintained in box 2 in case any drop keys need to be checked out and the drop/count team leader is not present. The second key to access this box is maintained in box 1 or by another drop team member. If the (security) key to the Drop Key Box is not maintained by another drop team member, it is checked out from the cage or AKTS. It takes two licensed people to access the Drop Key Box and a key log must be maintained to document key check out and key check in. The key log is forwarded to accounting once a page is complete. For any break taken either prior to or during the drop and count, all keys should be checked back into the Drop Key Box. At the conclusion of the break, all keys should be checked out again pursuant to standard key check out procedures. Alternatively, the keys may be maintained by at least three count team members who are required to stay together and are under surveillance at all times. Access to the keys in the Drop Key Box is pursuant to standard key check out and check in procedures.

In order to access the BV stacker on some slot machines, the drop team needs access to the Slot Machine Door Key. The Slot Machine Door Key may also be kept in the Drop Key Box.

If the count team uses "test money", which is a predetermined amount of money and tickets, and it is maintained in the count room in a sealed compartment for the purpose of testing the currency counter, the key to access the test money may also be kept in the Drop Key Box.

If the kiosk drop and/or count are performed at a time when the cashier is not present, the keys needed to conduct the kiosk drop and/or count can be maintained in the Drop Key Box or another key box with the same control features.

Keys needed to conduct the table count can be maintained in the Drop Key Box or another key box with the same control features. Note that the table drop box release keys are NOT allowed to be maintained in the Drop Key Box.

Only the keys needed to perform the specific function (e.g., slot drop) are checked out of the Drop Key Box. Upon completion of the function (e.g., slot drop), the keys are checked back into the Drop Key Box.

The drop and count teams must obtain only those keys that are necessary to perform their respective function (e.g., the drop team is not allowed to have the BV content key). Drop and

count functions may proceed simultaneously; however, the restricted keys must be maintained by the respective teams. The checking out of the Slot Machine Drop Key(s) or BV Release Key(s) signifies the beginning of the slot drop function. The kiosk count team can only check out the keys to conduct the kiosk count. All keys checked out are returned to the Drop Key Box immediately upon completion of the function for which the keys were checked out.

***[I]** The two locks providing access to the progressive controller must be keyed differently. One of the locks may be keyed the same as the slot machine drop cabinet. If one of the progressive controller access keys is the same as the Slot Machine Drop Key, this key must be maintained in box 1. One person may not have access to both progressive controller keys at the same time. One of the progressive controller keys must be maintained in box 1 and the other key must be maintained in box 2.

***[J]** The licensee may establish a BV Release Key Box, which is a two-keyed locked box. The slot tech maintains one key to this box and security maintains the other key. A duplicate of the slot tech's key is maintained in box 2. Security's key is maintained in box 1. The controls and procedures for checking out the BV Release Key are the same as for checking out any restricted key. It takes two licensed people to access the box and a key log must be maintained to document key check out and key check in. The BV Release Key is checked in and out of the key box as repairs are needed. The BV Release Key Box must be under surveillance and must be secured to prevent unauthorized access.

***[K]** Some slot machines allow patrons who have won credits greater than the hopper lock out amount to continue playing these credits once the slot attendant resets the game. If a jackpot of $1,200 or more occurs on one of these slot machines, a W-2G must be completed. To reset the game and allow the patron to continue playing these credits, the attendant uses a second reset key switch (which is in the same proximity as the jackpot reset key switch). The casino must replace the lock shipped with the machine with a casino specific lock and key before these games can be played. This key, called a W-2G reset key, is considered a restricted key and must be stored in box 2.

***[L]** If unused and excess chips and tokens are stored in a dual locked area, one key is maintained in box 1 and one key is maintained in box 2.

***[M]** Each table's progressive controller box must be housed such that access to the controller requires dual access, which may not necessarily be accomplished through the use of two keys.

<u>Other Key Control Procedures</u>

The Slot Machine Door Key, the BV Release Key Box Key, BV Release Key (see requirements noted above), Kiosk Door Key, Kiosk Stacker Key, Handheld Validation Unit Cabinet Key and Table Games Progressive Key may be checked out at the beginning of each shift for the entire shift. In between shifts, the keys may be transferred to the authorized individual on the following shift by having that individual complete the key log. The cashier does not need to

initial the log or physically transfer the key. Licensees utilizing an AKTS may not transfer keys between individuals. Keys must be returned to, and checked out of, the AKTS. The control objective is to secure these keys primarily if the casino is closed and to document who has control and responsibility for the keys.

All BV boxes must have a lock to restrict access to the box contents. This lock must be keyed differently than the BV Release Key, as well as the Slot Machine Door Key. All table game drop boxes must also have a lock to restrict access to the box contents, which must be keyed differently than the key to release the box from the table.

If slot count and table games count are performed in two separate rooms, each room must be keyed differently so that slot count team members may not gain unauthorized access to the table games count room and vice versa.

Broken keys, or keys for locks that have been changed, may be destroyed and discarded at the licensee's discretion, or given to a locksmith to destroy. If a duplicate key is issued in place of a broken key, the duplicate key control log must indicate this as the reason for removal of the key from the duplicate key locked box.

C. KEY CONTROL LOGS

Regardless of whether a manual or an AKTS environment is in place, access to all restricted keys must be documented.

Key control logs must be located near the associated key box. The entire transaction of checking keys out/in and recording of such is captured by a single surveillance camera.

In a manual environment, key logs are used to document key access. A key control log is kept for each locked box and is completed every time a key is checked out or in. The log is forwarded to accounting for review once a page is complete, but at least monthly. Key logs must include the following information: (It is recommended that the same controls be used for non-restricted gaming keys.)

1. Date of issuance.
2. Time of issuance.
3. Signature and gaming license number of the individual receiving the key (the person receiving is the person who will be using the key to complete a procedure).
4. Key number.
5. Reason for removal of key (e.g., perform table games drop, perform slot drop, etc.). The description must be detailed so a reviewer can determine what the key was used for.
6. Initials of cashier issuing key (if manual system is used).
7. Initials of gaming manager or security employee witnessing issuance of key.
8. Date of return.
9. Time of return.

10. Initials of individual accepting the return of key (i.e., cashier) if manual system is used.

When a key is requested in a manual environment:

1. The employee requests the key from the cashier. The cashier verifies that the person requesting the key has authority. If the person does not have authority, the cashier denies access.

2. If the employee has the authority, the key log is completed, noting the time and date out and the reason for removal (e.g., table games drop, slot count, etc.). The cashier records the key number, initials the log, gives the key to the authorized person, and the key log is signed by the employee taking responsibility for the key. The person signing the key control log is the person ultimately receiving the key (e.g., drop/count team leader).

3. When restricted keys are signed out, the gaming manager or security employee who authorizes the key check-out by providing the cashier with his/her locked box key also initials the log. The gaming manager or security employee must be present and observe the key check-out and key check-in processes.

4. When the key is returned, the cashier accepts custody and responsibility for the key by recording the time, date in, and initialing the key control log.

5. The cashier immediately places the key back into the key box, locks the box, and removes the access keys.

Accounting personnel review the key logs to ensure only authorized individuals accessed restricted keys, the length of time the key was checked out is appropriate for the function being performed, and that the log was properly completed.

D. TABLE GAMES AND PIT PODIUM KEY CONTROL

The Table Drop Box Release Keys maintained in box 1 may be keyed the same for blackjack, poker, craps and roulette. The Table Drop Box Content Keys maintained in box 2 may be keyed the same for blackjack, poker, craps and roulette. However, the Table Drop Box Release Keys must be keyed differently than the Table Drop Box Content Keys.

The Table Drop Box Release Key used to drop either the drop box or the poker jackpot award drop box can be the same key. The key to access the contents of either the table drop box or the poker jackpot award drop box can be the same key. However, the Table Drop Box Release Key for the drop box and poker jackpot award drop box must be keyed differently than the Table Drop Box Content Key.

The keys to the pit podium and table trays may be, but are not required to be, kept in box 1 or box 2. Access to the pit podium and table tray keys is limited to the pit supervisor, table games manager or gaming manager. If a pit podium bank is utilized, it must be keyed separately. Access to the pit podium bank is limited to the employee responsible for maintaining control over the assigned bank.

The Card Cabinet Key may be the same as the Dice Cabinet Key (primary and secondary storage), as long as adequate inventory controls are established for cards and dice.

Primary storage must be established by the licensee for extra dice. This area shall have two separate locks with one key maintained in box 1 (security) and the second key maintained by the table games manager or pit supervisor. A secondary dice storage area is optional and the two locks may be keyed the same as the two locks on the primary storage area.

E. AUTOMATED KEY TRACKING SYSTEM

An Automated Key Tracking System (AKTS) is defined as a system that controls access to restricted gaming keys through the use of passwords, bio-readers and/or other means whereby the cashier is not the primary key custodian.

Non-restricted keys may be maintained in the same AKTS boxes as the restricted keys; however, access to non-restricted keys should not adversely impact the regulation and control of restricted keys.

System Administration

The system administrator(s) must be a **KEY** licensed employee. This person(s) shall appropriately configure the AKTS to ensure proper authorization and access to restricted keys.

Examples of appropriate configurations include, but are not limited to, such things as providing access to restricted keys only to licensed employees that are appropriate for his/her job duties, setting time parameters as applicable for the length of time for key check out, and setting alarm features to monitor when keys are not returned within the set time parameters.

The AKTS access permissions must be configured in order to distinguish a key licensed employee performing in the capacity of the system administrator from the same individual accessing the system to perform his/her normal job functions (e.g., gaming manager).

Key authorization logs or signature cards must be maintained for an AKTS. The system permissions must accurately reflect the authorization reflected on the log or signature cards. In the setup of the AKTS, no access shall be granted that would allow any one individual sole access to restricted keys identified with a ❷ in the key inventory diagram presented above. Access to the keys must be controlled through appropriate access permissions. This may

include, but is not limited to, the use of passwords that provide access to the keys.

The names of persons whose employment is terminated must be removed from the system in a timely manner to preclude unauthorized access.

Any time the system administrator allows access to the AKTS locked boxes to perform maintenance, cleaning of the keys or any other purposes, the person accessing the keys must be accompanied by security personnel during the entire time of access. This access must be documented with the name of the individual accessing the keys, security personnel name and license number observing the access, the date and time of access and the reason for access.

System Operation

An AKTS must be monitored on a daily basis to ensure an appropriate key control environment. The AKTS must provide reports that detail each event for, or in relation to, key access in order to adequately monitor and review key control.

At the end of each gaming day the gaming manager or security personnel must generate AKTS reports documenting any restricted keys currently not stored in the AKTS. A review of the reports must be performed to ensure all restricted keys accessed throughout the gaming day which are not currently in use (e.g., by the drop or count teams, slot repair, on-duty employees, etc.) have been returned to the AKTS. Evidence of this review is forwarded to accounting after the review is complete. If any keys have not been returned, an investigation must be immediately initiated. The investigation must be documented and include, at a minimum, the key description, last person accessing the key, investigation performed and by whom, and the results of the investigation. This documentation is immediately forwarded to accounting. Accounting reviews the AKTS report and investigative reports for missing keys to determine the appropriateness of the keys checked out and any impact on gaming documents or variances noted on the statistical reports. Accounting's review is evidenced on the AKTS and investigative reports by the signature of the reviewer and date of review.

System Accountability

The AKTS must be monitored and reviewed by personnel who are independent of the AKTS administrator functions. The licensee must maintain a list, which includes the name, license number, and title of each AKTS administrator.

Accounting personnel are responsible for reviewing the following AKTS reports, in addition to reviewing the AKTS report generated at the end of each gaming day referenced above.

Key Transactions
Accounting personnel perform a review of reports generated by the AKTS that document key transactions. This review is performed on a timely basis (as defined in the written accounting plan) to ensure all restricted keys are returned within a reasonable amount of time pursuant to the

completion of the task that created the need for the key(s) removal and to ascertain if any unusual key removals or key returns have occurred. Timely investigations must be performed for any missing restricted keys, improper transactions, and/or unusual occurrences. The investigation results must be documented. This review is evidenced by the reviewer's signature and date of review. The Division is immediately notified if it is suspected there was unauthorized use of a restricted key, if there is suspicion of criminal activity in regard to restricted keys, if a restricted key is missing, if there is a system failure that requires the AKTS to be manually accessed, etc.

System Administrator Transactions
Accounting personnel perform a review of reports generated by the AKTS that document transactions performed by system administrators. This review is performed on a timely basis (as defined in the written accounting plan) to determine whether the transactions completed by the system administrators provide adequate control over access to restricted gaming keys. This review is to determine whether the system administrator's transactions were proper, reasonable, and authorized. Documentation forwarded to accounting, identifies the system administrator accessing the keys, security observing the access, the date and time of access and the reason for access. This information is compared to the system report which details the administrator's access. This review is evidenced by the reviewer's signature and date of review.

Any time persons are added to or removed from the system, accounting personnel compare the key authorization logs or signature cards to the system information to ensure that key access within the system is appropriate.

Any time inappropriate access is discovered or suspected, the surveillance coverage of the AKTS and any related areas must be reviewed. This surveillance coverage must be maintained until such time there is a resolution to the investigation.

AKTS Failure

The licensee must have procedures in place that adequately address key control in the case of an emergency or an AKTS failure. These procedures must ensure access to restricted keys requires the physical involvement of the gaming manager and security personnel. The key control logs used in a manual environment are used in this situation.

An emergency release access function is a function of the AKTS that allows an authorized person, through the use of specific log-in procedures or an Emergency Release Key, to access all keys maintained within the AKTS. If at any time the emergency release access is utilized, the gaming manager and security personnel must be present to access the keys. Each occurrence must be documented and the Division must be notified immediately in writing. The notification must include the date and time of access, the reason for the access, and the name and license number of all personnel involved in the access.

AKTS Installation/Upgrade

Installation and upgrades of an AKTS must be performed by licensed individuals.

F. DUPLICATE KEYS

Duplicate copies of all restricted keys are locked in the duplicate key box located in the vault and are only accessible by the owner/operator and/or gaming manager along with another licensed employee (i.e., no one person can access duplicate keys alone). The Division requires dual locks for the duplicate key box. Additionally, the duplicate keys to the vault must be properly secured in a manner that limits access to authorized personnel only.

If there is no vault, the duplicate keys are stored in a two-keyed locked box, under surveillance, located in a secure area limiting access to authorized personnel only. One key to the duplicate key locked box is maintained in box 1. The second key to the duplicate key locked box is maintained in box 2.

One duplicate key control log sheet must be used per restricted key. Each time a restricted duplicate key is received from the locksmith, or removed and/or replaced, an entry is made on that key's respective duplicate key control log.

Duplicate restricted keys must be inventoried at least twice a year. This may be accomplished in conjunction with the internal compliance officer completing the compliance checklist. The inventory must be documented. This documentation must include at a minimum the names, signatures, license numbers of the individuals performing the inventory count, the date the inventory was performed and the results of the inventory.

Upon receiving duplicate keys from a locksmith, or making duplicate keys in-house, the duplicate key control log must be completed with the following information (see columns labeled A on the duplicate key control log in Forms section):

1. Date key received.
2. Number of keys made.
3. Signature and license number of individual receiving key.
4. Number of keys remaining.

If a duplicate key is removed or checked out to an authorized employee for any reason, the duplicate key control log must be completed with the following information (see columns labeled B on the duplicate key control log in Forms section):

1. Signature and license number of individual issuing key.
2. Signature and license number of individual receiving key.
3. Reason for removal of key.
4. Date of issuance.
5. Time of issuance.

6. Number of keys remaining.

If a duplicate key is permanently removed to replace a broken key, the duplicate key control log must indicate this as the reason for removal of the key, and the columns labeled C on the log will be noted as "N/A".

When the duplicate key is returned, the duplicate key control log must be completed with the following information (see columns labeled C on the duplicate key control log in Forms section). If the duplicate key is transferred to another authorized individual before checking the key in, this must be noted on the log:

1. Signature and license number of individual returning the key.
2. Signature and license number of individual accepting the key.
3. Date of return.
4. Time of return.
5. Number of keys remaining.

G. KEY PROCEDURES FOR NON-OPEN HOURS

If a licensee is not open twenty-four (24) hours a day and utilizes a manual key control environment, the keys to access the restricted two-keyed locked boxes must be secured in a manner that precludes access to the restricted key boxes by any one individual. The licensee must document and have knowledge of where all of the keys to the two-keyed locked boxes are at all times. This could be accomplished through the use of a key log. The key to access the non-restricted key box must also be securely stored in a manner that precludes access by unauthorized individuals.

If a licensee is not open twenty-four (24) hours a day and utilizes an AKTS environment, it must be ensured that all restricted keys which are not in use (e.g., by the drop or count teams, slot repair, etc.) have been returned to the AKTS at the close of the gaming day.

FORMS

Following is a description of the forms discussed in this section. In some cases, sample forms are provided. **It is the licensee's responsibility to ensure that all forms meet ICMP requirements.** See the General section for further clarification.

Bill Validator Release Key Access Key Log

The Bill Validator Release Key Access Key Log is completed each time a key is removed or checked in from the Bill Validator Release Key Box. The log is forwarded to accounting once a page is completed but at least monthly.

Drop Locked Box Access Key Log

The Drop Key Box Access Key Log is completed each time a key from the Drop Key Box is removed and checked in. The log is forwarded to accounting once a page is completed but at least monthly.

Duplicate Key Control Log

The Duplicate Key Control Log is completed each time a restricted duplicate key is received, removed, and/or replaced. The log is forwarded to accounting once a page is completed.

Security Locked Box Access Key Log

The Security Box 1 Access Key Log is completed each time a key in box 1 is checked out or checked in. The log is forwarded to accounting once a page is completed but at least monthly.

Gaming Manager Locked Box Access Key Log

The Gaming Manager Box 2 Access Key Log is completed each time a key in box 2 is checked out or checked in. The log is forwarded to accounting once a page is completed but lat least monthly.

Non-Restricted Keys Locked Box Access Key Log

The Non-restricted Keys Locked Box 3 Access Key Log is completed each time a non-restricted key is checked out or checked in. This log is optional, but recommended. The log is forwarded to accounting once a page is completed but at least monthly.