Mille Lacs Band of Ojibwe Indians

Gaming Regulatory Authority

Detailed Gaming Regulations

DGR-17 Standards for Key Control

Table of Contents

1. General Key Standards

1.1. Segregation of duties shall be maintained between the key custodian and the locksmith if a locksmith is used. Sensitive keys are allowed to be ordered from an outside source.

1.2. The key custodian shall have access to restricted key blanks and cutting codes with an escort by Security Supervisor and above.

1.3. Access to sensitive key blanks and cutting codes shall require the same level of access the key requires (i.e. blank and cutting code for BVB content keys would require three associates from different departments, including at least one member of management.)

1.4. If a key is duplicated the associates who signed out the key that is being cut shall maintain custody of the key until it is entered into inventory and properly secured.

1.5. Sensitive keys shall be maintained in separate key lock boxes.

1.5.1. The Gaming Operation is prohibited from commingling sensitive (dual or triple access) keys with non-gaming keys.

1.6. All sensitive key locks shall be uniquely keyed.

1.7. The Gaming Operation shall develop internal controls for all single access keys that give access to Video Games of Chance (VGCs) and Table Games chip trays, that shall include, but are not limited to, controls for:

1.7.1. Inventory.

1.7.2. Replacement.

1.7.3. Destruction.

1.7.4. Access.

1.8. The Gaming Operation shall develop internal controls for all access control cards that include, but are not limited to, procedures covering:

1.8.1. Issuance.

1.8.2. Replacement.

1.8.3. Deactivation.

1.9. Perpetual individual records shall be maintained for each type of sensitive key, including spares, that include, but are not limited to, the following:

1.9.1. Number of keys in beginning inventory.

1.9.2. Date the key(s) was received.

1.9.3. Signature of associate(s) that received it into inventory with their legible unique identification number. If the inventory is computerized, name and file/identification number may be used.

1.9.4. Key name and description/number.

1.9.5. Date and time of issuance or replacement (month, day, and year).

1.9.6. Key tag/ring number it was placed on.

1.9.7. Signature of associate(s) replacing the key.

1.9.8. Reason for the addition or removal of the key.

1.9.9. Records shall be maintained for each key duplicated, including spares, that indicate the number of keys made or received and destroyed.

1.9.10. The GRA shall be notified by the vendor of shipment of sensitive keys covered by this section at least five (5) days prior to shipment. The notification shall include, but is not limited to, the following:

a. Number of keys being shipped.

b. Types of keys being shipped (key name and description/number).

c. Date keys are being shipped.

d. Expected date of delivery.

e. A GRA representative shall be present when the keys arrive for verification.

1.10. Spare Keys.

1.10.1. All spare sensitive or restricted keys shall be maintained in a manner that provides the same degree of control as is required for the original keys.

1.10.2. An inventory of spare keys shall be maintained in such quantity that there will always be at least one (1) spare key in inventory for each type of sensitive and restricted key.

1.11. All discrepancies shall be investigated and documented with the results forwarded to the GRA upon request.

2. Sensitive Key Cutting Standards

2.1. The gaming operation shall develop a system of internal controls for the cutting of sensitive keys. Such procedures shall include, but are not limited to, the following:

2.1.1. Secured location of blanks and codes.

2.2. Perpetual individual records shall be maintained for each type of sensitive key blank that include, but are not limited to, the following:

2.2.1. Number of key blanks in beginning inventory.

2.2.2. Blank key name and description/number.

2.2.3. Date the blanks were received.

2.2.4. Number of blanks received.

2.2.5. Signature of associate(s) that received the key blanks into inventory with their legible unique identification number. If the inventory is computerized, name and file/identification number may be used.

2.2.6. Date and time the key blanks are removed from inventory for cutting.

2.2.7. Number of blanks removed.

2.2.8. Signature of associate(s) that removed the key blanks from inventory with their legible unique identification number. If the inventory is computerized, name and file/identification number may be used.

2.3. Notice shall be forwarded to the GRA at least 5 days prior to the scheduled cutting, and shall include, but is not limited to, the following:

2.3.1. Keys being cut, key number/name/designation.

2.3.2. What the key(s) are for (drop etc.)

2.3.3. How many keys are being cut.

2.3.4. Where they will be cut.

2.3.5. When, date and time, the keys will be cut.

2.3.6. The five day notification may be waived by request at the discretion of the OGR&C management.

2.4. A log shall be kept of sensitive keys cut showing, but not limited to, the following:

2.4.1. What keys were cut (number/name/designation).

2.4.2. What the key(s) are for (drop, etc.).

2.4.3. How many keys were cut.

2.4.4. Who was present.

2.4.5. Date and time the keys were cut.

2.5. The GRA Board may require an OGR&C employee or designee to be present during the cutting of the sensitive keys.

3. Sensitive and Restricted Key Access Standards

3.1. Access to sensitive or restricted keys shall be limited only to those associates specified in writing.

3.1.1. The list of associates with authorized access must be updated by the Gaming Operation as often as necessary to correctly reflect current associate access.

3.1.2. The access list shall be provided to the GRA upon request.

3.2. Associates having control over a key which accesses a sensitive area must maintain control over their key at all times.

3.3. No one (1) associate or department is allowed to have access to more than one (1) key to a dual or triple access area with the exception of the Count Team during the drop or count.

3.4. Sensitive and restricted keys are prohibited from leaving the Gaming Operation.

4. Sensitive Triple Access Keys/Areas Defined

4.1. Triple access keys requiring three (3) individual signatures of associates from three separate departments, one of whom must be a member of management, with the exception of the count team, to obtain:

4.1.1. Table game and card games drop box contents key.

4.1.2. VGC BVB contents key.

4.2. Areas requiring triple access with the involvement of individuals from three (3) separate departments to access:

4.2.1. Lock boxes containing triple access keys, including spare triple access keys.

5. Sensitive Dual Access Keys/Areas Defined

5.1. Dual access keys requiring two (2) individual signatures to obtain:

5.1.1. Table game and card game drop box release keys.

5.1.2. VGC BVB release keys.

5.1.3. VGC logic door keys.

5.1.4. Progressive controller keys.

5.1.5. Locked dispensing machine key where controlled manual documents are dispensed (i.e. whiz machine).

5.1.6. Front door and control panel keys used to manually access the computerized key security system, if applicable.

5.2. Areas requiring dual access with the involvement of individuals from two (2) separate departments to access:

5.2.1. EPROM storage cabinets.

5.2.2. Card storage area.

5.2.3. Pull tab storage area.

5.2.4. Bingo storage area.

5.2.5. EPROM duplicator storage area.

5.2.6. Key(s) to any secured area where broken drop boxes containing locks are stored.

5.2.7. Storage rack for hot VGC BVBs, with the exception of the Count Team.

a. Cold locked spare VGC BVBs shall be stored in a designated single access area.

5.2.8. Storage rack for table or card games drop boxes, with the exception of the Count Team.

5.2.9. Storage area for sensitive locks with the exception of the Count Team:

a. All VGC locks with the exception of reset locks.

b. Table games drop box locks.

c. Table games release key locks.

5.2.10. Lock boxes containing dual access keys, including spare dual access keys.

5.2.11. Single access keys for a dual access area are considered restricted keys.

6. Restricted Keys Defined

6.1. The Gaming Operation shall define a list of restricted keys. Restricted keys are single access keys relative to gaming operations that are restricted by.

6.1.1. Slots department.

6.1.2. Table Games department.

6.1.3. Finance department.

6.1.4. Bingo department.

6.1.5. Pull Tab department.

6.1.6. Marketing department.

6.1.7. Information Technology department.

6.1.8. Card Games department.

6.1.9. Security department.

7. Inventory of Sensitive and Restricted Keys Standards

7.1. All key box locations that contain sensitive/restricted keys must maintain a current and accurate key inventory and key access list.

7.2. At minimum, the key inventory list shall include, but is not limited to, the following:

7.2.1. Key tag/ring number.

7.2.2. Key(s) name.

7.2.3. Key(s) description which shall match the physical markings on the key(s).

7.3. The Gaming Operation shall develop internal control procedures for the key inventory and key access lists that shall indicate which associates have the authority to make changes to key access lists including deletions and additions.

7.4. A documented inventory shall be conducted by the key box custodian on a daily basis for sensitive and restricted key lock boxes utilized during the day to ensure all keys are accounted for.

7.5. Personnel independent of the Security department and departmental key owner shall conduct an inventory of all sensitive and restricted keys, including spare keys, on at least an annual basis and forward the results to the GRA upon request.

7.5.1. All discrepancies will be investigated, with the results of the investigation documented and forwarded to the GRA upon request.

8. Broken, Lost, or Missing Key Standards

8.1. Any broken, bent, or otherwise damaged sensitive keys shall be handled following the requirements for an intact, functional key (i.e. if dual/triple access, handled as an intact dual/triple access key) until destroyed.

8.2. The Gaming Operation shall develop a system of internal controls related to the treatment of unaccounted for, stolen, lost, or missing sensitive and restricted keys.

8.3. If a sensitive key or restricted key is inadvertently taken off premises:

8.3.1. The GRA shall be notified within twenty-four (24) hours.

8.3.2. A security report shall be done and forwarded to the GRA.

8.3.3. The key control log shall indicate the key(s) were taken off premises.

8.4. In the event a sensitive or restricted key or lock is lost, misplaced, removed from premises, or missing for any length of time the GRA reserves the right to mandate replacement of said locks or keys.

8.5. Broken keys, unidentified/obsolete keys, or keys for locks that have been changed, shall be destroyed and discarded.

8.6. The Gaming Operation shall develop internal control procedures that include key destruction procedures for:

8.6.1. Broken keys.

8.6.2. Unidentified/obsolete keys.

8.7. The Gaming Operation shall develop internal control procedures for broken sensitive or restricted keys that shall include, but not be limited to:

8.7.1. Which associate(s) shall receive and replace the broken key.

8.7.2. Disposition of the broken key.

8.7.3. Notification to the GRA.

9. Sensitive and Restricted Key Control Log Standards

9.1. All key lock boxes that contain sensitive and restricted keys are controlled through restricted access and key control logs, which are completed (ditto marks, etc. are not allowed) every time a key is checked out and in.

9.2. Before a key can be issued, the associate issuing the key must verify that the associate requesting the key has authority to access the key.

9.3. The key control log shall include, but is not limited to, the following:

9.3.1. Date of issuance (month, day, and year).

9.3.2. Time of issuance.

9.3.3. Signature of associate(s) receiving the key(s). The associate(s) signing the key control log must be the individual(s) ultimately receiving the key.

9.3.4. Key tag/ring number(s).

9.3.5. Reason for removal of sensitive key(s) (i.e., perform VGC drop, etc.).

9.3.6. Signature of associate issuing the key(s).

9.3.7. Date of return (month, day, and year).

9.3.8. Time of return.

9.3.9. Signature of associate(s) returning the key(s). All keys must be returned by the same associate(s) who signed them out.

9.3.10. Signature of associate accepting return of the key(s).

9.4. An associate is prohibited from transferring possession of an issued key(s) to another associate without proper documentation in the key control log. The only exceptions to transference of the keys are:

9.4.1. In case of an emergency the key(s) can be returned by the associate's supervisor. The associate the key is transferred to must be authorized to obtain the key.

9.4.2. During the count, count room keys may be transferred between associates performing the count provided the keys remain in the count room until the end of the count and the individuals who initially signed the key(s) out is to return the keys.

9.5. An associate is prohibited from maintaining possession of sensitive keys during breaks. Key(s) must be signed back in at the key box location, with documentation in the key control log.

9.6. Physical copies of key control logs must be completed in ink.

9.7. Electronic versions of the key control log shall record the associate's identity.

10. Table Games and Card Games Key Control Standards

10.1. Table/card game drop box and progressive drop box.

10.1.1. The table/card games release key must be keyed separately from the key to access the table/card games drop box contents.

10.1.2. The key to access the contents of the table/card games drop box and progressive drop box shall be keyed differently.

10.1.3. The table/card game drop box release keys (key which releases the drop box from the table) shall be maintained by a department independent of the Table/Card Games department.

10.1.4. During the drop process, the associates authorized to remove drop boxes from the tables are the only associates authorized to have access to the drop box release

keys, with the exception of the count team during the count, in order to reset the drop boxes.

10.1.5. Associates 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 and release keys.

10.2. Table games and card games drop box access:

10.2.1. 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.

10.2.2. Unauthorized access to empty table/card game drop boxes shall not occur from the time the boxes leave the storage racks until they are place on the tables.

10.3. Storage Rack Keys

10.3.1. An associate independent of the Table Games department shall be required to accompany the table/card game drop box storage rack keys and observe each time a table/card game drop box is removed from or placed in the storage rack.

10.3.2. Associates authorized to obtain table/card game drop box storage rack keys shall be precluded from having simultaneous access to table/card game drop box contents keys with the exception of the Count Team.

11. VGC Key Control Standards

11.1. The following keys shall be keyed separately:

11.1.1. Soft count room key.

11.1.2. VGC door key.

11.1.3. BVB contents key.

11.1.4. Progressive controller key.

11.1.5. Logic door key.

11.1.6. BVB door key.

11.2. The VGC belly door key may be keyed the same as the VGC door key.

11.3. The BVB release keys shall be maintained by a department independent of the VGC department.

11.4. Only the associate(s) authorized to remove the BVB from the gaming machines shall be allowed access to the release keys during the drop process.

11.5. Associates authorized to remove the BVB shall be precluded from having simultaneous access to the BVB contents keys and release keys.

11.6. An associate independent of the VGC department shall be required to accompany the BVB storage rack keys and observe each time canisters are removed from or placed in storage racks.

11.7. An associate authorized to obtain BVB storage rack keys shall be precluded from having simultaneous access to bill acceptor canister contents keys with the exception of the Count Team.

11.8. The physical custody of the keys needed for accessing stored, full BVB shall require involvement of associates from two (2) separate departments, with the exception of the Count Team.

11.9. Only the Count Team members shall be allowed access to BVB contents keys during the count process.

12. Cage/Vault/Kiosk Key Control Standards

12.1. The following keys may be kept in a single lock box in the Main Bank:

12.1.1. Kiosk and ATM main door keys.

12.1.2. Kiosk-BVB stacker release key.

12.1.3. Currency dispenser cassette release key.

12.1.4. Currency dispenser cassette content key.

12.1.5. Vault keys.

12.1.6. Cashier keys.

12.1.7. Personal product vending machine keys.

12.1.8. Kiosk BVB contents key.

12.2. The following keys shall require a Cage and Security associate escort when keys leave the Main Cage:

12.2.1. Kiosk BVB stacker release key.

12.2.2. Currency dispenser cassette release key.

12.3. Kiosk BVB and currency dispenser cassette contents keys are prohibited from leaving the cage.

13. Drop and Count Keys Additional Standards

13.1. For all triple access keys required by the Drop and Count team, documentation must be completed to evidence that three (3) Drop and Count team members are present when the keys are issued and returned for the count of the gaming revenues. The drop team member(s) who signed or accessed the keys must accompany these keys at all times until the time of their return.

13.2. Access to a triple access key at other than scheduled drop and count times requires three (3) key associates from separate departments with segregated functions, one (1) of which must be a member of management, and must be present at the time the key(s) are issued. All three (3) persons are required to accompany the keys at all times until the time of their return. This access includes, but is not limited to, emergency drops.

14. Computerized Key Control Standards

14.1. A computerized key security system shall provide the same degree of control as indicated in the aforementioned key control standards, with the exception of system administrator controls.

14.2. Personnel independent of the gaming department shall assign and control user access to keys in the computerized key security system (i.e., system administrator) to ensure that slots, table games, card games, and kiosk keys are restricted to authorized associates.

14.3. Access to the manual override key, used to access the box containing drop and count release and content keys, requires the physical involvement of three (3) persons from separate departments, including management. The custody of the manual override key shall require the presence of the three (3) associates from the time of their issuance until the time of their return.

14.3.1. The date, time, and reason for access, shall be documented with the signatures of all participating associates signing out/in the manual override key.

14.4. Routine physical maintenance that requires accessing the manual override key and does not involve the accessing of any sensitive keys shall require the presence of two (2) persons from separate departments. The custody of the issued manual override key if the box does not contain sensitive keys shall require the presence of two (2) persons from separate departments from the time of their issuance until the time of their return.

14.5. The following shall be documented when the box is accessed using the manual override key(s):

14.5.1. Date.

14.5.2. Time.

14.5.3. Reason for access.

14.5.4. Signatures of all participating employees signing out/in the manual override key(s).

15. Lock Standards

15.1. All sensitive access locks (or interchangeable cores is using interchangeable core locks) shall be received and maintained in a secure manner requiring dual access to obtain.

15.2. VGC door locks and Table Games chip tray locks shall be received and maintained in a secure manner requiring dual access to obtain and follow all inventory control procedures outlined in this DGR.

15.3. Perpetual individual records shall be maintained for each type of sensitive access lock that indicates the following:

15.3.1. Number of locks in beginning inventory.

15.3.2. Date the locks were received.

15.3.3. Signature of associate(s) that received it into inventory.

15.3.4. Lock name and description/number.

15.3.5. Date of replacement (month, day, and year).

15.3.6. Time of issuance.

15.3.7. Signature of associate(s) replacing the lock.

15.3.8. Reason for addition or removal of locks.

15.3.9. Disposition of broken locks.

15.4. Inventory of sensitive access locks shall be maintained in such a manner that there will always be at least one (1) lock in inventory for each type of lock.

15.5. Inventory will be conducted at least quarterly, with the results forwarded to the GRA upon request.

16. Lock Destruction Standards

16.1. The Gaming Operation shall develop a system of internal controls for the destruction of broken and/or obsolete locks. The controls shall include, but are not limited to, the following:

16.1.1. How and where the locks will be secured until destruction.

16.1.2. Notice shall be forward to the GRA at least five days prior to the scheduled destruction.

16.1.3. The notice must include the following:

a. Description of method of destruction or disposal including:

i. Name of the associate responsible for destruction or disposal.

ii. Date, place, and time of proposed destruction or disposal.

iii. Proposed method for destruction or disposal.

16.1.4. The locks scheduled for destruction shall be logged with the log showing, but not restricted to:

a. What locks are being destroyed (code, number, etc.).

b. How many of each type of lock is being destroyed.

c. How the locks are being destroyed.

d. Associates involved in the destruction.

e. Date and time of the destruction.

16.2. The GRA Board may require an OGR&C employee or designee to be present at the destruction of the locks. The Board may require the destruction of the locks to be video recorded.

16.3. Any broken, or otherwise damaged sensitive locks shall be handled following the requirements for an intact, functional lock (i.e. if dual access, handled as an intact dual access lock, lock for a dual access area, etc.) until destroyed.

17. Key Controls Independent Review

17.1. A department independent of the key custodian shall perform the following procedures for computerized key security systems controlling access to sensitive keys.

17.1.1. Quarterly, review the report generated by the computerized key security system indicating the transactions performed by the individual(s) that adds, deletes, and changes users' access within the system (i.e. key custodian), and determines the following:

a. Whether the transactions completed by the key custodian provide adequate control over access to the sensitive keys.

b. Whether any sensitive key(s) removed or returned to the key cabinet by the key custodian was properly authorized.

17.1.2. For one day each quarter, review the report generated by the computerized key security system indicating all transactions performed to determine whether any unusual sensitive key removals or returns occurred.

17.1.3. Review at least 20% of users that are assigned access to the sensitive keys to determine that their access to the assigned keys is appropriate relative to their job position at least quarterly.

17.1.4. Perform an inventory of all sensitive keys and reconcile to records of keys made, issued, and destroyed at least quarterly.

History

Approved by Band Assembly on July 28, 2005.

Changes approved by the GRA Board on June 25, 2008. Effective Date: June 25, 2008.
Changes approved by the GRA Board on July 6, 2011. Effective Date: July 6, 2011.
Changes approved by the GRA Board on April 28, 2016. Effective Date: April 28, 2016.
Changes approved by the GRA Board on May 8, 2025. Effective Date: October 31, 2025.
Changes approved by the GRA Board on September 25, 2025. Effective Date: January 01, 2026.

Prior versions of this Detailed Gaming Regulation are available upon request from the Gaming Regulatory Authority.

Each Gaming Operation shall come in compliance with changes no later than January 01, 2026.