SECTION 6

GAMING SYSTEMS

A. GENERAL

Licensees may use a gaming system to capture required slot machine meters, drop and count information, and/or to generate gaming forms, documents, and required statistical reports as they relate to the reporting of AGP. A licensee must successfully test the gaming system and modules of the system (such as TITO, wireless handheld validation units, Electronic Promotional Credit System (EPCS), kiosks, pit, cage, and third party systems) before it can rely upon the system, or upon any information generated by the system, as it relates to the reporting of AGP. The licensee must test its system following the requirements outlined in Gaming Systems Testing section of the ICMP. The licensee cannot rely upon the system until these requirements have been met.

Generally, only licensed employees may have access to gaming systems. Unlicensed employees whose functions include viewing player points and redeeming applicable points for restaurant or hotel comps through a third party system (i.e., point of sale system), may have access for those functions only. Unlicensed employees cannot have the ability to log into the gaming system.

All gaming systems must have audit reports that provide a chronological list of events, and audit trails that document adjustments or changes to the gaming system. The system generated reports must include, at a minimum, the date, time, user or operator, and a description of the event. These reports are used to support adjustments and overrides and to aid in investigations for exceptions, meter errors and variances. Any necessary adjustment to and/or reconciliation of system reports must reflect the meter data for such machines. The licensee's accounting plan must reflect the appropriate audit and accounting procedures for this requirement.

Each licensee must maintain required documentation for three years. This data must include, at a minimum, revenue (actual) data, meter data, and other pertinent data used to create, investigate, and explain all supporting and required documentation. All documentation must be made available to the Division upon request and in a reasonable timeframe as determined by the Division.

The licensee must notify the Division if a system that reports or affects AGP is down for a total of 12 hours in any 30-day period. For example, if the system is down for one hour 12 times within a 30-day period, the licensee must notify the Division. Notification must be submitted via email to the Division at: DOR_CCBHCasinos@state.co.us or DOR_CrippleCreekCasinos@state.co.us, as appropriate.

Additional information, in the form of technical documents, may be found at the Division's website.

Non-Communicating Machines

Licensees must manually read and record all required soft meters, at each drop, for any machines that are not set up to communicate, are not able to communicate properly, or have stopped communicating properly with the gaming system. Anytime the gaming system fails to communicate accurate meters and information the licensee must revert to the manual capture and recording of soft meters, and use the soft meters in the generation of the required statistical reports. On a monthly basis, licensees must prepare and maintain a list of slot machines not connected to the gaming system along with the reason the slot machine is not connected. The list must include all slot machines connected to the gaming system that do not report all of the required meters.

Ticket In/Ticket Out (TITO)

A TITO enabled device can always generate on-line tickets. In addition, depending on the gaming system, it may also generate delayed or off-line tickets when the gaming system is not communicating properly with the ticketing functionality. See CLGR 30-1272(3) for more information regarding these tickets. Licensees must notify the Division, via email, when they are going to enable off-line or delayed tickets.

Licensees are required to complete the TITO device, kiosk, and cage/wireless handheld validation unit checklists anytime a slot machine, kiosk, or cage/wireless validation unit is added to the gaming floor or cage, moved from one location to another on the gaming floor, whenever slot machine options or the asset number are reconfigured in the gaming system, and when slot machines are TITO-enabled. Also, licensees must complete TITO device checklists any time slot machines are converted from one game or denomination to another game or denomination. These machines, kiosks and validation units must pass the checklist requirements prior to being placed into service. A checklist must be completed for every machine, kiosk and unit. Licensees must maintain these forms for Division review.

All slot coupons must be generated using the licensee's approved gaming system. The licensee must follow the configuration guidelines outlined in the manufacturer's specifications to ensure all coupons are cashable. See TITO section in the ICMP for guidelines regarding slot coupons.

Overrides are defined as changes to system information made at the time of the event. Licensees must have appropriate access rights in place to prohibit any changes to system information for tickets or coupons. Any licensed employee granted access to produce slot coupons cannot be granted access to redeem them.

The status of a ticket or coupon that has been redeemed, expired or voided must not be changed. If an active ticket or coupon cannot be properly processed under normal circumstances, a supervisor must provide system and/or written authorization for the completion of the transaction.

TITO tickets must expire 120 days from issuance. Slot coupons must also have an expiration date; however, there are not a specific number of days in which they must expire.

Cage and Pit Systems

In the event the cage and/or pit systems go down, the licensee must revert back to the manual process.

Electronic Promotional Credit Systems (EPCS)

EPCS means a system of components, hardware, software and communication technology that securely transmits credits to and from a slot machine in the form of electronic promotional credits. EPCS are any systems that maintain electronic promotional credits. EPCS allow patrons to play slot machines using a player card with a magnetic strip to download credits to a slot machine. EPCS gaming transactions at the slot machine are entirely electronic.

EPCS must be controlled in a manner that precludes any one individual from fraudulently accessing promotional events and/or electronic credits associated with individual patron's membership information.

B. DOCUMENTATION REQUIREMENTS

In order for the Division to rely on any documentation it will require proof that it was reviewed, completed, checked and/or verified.

General Requirements

Requirements for all documentation include legibility, signatory, retention and accessibility. All documents must be clearly legible, the font must not be broken up or patchy, and lines cannot overlap. Information such as page numbers, dates, headers or footers cannot be illegible or missing. If there is a handwritten note on the original document it must be legible on all copies. When signing or initialing a document the signature/initials must be clear and must not block any information contained in the document. The signature/initials must include legible license number and date. Any time the term signature or initials is used for any document, this always means the document requires a signature or initials, date and legible gaming license number of the individual who completed the document and/or the reviewer who ensured the document was completed and a signature/initial was indicated.

Checklists

The Division will provide checklists to the licensee's ICO along with a completion deadline. Completed checklists must be submitted to the Division by the deadline. These checklists are used by the Division as a tool to help ensure Division requirements are completed on a consistent

basis. They must be filled out completely and the responses must be clearly marked. Responses must be circled in such a way to clearly indicate the intended response (Yes or No).

C. PHYSICAL SECURITY

Keeping the computer room safe from unauthorized individuals is necessary to ensure that computer systems remain uncompromised. Safeguards that prevent employees from accessing the computer room without proper authority and proving their identity must be in place. Logging the timeline and reason the individual entered the computer room is necessary in resolving any issues that may arise.

The computer room must be secured in a manner that only allows authorized access. Methods such as cipher locks, biometrics, badge scanners, or door keys must be used to secure the computer room. The licensee must maintain a list of authorize personnel who are exempt from completing the access log when entering the IT room. Unauthorized individuals who enter the IT room must complete a log that includes date, time of arrival and departure, employee name, and reason for entry. The log must be reviewed, at least monthly, by the IT manager or ICO if the casino has only one IT staff member.

Protecting the computer room from power fluctuations, heat, and other environmental risks helps ensure the availability of the system. Surge suppressors, UPS, battery backups, or line conditioners must be in place to prevent a system failure due to electrical outages, spikes and surges. The gaming system must be able to remain in operation for a minimum of one hour or until the IT staff can bring the gaming system down in a controlled manner.

Network equipment located throughout the casino must be secured in a manner that only allows authorized access. Used or unused network connections must not allow unauthorized access to the casino's network. This may be accomplished with a locking cover, unplugging the cable from the switch, making the port inaccessible or logically disabling the port. An inventory of all ports must be maintained.

D. LOGICAL SECURITY

Logical security is comprised of three areas: account management, password management and security settings. Account management consists of networks and system accounts. Password management focuses on password requirements for the various types of passwords. Security settings are default settings found in hardware and software.

Account management includes user accounts, or accounts that are typically used for business functions. Devices or accounts that timeout must be re-authenticated. Accounts that are members of default groups that are not being used must be removed. If an account is not being used it must be removed or disabled. The licensee must have a formal process that ensures only accounts assigned to individuals are allowed unless otherwise specified. The process must be documented and approved by casino management.

Password management is based upon whether or not the account has elevated privileges. Elevated privileges are typically defined as a set of permissions that are greater than a normal business account. An account with these privileges can usually access the system in such a way that if misused, could harm the system. The IT department must have a documented account and password management policy that includes procedures to handle these accounts. System accounts with elevated privileges must have their passwords changed annually or when a person with knowledge of the passwords is no longer employed by the licensee. Complex passwords must be used unless unavailable due to limitation within the software. System accounts must not be used by a licensee in lieu of his/her assigned user account.

Default settings must be set to a level that ensures data integrity, accuracy, availability and security. Default settings include hardware configuration, accounts and passwords, or a set of enabled functions that might not be needed by the licensee. These settings must be reviewed and configured to best meet the casino's business needs.

E. SEGREGATION OF DUTIES

Understanding the permissions assigned to each gaming system role and account is vital to maintaining segregation of duties. For example, a casino employee should not have a level of access to the gaming system that enables him/her to perform transactions on regulated data across an entire process.

The casino must maintain the segregation of duties matrix (which can be found on the Division's website) and update it annually at a minimum. The casino must provide documentation that clearly demonstrates that all permissions within a gaming system are identified and explained. All employee access must be approved by management before they are given access. All manually documented permissions must be reviewed and compared to a system generated permissions report. An annual review of the permissions and user accounts within the permissions must be completed.

The casino must also understand what access is given at a user account level and ensure that a user account does not have a level of access that may create a segregation of duties violation. Typically, this happens as a person changes jobs and (s)he is added to new role without the old role being removed. It can also happen if a person has two jobs within the casino. The licensee must explain and document employee name, assigned positions, why a user account is given the permissions it is assigned and the name and title of the approver. The explanation must also include an analysis of segregation of duties and identify any violations.

The casino must maintain documentation that includes full name, title, Colorado gaming license number (if applicable), and reporting structure for all IT employees, corporate IT, out of state IT personnel, and IT contractors who have access to the gaming system. Employees with IT functions are generally given elevated privileges within the system. Tight controls must be in place for these accounts. The IT personnel must not be able to initiate, perform, override or review any transaction that occurs as a result of gaming activity.

Additionally, employees must follow the minimum standards to ensure that appropriate controls segregate revenue reporting functions (e.g., accounting), from revenue generating functions (e.g., count team). Users involved with the collection of revenue are prohibited from having access to any revenue or reporting capabilities in the system. This is not intended to prohibit count team members from printing the required ticketing report for the purposes of ticket counts. Also, the IT staff must not be able to initiate, perform or override any transaction that occurs as a result of gaming activity with the exception of incidents that are documented in the RAMP log and approved by management for fixes and maintenance (i.e., jackpot transaction assigned to IT manager to fix a problem). The ICO or IT Management must review changes made to IT Staff permissions relating to fixes and maintenance and compare the changes to the RAMP log every month. The review is performed to ensure that all permission changes are logged. The review should also ensure that all permissions that no longer needed are removed. Please refer to the RAMP Log section for additional information.

F. NETWORK TOPOLOGY

Networks are the foundation for a secure computing environment. The correct design is critical to implement an in-depth strategy that minimizes risk. A properly designed network can create an environment of accuracy, security, availability, and data integrity. Licensees are responsible for the security of the casino's network.

Licensees must document their entire network, including the gaming system, using a diagram and indicate how the network is secure. The licensees must indicate if the network operates on a virtual network. Licensees must indicate if their gaming network is segmented from the rest of the network.

The licensee must document the gaming system versions including modules, collection units, third party programs and Slot Machine Interface Board (SMIB) versions. The versions must be verified against the installation/upgrade notification forms that were sent to the Division prior to the installation or upgrade. Any discrepancies must be reported to the Division via email address stated in the General subsection of this section. This full verification of all gaming system hardware/software must be documented and performed at the completion of each installation/upgrade or annually, whichever is sooner.

G. RAMP (**R**emote **A**ccess**, M**aintenance and **P**roblem**) LOG**

Licensees must maintain a gaming system log (RAMP log) that documents, at a minimum, system upgrades, modifications, maintenance, problems, and all remote access where the connection is outside the licensee's wide area network (WAN). Any event indicated on a gaming system log that requires action must be recorded in the RAMP log.

The system log can be an electronic searchable document (e.g., spreadsheet) or a hard copy that is filled in manually.

The RAMP log must include, at a minimum:

1. The date and time maintenance was performed or date and time the problem was identified.

2. The area of the casino (e.g., accounting, slots, cage, IT) the problem impacts.

3. A detailed description of maintenance performed or of problem identified. For example, maintenance would include rebooting gaming system servers, database maintenance, installing updates, etc.

4. The full name, license number and position of person who identified the problem (N/A if maintenance). This can be the individual who updated the log and forwarded the information to the IT department or it could be an individual from the IT department who updated the log based on the issue (s)he discovered or based on information provided by a casino employee.

5. The full name, license number and position of person who either performed maintenance, problem investigation and follow-up, or remotely accessed the system. If the system was remotely accessed, the log must indicate that remote access occurred. Any individual who remotely access the gaming system must have a valid Colorado gaming license.

6. The system manufacturer's case number if the manufacturer was contacted (N/A if not contacted).

7. The date and detailed explanation of how the problem was resolved (N/A if maintenance) or date and type of modification made to the system (if applicable).

The log must be maintained up to date with every area filled in.

It is acceptable to have a legend on the bottom or top of each page to explain entries such as names or performing system maintenance. If a legend is not used, then all of the required information must be completed in each area of the log.

The following are a few examples:

Example for log item #1 above – Maintenance is performed every month to archive redeemed tickets. The person entering information into the log would enter the date in the field for 1 above and then write/type Archive in area 3 above. The legend would tie back to the word Archive by stating "Archive" = Archiving redeemed tickets in the gaming system to prevent duplicate validation numbers due the SMIB's buffer getting full.

Example for log items 3 & 4 above - Mortimer Sneed is usually the individual that identifies the problems and/or performs maintenance on several of the various entries. The log for 4 above

would have Mortimer in 3 above. The legend would tie back to the word Mortimer by stating "Mortimer" = Mortimer Sneed, IT Director, license number xxx.

The log must be reviewed by the IT Manager/Director on a regular basis to ensure the log is being prepared correctly and to identify on-going issues.

H. DATABASE SECURITY

It is the responsibility of the licensee to maintain data integrity of all gaming system. Direct access to the database that contains revenue data represents a risk to the accuracy, security, availability and integrity of the gaming environment.

Software upgrades and updates as outlined in the ICMP must be submitted to the Division via email on the required Installation/Upgrade/Test Notification form located on the Division's website.

Licensees must maintain a secure control environment of their information technology network. This includes, but is not limited to, logical and physical controls of software, hardware, tapes, backups, disk, etc., application controls as well as any additional controls deemed necessary to protect the integrity of all networks, applications, databases and data.

Any changes to data within the gaming system database must be performed through the gaming system vendor's application or gateway. Read only access to the gaming system database is permitted for business purposes. The only time user and administrator accounts with elevated privileges, may access the database without prior notification to and acknowledgment from the Division is for IT functions such as maintenance, repair, or upgrades. The licensee must ensure that the RAMP log is updated for all maintenance, repairs, or upgrades. If the casino is under a maintenance agreement, the vendor must still be contacted in accordance with the maintenance agreement prior to initiating the maintenance, repair or upgrade.

Accounts with elevated permissions in the database environment must be unique for each user and must not be shared among the casino employees. Passwords for system accounts that allow software packages access to the database and have the ability to modify the database or objects within the database must never be shared. The accounts must only be used by the system and never by a casino employee in lieu of his/her personal account. System accounts must always have their default password changed at install or system upgrade.

Third party software is defined as any software that impacts the gaming system that did not come from the gaming system vendor. This can mean purchased software from an outside source such as a company or contractor, or software developed in-house. Third party software programs must use the gaming system's gateway. Licensees using third party software that does not go through a gateway must request a variance and receive approval from the Division prior to use. This must be accomplished by submitting a variance request to the Division and receiving the Division's

approval. System accounts used by the third party software must be documented and the accounts must not be used by individuals in place of their assigned account.

System Disruption

When an unanticipated incident occurs that causes a significant disruption in the collection, accuracy, integrity, or availability of the gaming system, the licensee must immediately contact the appropriate IT resources, such as local IT staff, IT contractor or gaming system vendor, to begin the troubleshooting process. The licensee must add an entry to the RAMP log, and inform the Division as soon as practically possible via e-mail. The e-mail must include, but is not limited to, the following:

- a detailed description of the problem,
- why they think the problem occurred,
- if the manufacturer was contacted to assist in or to resolve the issue and if not, why not,
- the time it was identified,
- a brief statement about where the casino/vendor is in the troubleshooting process, and
- the manufacturer's case number (if applicable).

The Division does not require that the licensee wait for an approval from the Division before proceeding with the solution.

After the problem has been resolved, a follow up email must be sent to the Division within 48 hours of resuming normal operations. The email must include a description of and resolution to the problem.

I. WIRELESS

The Division recognizes secure and private wireless local area networks (WLAN) as an approved technology. ~~for limited applications. Original gaming data, other than wireless TITO ticket validation, cannot travel across a wireless segment. Casinos~~ Licensees are ~~not~~ authorized to utilize a WLAN for activity that can, or has the potential to, impact gaming transactions, gaming system transactions or the calculation and/or reporting of adjusted gross proceeds (AGP) ~~unless specifically allowed in the ICMP~~. For the purposes of this document a WLAN is defined as all components connecting to a system or network using wireless technology. This includes but is not limited to devices using cellular networks, near-field communication (NFC), Bluetooth, radio-frequency identification (RFID), and Institute of Electrical and Electronics Engineers (IEEE) 802.11x standards.

~~Casinos with the same ownership or casinos with an unattached business office may establish a wireless bridge to transmit a copy of gaming data. The casino must follow all rules for segregation of data between same ownership casinos, for example ticketing data. Subsequent to the data being written to the gaming system's database, a copy of the gaming data is permitted across the WLAN. This includes results from queries, reports, or copies of the database itself.~~ It

is the ~~l~~Licensee's responsibility to ensure the security of all data traveling in the WLAN. ~~The licensee must submit the notification form prior to installing a WLAN.~~ An Intent to Install form must be submitted and approved prior to installing a new WLAN or updating WLAN systems/components. All WLAN system ~~components~~devices must be physically secured. The Licensee must implement processes and procedures that ensure their endpoint devices with which patrons may interact are secured, this may include but is not limited to mobile devices such as robots, tablets, laptops, mobile kiosks, player cards, or gaming devices such as chips, dice, or other devices offering kiosk functionality. Licensee's endpoint devices must be stored in a way that limits transmission when not in use. For example, storing tablets, phones, chips or dice in a RFID blocking cabinet. All WLANs must be segmented from the rest of the network, at a minimum, by a firewall that meets current ~~computer~~ industry security standards~~, such as stateful packet inspection, authentication and encryption. The version of encryption used must be the most current version that the equipment is capable of and has not been compromised~~.

Authentication requirements for WLAN devices include using strong passwords, changing default passwords, multi factor authentication (MFA) and minimizing the number of people who have access to accounts with elevated privileges. Strong password management requirements must be implemented for accounts (user and device) on the WLAN. ~~Accounts with elevated privileges must have their passwords changed at intervals not to exceed 90 days by the IT Department. The changing of passwords, not the actual password, must be documented and reviewed by the ICO. A system generated report that indicates when the password has been changed will suffice.~~

Due to cryptographic strength being crucial to a secure a WLAN, ~~encryption versions must be current with industry standards and~~ pre-shared keys must be managed, documented and changed whenever a person with knowledge of the keys has left, or a security incident occurred~~, or at least annually~~. The version of encryption used must be the most current version that the equipment is capable of and has not been compromised. If a security incident occurred on the WLAN, the Division must be notified as soon as practically possible and again within 48 business hours after the incident has been resolved.

~~All~~ WLAN infrastructure components such as, but not limited to, access points, wireless management systems, firewalls, security appliances, ~~and~~ Intrusion ~~Detection~~ Prevention Systems (I~~D~~PS) and Intrusion Detection Systems (IDS) must be physically secure. Access points must be mounted using tamper proof mounting hardware in an area that does not allow for easy physical access or secured in a locked cabinet or room. ~~The o~~Other WLAN infrastructure components must be in a secured room that is locked at all times and only allows authorized access. See section C. Physical Security for more information.

~~All d~~Default settings must be changed before implementation. Changes to the default settings must be documented.

Parameters that should be changed include but are not limited to:

- Default pre-shared key

- SSID
- SNMP community strings (when possible)
- Encryption Keys
- Passwords
- ~~Disable any unnecessary ports, protocols, broadcasts or other options~~
- ~~Change clock settings to synchronize with the casino's time system~~
- ~~Set a session timeout (to prevent hijacking of abandoned authentication sessions)~~
    - ~~Disable WPS~~

~~All default passwords must be changed before implementation, such as the default password for the administrator account. Default configuration parameters must also be changed, such as the default Service Set Identifier (SSID)~~ Changes to the default settings must be documented and reviewed by ~~the ICO~~a person not involved or responsible for the configurations. The review must be documented and validated with signatures.

The WLAN must be documented in ~~a~~the Licensee's network diagram. The diagram must include all components of the WLAN as well as the path to the wired network. The diagram must include devices using endpoint wireless~~data moving in the WLAN must be documented within the diagram. The diagram must include near field~~ communication protocols (like Bluetooth, NFC, RFID) except for input devices on endpoint workstations such as wireless keyboards and/or mice. The network diagram must be updated and submitted to the Division when there is a change to the ~~network~~WLAN.

Wireless handheld validation devices/systems must be tested and approved in accordance with the Section 7 ICMP Gaming System Testing ~~section of the ICMPs~~. In addition, process requirements related to handheld wireless devices can be found in the TITO section of the ICMP.

Endpoint devices, including but not limited to tablets, laptops, workstations, phones, gaming specific devices such as kiosks, tables (readers embedded in tables), chips, player cards and dice, or any other device connected to the wireless network must use encryption, authenticate when possible, and be updated at the product manufacturer's recommended intervals to mitigate vulnerabilities.

An inventory of endpoint wireless devices must be maintained, and when possible, compared to a system generated report.

Patrons must be informed that they are being tracked if they have any wireless/RFI device or software installed that is owned by the Licensee in their possession.

The Licensee must have processes and procedures in place to manage/remediate missing wireless devices. The Licensee must also have a response plan in place to monitor, disable, mitigate and respond to unauthorized devices accessing the WLAN.

J. BACKUP AND RECOVERY

A successful backup and recovery strategy allows a business to recover data when a data loss event occurs. Events can include hardware failure, intentional deletion, natural disasters, accidental loss or data corruption. The strategy should include contingency plans, media management, backup schedule and, verification and testing of the backup system.

The licensee must create a written backup and recovery plan. The plan must include, at a minimum, the following:

1. How often backup will be performed, type of backup that will be performed each time (full, deferential, incremental); the type and location of media storage.

2. What information will be saved in order to comply with CLGR 30-1607.,

3. What the licensee will do if the backup interferes with business operations.

4. How the licensee will ensure that saving gaming data while a system is writing to the files does not compromise the integrity of the backup

5. If two backups in a row or four non-contiguous backups in any calendar month are missed or non-usable, an IT staff member or person responsible for the IT function in the casino must take immediate corrective action. The problem and corrective action must be documented on the RAMP Log.

6. Backup and recovery testing must be performed at least twice a year. The results of a completed restore must be detailed with supporting documentation. The restore must include gaming data and be usable by the gaming system. The testing must continue until a successful restore has been completed. The summary of the results of every restore must be recorded on the RAMP Log.

7. How the casino will physically manage the media to ensure that no gaming data is lost, including the tracking of the media so data does not leave the business in an unauthorized fashion.

When decommissioning an old backup system, the licensee must ensure it meets the three year retention requirements as stated in CLGR 30-1607. If the licensee is using media from the old system to meet the requirement, the media must be usable and the data recoverable within the requested timeframe of the Division.

K. SLOT MACHINE MANAGEMENT

Slot machine testing must be performed on slot machines when they are added to the gaming floor or when communication has been broken and the machine must be reconfigured to establish

communication. This includes new machines, machines moved to the gaming floor from storage, machine conversions and any other situation that would qualify under slot machine management. The licensee must have written procedures in place that list the type of slot floor additions and changes that would result in the testing of the slot machines, the name of the spreadsheet or worksheet that will be used to support the required information for option 1 or option 2 listed below.

There are two options for slot machine testing after the licensee has received permanent approval to rely upon its gaming system:

Option 1
The meter reader(s) must record the beginning and ending soft meter readings for coin in, coin out (for non-ticketing machines), coin drop and/or bill in, ticket in, ticket out, CEP In, NCEP In or NCEP Out depending on the functionalities enabled. For example, if the licensee does not have ticketing enabled on the slot machine the casino would not need to record the ticket in or ticket out meters. Likewise, if the licensee does have ticketing it does not have to record the coin out meter. The licensee must have an in-house form, which at a minimum, includes:

- beginning and ending soft meter readings,
- beginning and ending system meter readings,
- machine number, and
- date, time and signature of individual(s) who recorded the meters readings.

In addition to the previous requirements, all documentation must meet the Division's documentation standards. The licensee can attach a print out or screen shot of the beginning and ending system meter readings in lieu of recording them on the form. If a print out or screen shot is attached, the in-house form must refer to the print out; for example, a statement that says "see attached screen shot" in the system meter reading area would suffice. This area cannot be left blank.

The licensee must use the in-house form, stated above, to complete a Meter Comparison Report (MCR) which compares the soft and system meter reading incrementation for each meter. A sample of the MCR can be found in the ICMP forms area. In the MCR example there is a summary recap box; it is not necessary to include the summary recap box on the bottom of the page. In the event the meters do not pass testing, the licensee must resolve the issue, continue to take meters and update the MCR until the meter(s) have passed. The completion of MCRs must continue until the issues have been resolved, there are no variances between the soft and system meter incrementation, the MCR is signed and dated.

Option 2
At the time the slot machines are ready for patron play, the licensee will begin the testing process using the reports from the first drop period. The statistical reports (Drop, Ticket In, Ticket Out, CEP In, NCEP In and NCEP Out) must be reviewed within 24 hours of the completion of the

physical drop. The licensee must have some type of documentation that indicates the date the machine went live (e.g., internal spreadsheet when a machine is converted or added) to support that the reports were printed or viewed within 24 hours of the completion of the drop (e.g., printed report with the date the reports were printed).

Any statistical reports that indicate variances for any machines require accounting personnel to record all applicable slot machine soft meters and corresponding system meters for any machine with a variance. Meter testing must begin immediately by recording the soft and system meters and completing a MCR which compares the soft and system meter reading incrementation. A sample of the MCR form can be found in the ICMP forms area. In the MCR example there is a summary recap box; it is not necessary to include the summary recap box on the bottom of the page. In the event the meters do not pass testing, the licensee must resolve the issue, continue taking meters and update the MCR. The testing must continue until all applicable meters have passed testing, and the MCR is signed and dated.

Regardless of the option selected, the statistical reports must be accurate. If the variance was caused by a *clerical* error, it must be corrected and supported by the appropriate documentation. If the variance was caused by a *non-clerical* error or the meter fails testing, it must be investigated and the results of the investigation documented.

L. EMPLOYEE CONFIRMATION & TERMINATION

Licensees are responsible for controlling access with regards to enabling and disabling users from their gaming systems. Licensees are required to ensure that all employees, active and terminated, are listed on the Division's monthly list per CLGR 30-404. Currently, licensees use Revenue Online (www.colorado.gov/revenueonline) for this monthly reporting. Casinos with like ownership must ensure that Revenue Online is updated for all licensees even if the same employees work for each of the casinos.

All casino employees, licensed and unlicensed, must be listed and updated in Revenue Online at least monthly. The licensee must also ensure that employees with access to gaming system(s) have their access disabled by either locking, inactivating or deleting the user from the gaming system within three days of the employees actual termination date. The three day window begins when the casino has constructive knowledge, either by the casino initiation or by the employee initiation that the employee is no longer working at the casino. The actual termination date is when the casino notified the employee that he/she is terminated (three day window begins immediately), or the employee notified the casino of his/her last day (the three day window begins at the end of the shift on the last day). The licensee must have system reports that list both active and disabled users from the gaming system(s).

The following must be performed on at least a quarterly basis:

1. Reconciliation of the report(s) generated from the Human Resources (HR) department that provides a list of terminated employees along with the date of termination compared

to the end date listed in Revenue Online. It will be necessary to download and print or save the Revenue Online database.

2. Reconciliation of the gaming system generated report(s) (printed and/or saved) that indicates the name (user or employee number) and date that employees were disabled from the gaming system database(s) compared to the end date listed in Revenue Online.

3. Reconciliation of the active employee report(s) generated from the HR department (printed or saved) compared the active employees listed in Revenue Online.

4. Reconciliation of the active employee report generated from the HR department compared to the employees that have access to the gaming system databases.

Any differences in the reconciliations must be identified and further investigation must be performed. A detailed explanation of the reason for the difference must be included. All the documents stated above must be printed or saved to support the reconciliation processes. Evidence of the reconciliations must be reviewed at least quarterly by someone independent of this process.

If the casino identifies employees that have not been removed within three days, the process listed below must be completed. For employees whose access was not disabled within three days, a review of all system generated logs must be performed to confirm that the user did not access any part of the system between the HR termination date and the system termination date. This review must be documented.

The licensee must notify the Division via the relevant email address stated in the General subsection of this section with, at a minimum, the following information:

1. employee name(s),
2. date of HR termination,
3. date of system report termination,
4. which gaming system(s), user names, and/or modules/databases the employee was not disabled from within three days,
5. reason the employee was not disabled from the gaming system(s), and
6. if the employee did in fact access any of the gaming system(s) between the two dates.

A copy of the emails must be maintained with the system generated logs. Self-reporting after the fact is not a substitution for the proactive monitoring of the process of disabling access within three days of an employee's termination.

FORMS

Following is a description of the forms discussed in this section. In some cases, sample forms are provided and all of the forms are located on the Division's website athttps://sbg.colorado.gov/gaming. **It is the licensee's responsibility to ensure that all required forms contain the minimum required information and meet ICMP requirements.** See the General section for further clarification.

RAMP (Remote Access, Maintenance and Problem) Log

This log is used by licensees to document all remote access to the gaming system, any system maintenance performed as well as any system-related problems, issues, upgrades. If, for example, a system vendor (or other authorized user) is on the licensee's premises and logs onto the system from the licensee's terminal to perform system maintenance and/or to perform some "fix", this log is used to document this action.

Installation/Upgrade/Test Notification (notification form)

Licensees are required to complete and notify the Division, in writing, of the intent to install, modify or upgrade any system a minimum of 30 days prior to the anticipated installation, testing and/or go-live date. The system notification form is located on the Division's website.

TITO Device Checklist

Licensees are required to complete the TITO device checklist for all TITO devices. These machines must be tested thoroughly prior to being placed into service. Licensees must maintain these forms for Division review. Any problems must be addressed prior to a TITO device being placed into service. Any issues must be logged on the RAMP Log. A copy of the checklist is located on the Division's website.

Kiosk Checklist

Licensees are required to complete the Kiosk checklist for all TITO devices. Kiosks must be tested thoroughly prior to being placed into service. Licensees must maintain these forms for Division review. Any problems must be addressed prior to a Kiosk being placed into service. Any issues must be logged on the RAMP Log. A copy of the checklist is located on the Division's website.

Cage/Wireless Handheld Validation Unit Checklist

Licensees are required to complete the Cage/Wireless Validation Unit checklist for all Cage Validation Units and Wireless Handheld Validation Units. These units must be tested thoroughly prior to being placed into service. Licensees must maintain these forms for Division review. Any problems must be addressed prior to a validation unit being placed into service. Any issues must be logged on the RAMP Log. A copy of the checklist is located on the Division's website.