SECTION 13

SURVEILLANCE SYSTEM STANDARDS

A. GENERAL

Surveillance system standards apply to all license groups, unless otherwise noted.

All casinos shall have in place digital recording systems that meet the requirements of this section.

All casinos shall have digital cameras in place for primary coverage of all Gaming Activities on the gaming floor. As of January 1, 2024, analog PTZ~~'~~s will no longer be allowed for primary coverage of any Gaming Activities and may only be used for supplemental coverage, unless approved by the Director of the Colorado Division of Gaming.

All surveillance systems and camera coverage of all gaming activity and devices must receive initial approval from the Division prior to being utilized. After the initial approval, the licensee may make ~~the approved changes to its cameras~~ replacements to its cameras and hard drives but any changes to the surveillance system or gaming/critical camera layout requires ~~an approval~~the licensee to submit the Camera/Hard Drive Change Form and submit it to ~~by~~ the Division. The changed cameras and hard drives can be used immediately but the Division will perform an inspection within 10 days of the changes being implemented. Additional information can be found in the Notification Requirements document.

Each casino must have a surveillance review / monitoring room in-house. ~~Exceptions~~ The Division Director, or designee at its discretion may approve exceptions~~would~~ only ~~be~~ for commonly owned casinos, which are within the same County. In that case, ~~T~~the surveillance monitoring room must be within one of the commonly owned casinos and each casino requires a surveillance reviewing room / workstation in a secured location under surveillance camera coverage.

All personnel installing, cleaning, maintaining, and repairing surveillance equipment on site, including but not limited to, cameras, recording devices/servers (DVRs, NVRs), and network equipment (including switches and data cables), must be licensed by the Division of Gaming and report to the Surveillance Department.

The time displayed on the surveillance systems must be within 30 seconds of http://www.time.gov/ or the surveillance system's time must be synced to the same source that the licensee utilizes for its gaming system.

A date/time must be ~~imbedded~~embedded on all recordings of gaming areas. The date and time must be synchronized and set correctly and must not significantly obscure the ~~picture~~image.

Licensees are responsible for ensuring all surveillance equipment is properly functioning and the playback quality meets Division requirements.

The licensee must have all documentation, approvals, and variances, or copies thereof, relating to surveillance, kept in the surveillance review / monitoring room and available upon request.

The licensee is responsible for training licensed surveillance employees in game protection, the play of all games, the odds payouts of table games, investigations, and the use of its surveillance system.

SPECIFIC STANDARDS

B. DEFINITIONS

1. **Closed Network:** A closed network restricts access to authorized users only, ensuring only a specific group can communicate or interact with the network.
2. **Group A License:** Means a licensee who has 1-74 slot machines only. (CLGR 30-1601)
3. **Group B License:** Means a licensee who has 75-299 total devices or at least one table game. (CLGR 30-1601)
4. **Group C License:** Means a licensee who has 300 or more total devices (CLGR 30-1601)
5. **Cloud Based Storage:** The retention of non-gaming and non-critical cameras to an approved internet-based storage platform that is located on a remote, secured server.
6. **Critical Areas:** Includes cage, Keno drawer(s) area(s), vault, count rooms, table games, drop route, and any required cameras inside the surveillance room.
7. **Digital Resolution:** Refers to the number of pixels that make up an image or display.
8. **DVR (Digital Video Recorder):** Is an electronic device that records from analog cameras and turns the video into a digital format at the recorder.
9. **Fields:** One field is defined as half of one frame (older video equipment).
10. **Fisheye/360 Camera:** A digital camera that continuously records a designated 360 degree area regardless of what is being viewed live.
11. **FPS (Frames Per Second):** Frames per second is the measurement of the frequency (rate) at which an imaging device produces unique consecutive images called frames. Each frame consists of two fields.
12. **IP (Internet Protocol) Camera:** An IP Camera is a camera that receives control data and sends image data via an IP network.
13. **Monitor Size:** The display area measured diagonally and excludes the cabinet/frame of the monitor.
14. **Notification System:** A alert system that provides a notification when a panic alarm is activated.
15. **NVR (Network Video Recorder):** An NVR is an electronic device specifically for digital video, that encodes and processes video data at the camera and receives video streams over a network.

16. **Progressive Scan:** This is a method where each frame is captured as a whole, as opposed to splitting each frame into two fields. (modern video equipment – replaces "Fields").
17. **PTZ (Pan, Tilt, Zoom) Camera:** A camera that can pan 360 degrees left and right, tilt up and down, and zoom in and out. PTZ cameras only record the image being viewed at the time of the recording.
18. **Remote Access:** Remote access is any access (internal or external to the licensee's physical premises), including through use of personal electronic smart devices, to the surveillance system that originates from outside of the physical location of the surveillance monitoring room. If the licensee's in-house technicians are using licensee-issued personal electronic smart devices, then these devices may be used outside of the surveillance monitoring room but must only be used by in-house technicians while working. These licensee-issued personal electronic smart devices shall not be taken off property.
19. **Satellite Workstation:** Refers to any computer terminal(s), outside of the surveillance review / monitoring room that can be used to access and/or manipulate the surveillance system's operating system or user interface program.
20. **Stationary / Fixed Camera:** A camera that once installed cannot be moved by the surveillance system.
21. **Surveillance System:** Means a system containing video cameras, data lines, viewing monitors, digital servers, data switches and other ancillary equipment.

~~1.~~ **Workstations:** Refers to any computer terminal(s) within the surveillance review / monitoring room that can be used to access and/or manipulate the surveillance system's operating system or user interface program.~~Surveillance System – means a system containing one of more video cameras, monitors, servers, switches, and/or ancillary equipment.~~

~~2. PTZ Digital pan-tilt-zoom camera.~~
~~3. IP – Internet Protocol camera.~~
~~4. Stationary cameras - once a camera is installed it cannot be remotely moved.~~
~~5. Fisheye Camera – camera that is able to PTZ and record 360 degrees.~~
~~6. Monitor Size – the display area measured diagonally and excludes the cabinet.~~
~~7. Critical areas – includes cage, Keno drawer(s) area(s), vault, count rooms, table games, drop route, and any required cameras inside the surveillance room.~~
~~8. DVR – digital video recorder.~~
~~9. FPS – Frame rate or frame frequency per second. FPS is the measurement of the frequency (rate) at which an imaging device produces unique consecutive images called frames. Each frame consists of two fields.~~
~~10. Fields – One field is defined as half of one frame.~~
~~11. TVL – Total video lines of resolution.~~
~~12.~~22. ~~Remote access – any access to the surveillance system outside the company firewall.~~

C. EQUIPMENT

1. Cameras

All cameras must meet or exceed the requirements set within the applicable sections.

All IP stationary and IP PTZ/~~Fisheye~~fisheye cameras covering critical areas will be at a minimum rate of 22 FPS and must be of sufficient clarity to meet the requirements of this section.

All IP stationary cameras covering gaming floor areas will be at a minimum rate of 15 FPS and must be of sufficient clarity to meet the requirements of this section.

All remaining IP stationary cameras covering non-~~critical~~gaming areas will be at a minimum rate of 7.5 FPS and must be of sufficient clarity to meet the requirements of this section.

All PTZ/~~Fisheye~~fisheye cameras must be 360 degree functional in gaming areas ~~and must be enclosed in a shaded housing, so that it is hidden from view~~. All PTZ cameras must be enclosed in a shaded housing, so that it is hidden from view. All stationary fixed, PTZ/~~Fisheye~~fisheye cameras that are required by the Division shall be digital color stationary fixed, PTZ/~~Fisheye~~fisheye cameras.

Auto iris lenses are acceptable, if they are properly adjusted at all times. However, manual iris lenses, or auto iris lenses with a manual override, are required for PTZ/~~Fisheye~~ cameras.

2. Monitors

One–digital monitor in the surveillance review / monitoring room shall have the capability of displaying any camera (live or playback) in a 23-inch or greater viewable area, not to include system controls.

Licensees ~~with 500 or more devices~~ will provide a separate monitoring station / review room for reviews that does not interfere with normal operations or an assigned surveillance employee.

3. ~~Work Stations~~Workstations / Satellite Workstations

All work stations must be capable of video review in forward, reverse, slow motion, and frame-by-frame.

- Workstations must be within the physical confines of the casino's surveillance monitoring / viewing room.
- Workstation access permissions must be established to prevent any unauthorized access.
- Satellite Workstations outside of surveillance monitoring room / review room requires written approval from the Division prior to set-up and implementation.
- Satellite workstations are prohibited from having playback review, PTZ control nor video copying capability.
- Satellite workstations are required to be in a secured location which prevents unauthorized viewing and under surveillance camera coverage unless approved in writing by the Division.

- Satellite workstations are required to have log-in credentials. Users must log out immediately upon leaving the workstation. Safeguards such as automatic logout must be enabled, which shall log out a user after 15 minutes of inactivity when a user fails to logout after using the workstation.
- Satellite workstations camera access is required to be approved by the Division.
- Satellite workstations camera access shall only be requested for job specific cameras.
- Satellite workstations user access is required to be approved by the Division, by title.

The licensee must have an audible and visual failure notification system that provides notification of any recording system failure within ~~1~~5 minutes. Personnel staffing the surveillance review / monitoring room must be able to initiate a failure, within the system, or by physically unplugging a non-critical connection, upon request by the Division. All recording failures must be addressed within one hour of system notification.

All recordings must be erased or destroyed prior to disposal, sale to another licensee or manufacturer, or when discarded by any other means.

4. Printers/Email

If the surveillance review / monitoring room does not have the capability to deliver a clear still photo of a camera image through email, then one color capable video printer is required in the surveillance review / monitoring room.

D. CASHIER CAGES KENO WRITER STATIONS, VAULTS, COUNT ROOMS, ELEVATORS, AND KIOSKS

In all count rooms, cages, and vaults, cameras must be positioned so that all areas in the room are covered to include but not limited to, access points to and from the underside of desks and counters, storage areas, and to the highest area where an item can be stored. New and replacement cameras shall be replaced with color ~~capable~~ cameras.

Video surveillance must cover all areas where chips, tokens, cash, and other cash equivalents are stored.

Count rooms, vaults, cashier cages must have room lighting that is hard wired. There must be no ability to turn off the lights from inside the room, or near the doors.

1. Count Rooms

In the count room, stationary cameras must provide a close up, unobstructed view of the cash/coin counting table where the actual count takes place. During the count, the count team members, whether removing monies from the bucket or box, counting, sorting, verifying, or storing, must not obstruct the camera view of the monies.

The location where monies are set aside, until the end of the count and cashier verification, must be recorded by surveillance cameras that are located close enough to the monies to identify individuals accessing the funds, ensure the monies are clearly distinguishable, and can differentiate between money and other papers.

With a combination of cameras, all areas in the room shall be covered by unobstructed camera coverage. There shall be no lapses or gaps in coverage. Coverage must include the highest accessible areas where money or items can be stored.

Count rooms require audio to be recorded to the surveillance system. Signage shall be displayed notifying individuals within the count room that audio recording is occurring.

2. Cashier's Cage

In the cashier's cage, stationary cameras must provide a close up view of the cash/coin, slot coupon, and ticket transactions. Transaction areas must be clearly marked on the counter so that cashiers know where to place currency and documents.

Transaction cameras covering this area must be able to differentiate between bill denomination, slot coupon value, ticket value, and chip value, check value, and read the driver's license (at a minimum the first and last name, address, date of birth and driver's license number) of the person making a transaction, which requires a driver's license or personal identification. Designated cameras must view the full faces of patrons and employees making transactions with sufficient clarity to identify them at all cage windows on playback.

The location where monies are set aside, until the end of the count and cashier verification, must be recorded by surveillance cameras that are located close enough to the monies to identify individuals accessing the funds, ensure the monies are clearly distinguishable, and can differentiate between money and other papers

3. Elevators

Elevators used for transporting drops, fills, credits, jackpots, and gaming monies must have adequate surveillance coverage for the protection of assets, inside the elevator and at each opening on the floors. Small lifts, generally used to move small items from floor to floor, ~~Dumb waiters need~~are not required to have surveillance cameras inside, but must ~~still~~ have surveillance camera coverage at each opening on the floors.

4. Kiosk

All cash transaction devices which are an extension of the cage, such as a kiosk or other type of device that redeems gaming tickets, slot coupons, or exchanges coins, bills, or tokens shall have adequate surveillance coverage for the protection of assets. Identification of person(s) using the

device must include a view of at least one half of the person's face and close enough to identify the person using the device. Stand-alone ATM machines are exempt from this requirement.

Jackpot kiosks must have stationary cameras providing a close-up view of the jackpot slip and funds. Transaction cameras covering this area must be able to differentiate between bill denomination and tie to the jackpot slip. Designated cameras must view the full faces of employees with sufficient clarity to identify them at all kiosks on playback.

5. Key Box and Lock Systems

Restricted key boxes, duplicate key boxes, an automated key tracking system, and any other key lock system must be under surveillance.

6. Internal Hallways to and from Count, Vault, and Cashier Rooms.

Internal hallways to and from count, vault, and cashier rooms must have adequate surveillance coverage for the protection of assets.
~~Pouch Banks/Cabinets~~

7. Pouch Banks/Cabinets

All pouch pay, pouch bank, or change pouch, as well as their storage cabinets, lockers, or racks, etc., shall have adequate surveillance coverage at all times for the protection of assets.

8. Panic Alarms

Each cashier window shall have a panic alarm that notifies the surveillance department of an incident through a notification system. If manned surveillance is not required, the casino will draft emergency notification procedures that will be submitted to the Division for approval prior to implementation.

E. TABLE GAMES

Licensees may use either dedicated stationary cameras, dedicated PTZ/~~Fisheye~~fisheye cameras, or a combination of both, to meet the following requirements. Licensees with table games shall have a manned surveillance review / monitoring room whenever the table games in the establishment are open for play (see staffing requirements below).

Coverage of table games must be able to view the ~~patron and/ or dealers face,~~ cards, chips, tokens, cash, shuffler~~s~~, toke box, drop slot and play areas of each table. Cameras must be able to distinguish card values on the normal setup and playback. Any electronic table capable of game recall is not required to have coverage that reads individual card values or suits, if surveillance personnel have access to this system and when approved by the Division of Gaming. Table games linked to a progressive jackpot must have stationary camera coverage of the access to the

progressive controller computer and the progressive amount signage. Multi-table progressives within the same facility only require one progressive amount signage recorded. ~~A person's face at a gaming table, is defined as the ability to view at least one half of the patron and or the dealer's face.~~ Surveillance video must be able to view and record all error indicators on all shufflers being used on all table games.

During the course of play on any table game, the dealer must not obstruct the camera view of the table tray, drop slot, or tip box.

The soft drop route must be under stationary or PTZ/~~Fisheye~~fisheye camera coverage.

PTZ/fisheye cameras are required to identify all individuals, including but not limited to patrons, dealers and other casino staff, within the pit and table area.

BLACKJACK, HOUSE BANKED POKER, BACCARAT, BIG 6 WHEEL, OR OTHER VARIATION GAMES.

All Gaming tables within this section must have stationary digital camera coverage. Cameras must be positioned to provide an overview of the entire table, outside bumper to outside bumper, including the table tray, table game validation unit and drop slot, toke box/tube, and an automated shuffler (if applicable) while the game is in play. Stationary cameras must be able to distinguish all chip, cash, card, tickets, and total values of wagers on the normal setup and playback.

On all house banked poker tables, surveillance coverage is required to read suits and differentiate between chip/token, cash, ticket, and total wager values on playback. Surveillance coverage must also provide a view of the table tray, drop slot, tip box, toke tubes, automated shuffler, and must cover the entire table, which includes outside bumper to outside bumper.

On all Big 6 Wheel tables, ~~C~~ccameras must be positioned to provide an overview of the entire table, outside bumper to outside bumper, including the table tray, tip box, toke tube, drop slot, and the wheel, while the game is in play. Stationary cameras must be able to distinguish all chip, cash, card, ticket values, and total wagers on the normal setup and playback. All Big 6 Wheel games shall have one [1] dedicated camera viewing the Big Wheel.

PAI GOW TILES

All Pai Gow Tiles tables must have stationary digital camera coverage. Cameras must be positioned to provide an overview of the entire table, outside bumper to outside bumper, the table trays, drop slots, tip boxes, toke tubes, tile value, and determine the value of any and all wagers made, tips received and dropped, live and on playback.

POKER

All player banked poker tables must have stationary digital camera coverage that includes the table tray, rake slide, jackpot drop area, tip box, muck cards, shuffling device, and the wagering pot. Surveillance coverage must be able to distinguish the suits of the community cards and the winning hand on playback. Surveillance coverage must also view the entire poker table, which includes the back of chair to the back of chair.

All poker table tray storage cabinets, lockers, racks, table games validation units, etc., shall have adequate surveillance coverage for the protection of assets.

All poker imprest banks, which are the point of chip and cash transactions for the poker tables, must have the same camera coverage as that of a cashier's cage.

ROULETTE

All roulette tables must have a minimum of one stationary digital camera. The cameras must be positioned to provide an overview of the entire table, to view the rails which hold chips (if any), the table trays or chip storage area, the drop slots, tip boxes, and be able to determine the value of any and all wagers made, including tips received, live and on playback.

Stationary camera coverage must also cover the wheel, so as to be able to determine the outcome of the game, live and on playback. Stationary camera coverage shall be able to identify chip values.

CRAPS

All craps tables must have stationary digital camera coverage. Cameras must be positioned to provide an overview of the entire table, to view the rails which hold chips (if any), the table bank ~~trays~~, drop slots, table game validation units, the dealer working stacks of gaming chips, and tip boxes, tips received and dropped, live and on playback. Camera coverage must be able to identify the dice value.

F. SLOT AREAS

Licensees may use color stationary digital, dedicated PTZ, dedicated ~~fisheye~~fisheye~~, or~~ /360 cameras, or a combination thereof any to meet the following requirements.

Cameras must be positioned so the route of any person walking through the slot gaming area is covered at all times. All slot machines must be under stationary camera surveillance with sufficient coverage to protect assets. Coverage must include the access to the progressive controller, the candle, and the slot machine doors.

Surveillance coverage also must include aisles where hard drops are transported. During the drop, the route must be under coverage. The slot machine surveillance coverage must be able to

determine if a person is accessing the slot machine, the drop box, or is playing the slot machine on playback.

Any multi-linked progressive slot machine offering a payout greater than $1,000,000 and/or **any** non multi-linked slot machines offering a payout of more than $500,000 must have coverage of the progressive jackpot liability in addition to the above-required coverage. One camera showing the same liability for multiple banks of the same progressive may be allowed.

Each slot machine must have the ability to have its unique slot machine number be observed by a surveillance PTZ or stationary camera.

G. OTHER STANDARDS

For licensees with a dedicated Surveillance Department, the Surveillance Department operations and reporting structure must be independent of other casino departments, and other department management/supervisors in order to reduce or eliminate undue external influence, conflicts of interest, or bias.

The Surveillance Department must have a designated Surveillance Director or Manager. This position may not be responsible for the operation or administration of any other casino department (with the exception of the Security Department). If a Surveillance Director or Manager has the power to exercise a significant influence over decisions concerning any part of the gaming operation (the Surveillance Department), they must possess a valid Key License (*Reference CLGA 44-30-103(17)).* Any questions or concerns pertaining to this requirement should be directed to the Agent-In-Charge at your local Gaming Field Office.

The licensee must have surveillance procedures relating to Responsible Gaming. This would include, but is not limited to, identifying if Surveillance has the ability to monitor a slot management system that will receive/display alerts if a self-excluded patron inserts their own player's club card and that Surveillance must be notified of and monitor any Self-Excluded patron reported on property.

All camera views of gaming areas must be continuously recorded 24 hours a day. The use of motion detection for non-gaming areas is authorized with a five second pre-event recording with Division approval prior to initial use.

A complete index and guide to the casino cameras, monitors, and controls must be available in the surveillance review / monitoring room. This guide must include a map of the camera locations, direction of coverage, camera numbers, and operating instructions for the surveillance equipment. In addition, for unmanned surveillance review / monitoring rooms, a complete guide showing the chronological order of the hard and soft drop from start to finish must be available. The guide should have camera numbers and details of the machines covered. All surveillance recordings in critical gaming areas must be kept a minimum of 15 days or until gaming

document reconciliations have been completed by accounting, whichever is longer, and 10 days for all other gaming areas.

All video losses, that are not a result of routine maintenance, that exceed ~~1~~5 minutes for critical cameras or an hour on other required gaming cameras must be immediately reported to the Division. Any surveillance system component failure that affects the ability to review required coverage or to conduct an investigation must be reported to the Division in accordance with the reporting requirements.

When necessary to perform maintenance on recording systems, a casino may temporarily take system components offline to perform those functions. Proper planning and communication must take place to ensure gaming functions are not impacted by offline components (for example, a table game with no video coverage is closed, or a cage window with no coverage is not used). If it becomes necessary to take the surveillance system completely offline, the Division of Gaming must be notified prior to disabling, and gaming operations must cease prior to the commencement of the planned maintenance. Maintenance functions would generally be described as rebooting, defragmenting, or other necessary information technology functions necessary to keep the surveillance recording system operating properly.

-Access to surveillance review / monitoring rooms shall be limited to licensed employees that are essential to surveillance operations. This includes~~,~~ ICO's, casino shift managers, law enforcement agencies, licensed service personnel, and others when approved by the Division. The surveillance ~~room manager~~Director (or Manager for facilities that do not have a Director) has final authority regarding the authorization of access by casino personnel, except when the Division requires or authorizes access. A current list of authorized employee~~s~~ titles and service personnel that have access to the surveillance review / monitoring room must be posted in the surveillance review / monitoring room.

Surveillance review / monitoring room access lists must be submitted to the local Division Office with any changes and all changes require Division approval. The access list can list the titles of positions authorized and is not required to list specific names of individuals.

~~Each casino must have a surveillance room in-house. Exceptions would only be for commonly owned casinos, which are within the same County. The surveillance room must be within one of the commonly owned casinos.~~ The casino will provide a review station, email capability, or printer, map of cameras, and communication in the property that does not house the surveillance review / monitoring room if the casinos are not contiguous. All equipment and security standards in the review station room will meet the minimum criteria set forth by this ICMP section.

Surveillance review and monitoring rooms must remain locked and must have room for at least two people to view monitors. Licensees that have other functions housed in the surveillance review / monitoring room must receive Division approval. At least one surveillance camera must

be in the surveillance review room and in the surveillance monitoring room to record employee and visitor activity.

Group C Licensees ~~with 500 or more total gaming devices (slot machines and table games)~~ must have manned surveillance review / monitoring rooms at all times~~during gaming hours, and during the drop and count procedure~~. Group B Licensees ~~with less than 500 gaming devices but~~ having one or more ~~craps~~ table game(s) must have staffed~~manned~~ surveillance employees during the hours that any ~~craps~~ table game(s) is open for play.

Surveillance Staffing Requirements (Single Site, Single surveillance review / monitoring room):

- Group A Licensees may have an unstaffed surveillance review / monitoring room. The drop and count procedure must be recorded. If the slot machine drop and count is not reviewed by surveillance, surveillance footage must be maintained until all slot machine variances have been adequately investigated and a cause for the variance identified. If the cause for the variance was not identified by revenue audit/accounting or the slot department during the initial investigations a surveillance review must be performed within 72 hours after revenue audit/accounting has reviewed the documented investigation results completed by the slot department.
- Group B Licensees must have a surveillance review / monitoring room staffed by at least one (1) person at all times that table games are open for play. The table drop and table count procedure must be monitored and recorded. If the slot machine drop and count is not reviewed by surveillance, surveillance footage must be maintained until all slot machine variances have been adequately investigated and a cause for the variance identified. If the cause for the variance was not identified by revenue audit/accounting or the slot department during the initial investigations a surveillance review must be performed within 72 hours after revenue audit/accounting has reviewed the documented investigation results completed by the slot department. There must be at least one (1) person present during all hours of operation, that is competent in the use of the surveillance system and equipment.
- Group C Licensees must have a surveillance review / monitoring room with at least one (1) person present at all times.
    - **NOTE:** Staffing requirements are based on total gaming devices **AND/OR** the presence of open table games

Combined surveillance monitoring rooms, for Licensee's within the same county, are permitted, with prior Division approval. Staffing requirements for combined surveillance monitoring rooms will be staffed according to the total number of device and table games for those Licensee's. ~~If the licensee has a combined surveillance room with a second and or third casino, manned surveillance will be required if the total number of gaming devices between all of the casinos is 500 or more.~~

~~Each combined surveillance room must be staffed for each individual license in accordance with the above minimum staffing requirements. An authorized person competent in the operation of~~

~~the surveillance equipment must relieve the surveillance agent/operator for any and all breaks.~~Exceptions to the Group B and C Licensee surveillance staffing requirements will be made, for any and all breaks of surveillance employees, by a Key on Duty competent in the surveillance requirements and operations.

Surveillance recordings, to include recordings for evidentiary purposes and clear still photos must be maintained for a minimum of three years and made available to the Division upon request. All Licensee's must be able to provide an AVI or MPEG format of video upon request by the Division of Gaming, Law Enforcement, or the District Attorney's office of the jurisdiction the licensee is in.

Group B and C Licensee ~~Manned~~ surveillance review / monitoring rooms must have the ability to immediately send and receive emails of still pictures to the Division of Gaming and law enforcement for the purpose of disseminating information of suspects involved in illegal activity. The e-mail account cannot be networked with the surveillance system.

Licensees may utilize an approved cloud based storage platform for non-gaming and non-critical cameras upon approval by the Division of Gaming. No cameras with a view of the gaming floor shall be added to the cloud based storage platform. Access to those cameras will mimic existing established access procedures to prevent unauthorized access to the cameras or recorded footage. Cameras must be approved by the Division of Gaming prior to being added to the cloud based storage platform.

H. DIGITAL SURVEILLANCE

All digital recording devices are required to record, review and download simultaneously without an interruption of the record mode. Digital recording devices must be connected to an uninterruptible power source to ensure safe shutdown of the system in the event of a power loss, and must reboot in the record mode. Uninterruptible power sources are required to be tested, and results logged, annually.

In the event of a complete power failure in a casino or power failure in the pit area or surveillance review / monitoring room, all table games, cashier cage and vaults, and count rooms must be shut down until power is restored and the surveillance system is fully operating. Should the power or surveillance system shut down, it is proper to complete the hand in play before table play is stopped. The operations ~~games~~ may only commence if power has been restored, or if the establishment is equipped with a back-up generator able to fully operate all surveillance systems.

~~When necessary to perform maintenance on digital recording systems, a casino may temporarily take system components offline to perform those functions. If it becomes necessary to take the surveillance system completely offline, the Division of Gaming must be notified, and gaming operations must cease prior to the commencement of the planned maintenance. Maintenance functions would generally be described as rebooting, defragmenting, or other necessary information technology functions necessary to keep the digital surveillance recording system~~

~~operating properly.~~

~~Maintenance functions shall be performed at a time when it is least disruptive to operational functions of the casino and are exempt from the notification requirements of one hour for non-critical coverage loss and the notification requirements of 15 minutes for critical loss. Any other surveillance losses or system component failure shall continue to be reported to the Division of Gaming as required.~~

The licensee must provide the Division with the necessary software/hardware to review a proprietary downloaded recording. The media player must be ~~imbedded~~embedded within the recorded medium and must be capable of review in forward, reverse, slow motion, and frame-by-frame.

The licensee is responsible for supplying the below listed mediums for the amount of recorded information being downloaded and transferred to flash drive, memory stick, USB, or a portable hard drive. VHS (or any other video tape), ~~along with~~ CD~~'~~s, and DVD's are ~~not an acceptable format for the~~ no longer acceptable forms of media for download or storing of video information required by the Division.

All necessary cables, programs, and instructions for use must be supplied with these devices. The licensee must ensure that appropriate policies and controls are in place outlining the device check in/out process. Upon completion of use, the Division will return the equipment to the licensee. The licensee will provide a carrying case for the medium, if applicable.

An authentication process or watermark will be required to authenticate dates/time and validity of live and archived data. The authentication and/or watermark must be visible on the archived data as a visual verification. All surveillance personnel, or persons responsible for an unstaffed surveillance review / monitoring room must be able to demonstrate the authentication/watermark process upon request.

The Division must be notified in advance if a licensee intends to utilize AI (Artificial Intelligence) functions with their Surveillance System. For the purpose of this section, 'AI functions/systems' shall be defined as those that perform biometric identification, behavioral profiling, or external data processing beyond the local closed network. This includes, but is not limited to, Facial Recognition software or systems. The licensee must submit information pertaining to the use of AI. This information shall include the following:

- Manufacturer and Program Name.
- Purpose and function of the software and how data will be used.
- Is the program a current system feature or a stand-alone add on to the existing system.
- Location where the data will be stored.
- How data will be added or removed.
- Who will have access to the data.
- Policy/procedure to ensure that data is used only for the purpose intended and confidentiality will be maintained.

- Cameras that will be used in conjunction with this software.
- How the program will integrate with the current surveillance system.
- Identify if the program can be accessed from external sources, regardless of whether or not external (remote) access will be used.
- Any remote access to this system must be pre-approved in writing by the Division.

If the licensee uses a network for the digital recording equipment, it must be a closed network with limited access, unless approved by the Division of Gaming. A closed network may utilize firewalls or network components that are interlinked and only communicate internally and restricts or eliminates access from outside the closed system. External connections, outside of the closed system, would include having the internet accessible on the same computer that accesses the surveillance system, an unprotected or unrestricted IP address on a surveillance server (NVR), computer sharing software that allows the external source to manipulate the house surveillance computer/workstation, screen sharing software that allows the external source to view the surveillance computer/workstation, or a physical hardwire data line connection to an open network port on site. If the licensee has cameras on an approved cloud based storage platform, this would not fall under the requirements of a closed network. Casino personnel are required to demonstrate this upon request by the Division.

Network equipment located throughout the casino's property must be secured in a manner that prevents unauthorized access. Used or unused network connections must not allow unauthorized access to the surveillance network. The licensee must have procedures in place that prevent unauthorized access to the surveillance system.

The licensee may allow remote access to its network for emergency maintenance purposes ~~and within the casino~~ with prior approval by the Division. Written procedures must be submitted to the Division for approval prior to allowing the remote access. Written procedures will specify that the surveillance internet access utilizes a process where an ethernet cable is plugged into the system before access is given and unplugged when the access ceases. The remote access must be on a secure network. Any individual who remotely accesses the surveillance system must have a valid Colorado gaming license.
Licensees must maintain a manually generated and system generated log that documents system upgrades, modifications, problems, and all remote access.

The system access log must be maintained at all times and include, at a minimum:

1. Date of remote access;
2. Reason for the remote access;
3. Full name, license number & position of person remotely accessing the system;
4. Description of how the problem was resolved or modification made to the system.

The system generated log, at a minimum, must include the date, start time, and end time of access. The report must be printed monthly and traced to the manual log. The Division must be notified, in writing, of any variance between the manual and system log, which must include an explanation for the variance, and a reconstruction of the events that occurred. The system and

manual log must be maintained together in the surveillance review / monitoring room and available to the Division upon request.

The use of any video and/or still images obtained from the remote access is strictly prohibited outside of what is defined and approved within the written procedures.

For Licensee's that receive approval for emergency maintenance remote access procedures, additional procedures will be submitted to the Division which allows the Division access through similar procedures, when the Division dictates that an emergency life safety incident exists.

Surveillance review / monitoring room equipment must have total override capability over all other remote access service equipment located outside of the surveillance review / monitoring room, even if that access is from within the same building.

Critical areas, table games, and PTZ/~~Fisheye~~fisheye cameras covering critical areas and table games will be at a minimum rate of 22 FPS with two fields per frame (or progressive scan) and must be of sufficient clarity to meet Division requirements. Recording of non-critical areas will be at a minimum rate of 7.5 FPS with two fields per frame (or progressive scan) and must be of sufficient clarity to meet Division requirements.

If the licensee's surveillance system records its working monitors (work stations) or call up monitors at a rate of 22 FPS or more, the requirement for FPS on its PTZ/~~Fisheye~~fisheye cameras covering critical areas and table games will be considered met.

I. EMERGENCY PROCEDURES

Licensees will develop procedures for critical incident observations and notifications and will ensure surveillance employees and the Key on Duty are trained in the appropriate response.

Each Surveillance, Security and Key on Duty employee will be trained annually on critical incidents.

Procedures will be developed and submitted to the Division for approval, to allow for first responders to gain access to keys for restricted areas~~keys~~ during a critical incident.

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 Section H. Digital Surveillance for further clarification.

Surveillance Equipment Maintenance Log

A log which documents all maintenance to surveillance equipment.