STOREY COUNTY ADMINISTRATIVE POLICIES AND PROCEDURES

NUMBER: 018
EFFECTIVE DATE: 07/03/18
REVISED:
AUTHORITY: BOC
COUNTY MANAGER: PAW

SUBJECT: SURVEILLANCE IN THE WORKPLACE

I. Purpose

Storey County recognizes that maintaining the safety and security of employees, customers, and county property is best implemented with a multi-faceted approach. To the extent that modern technology provides tools to maintain safety and security, the use of technology such as video surveillance is supported by the board.

Surveillance systems may be used around buildings, public areas, on county property, county vehicles and equipment, and on peace officers as allowed and regulated by NRS. Video surveillance, and data management and retention, will conducted in accordance with applicable state laws.

Managing and communicating allowed video and audio recording device use by employees, members of the public, and others is also important to ensuring that certain rights of employees and members of the public are protected.

II. Placement and Notification

A. Video surveillance systems may cover publically accessible places on county property including buildings; hallways; lobbies; areas within offices where public access exists; cafeterias and libraries; meeting rooms; county roads, sidewalks, parking lots, parks, pools, and indoor and outdoor public places.

B. Video surveillance is prohibited in areas where there is a reasonable expectation of privacy, including but not limited to, restrooms, locker rooms, clothes changing areas, and fire district or county employee bedrooms and sleeping areas.

C. Video cameras will be placed in conspicuous locations. This policy encourages video cameras to be highly visible and installed in prominent locations in order to deter criminal activity. Use of hidden video surveillance devices is prohibited.

D. Use of video surveillance within employee office areas may be used to monitor specific areas where public access exists (e.g., front counter area), where valuable or highly sensitive property or materials are located (e.g., vault, safe, server room, equipment station, vehicle fueling station, cash drawer, etc.), or where there is a need to for enhanced security and safety (e.g., public utilities, water treatment, chemical storage, etc.).

E. Placement of video cameras will avoid to the extent feasible or to the extent that the device fails to fulfill a direct safety purpose, direct view over employee office work stations and employee office computer monitors. In such case that an

employee's office work station and/or office computer screen may be visible from the video surveillance device, the department head shall approve or deny its placement at that location, subject to approval by the County Manager. Video surveillance within the Sheriff's Office, its substations, the jail facility, and other buildings thereof are subject only to the Sheriff's approval.

F. Law enforcement "body-camera" use will conform to the applicable NRS and Sheriff's Office policies, and is not subject to this policy.

G. Unless written consent is provided by the affected property owner and its tenants, video cameras must not be situated so that they cover or monitor neighboring properties or buildings not owned by the county, including but not limited to, neighboring buildings, yards, garages, and windows. A camera's resolution capability and ability to zoom and pan must be taken into consideration for this purpose. Such systems are not prohibited from covering or monitoring adjacent streets, sidewalks, parks, vehicle parking lots, and public places. The affected property owner and its tenants may revoke the consent at any time, at which point the county must within two work days make necessary corrections to the video cameras to comply with this section.

H. The location, placement, function (e.g., zoom, pan, etc.), view span, and type for each video surveillance device are subject to approval by the County Manager.

I. Surveillance systems may operate 24 hours per day on a year-round basis at any and all times during business hours and non-business hours.

J. Surveillance system display monitors must not be located in areas that enable public viewing.

K. The county will notify employees that video cameras may be used on county premises. The notification will be performed by making this policy available on the county website.

L. Any exterior video camera placed on a building within the Comstock Historic District must receive a certificate of historic appropriateness from the historic district. Extra care must be taken to ensure that video surveillance devices do not cause detriment to the aesthetic authenticity and character of any historic building, with special care toward public areas in and near the historic buildings.

III. Systems Use

A. The use of video surveillance equipment on county property will be with the knowledge and consent of the County Manager or his/her designee(s), and may include the county Emergency Management Director as appropriate.

B. The County Manager will designate employee(s) who have authorization to view and access surveillance equipment. The authorization may be revoked by the County Manager at any time and for any reason.

C. Employees and the public are prohibited from unauthorized use, tampering, destroying, copying, distributing, or otherwise interfering with surveillance equipment and recordings. Discipline up to and including termination may be imposed in accordance with the Storey County administrative policies.

D. The County Manager or his/her designee, and/or the Administrative Officer and/or Personnel Director, may conduct periodic audits of the surveillance system to ensure that use and access to the system is done in accordance with this policy.

E. Surveillance recordings may be used as evidence that an employee, vendor, member of the public, or other person(s) has engaged in behavior that violates county policies or state/federal laws.

F. Surveillance systems may not be used for the purpose of performing employee performance evaluations, monitoring employee compliance with dress code policies, monitoring employee attendance or timeliness, or for monitoring general employee performance. Surveillance systems may be used in any investigation to confirm violations of county policies. Surveillance systems and recordings may not be used to bully, harass, embarrass, or publically tarnish the reputation of, or treat unethically, any employee or person.

G. Video surveillance recordings may show clear video; time, date, and year; and location of the associated device; may employ infrared and other night vision; and may zoom, pan, and track individuals, vehicles, or other movement within the field of vision. The system may employ vehicle and vehicle license plate recognition and other recognition capability.

H. Security video surveillance footage may not be displayed on any website, social media, or other media of the county. Special exceptions may be made by the County Manager on a case-by-case basis. This section does not apply to webcams, weather cams, wildlife cams, and other similar video footage.

I. Court proceedings, video arraignments, and court and detention facility conference recordings may not be displayed on any website, social media, or other media of the county.

J. No person will operate, monitor, or access archived footage of the surveillance system until s/he has read and demonstrated in-writing his/her understanding of this policy.

IV. Audio Surveillance

A. Except as otherwise provided by this section, audio surveillance systems are subject to the provisions of this policy governing video surveillance systems.

B. Audio surveillance may only take place in vaults, safes, hazardous material storage areas, and other areas where valuable or highly sensitive property or materials are located (e.g., an office vault, safe, server room, equipment station, etc.); Sheriff's offices, substations, jail facilities, and other Sheriff's facilities; areas designated by the Emergency Management Director as high security or highly sensitive to exterior threat; and other areas where the county determines that there is a clear need for enhanced security.

C. Audio surveillance is prohibited where there is reasonable expectation of privacy including, but not limited to, restrooms, locker rooms, employee break rooms, clothing changing areas, and fire district employee bedrooms and sleeping areas. Audio surveillance is prohibited in employee offices and at employee work stations, except as may be appropriate under section (IV)(B) above.

D. A prominent sign(s) must be displayed in a conspicuous part(s) of the area under audio surveillance. The locations must include, but are not limited to, the entrance of that area. The sign must clearly advise all persons that the subject area is under audio surveillance.

E. Audio recordings by the employer, employees, and members of the public, not associated with this section, will conform to the applicable provisions of this policy and the NRS.

V. Data Storage and Security

F. Surveillance recording systems must be maintained within a secured location within a county building(s). The entrance to the room or area containing the surveillance recording system must be located so that it is not readily accessible by employees or the general public, and it must be locked at all times except during maintenance or repairs and when under direct supervision by the authorized person(s). Electronic safeguards will be incorporated into the system and maintained including, but not limited to, password protection, well-managed firewalls, and encryption to protect the systems from hackers, unauthorized users, and unauthorized use. The digital system must incorporate a video verification encryption code (watermark).

G. Surveillance recording will be stored for a minimum of 14 days after the initial recordings and for a maximum of 60 days after the initial recording. The maximum period may be deviated slightly according to recording system parameters for data writing over hard-drives.

   Specific recordings may be retained for longer periods when they are suspected to contain evidence of misconduct, policy violations, crimes, or matters which are under investigation by law enforcement officials, the Administrative Officer and/or Personnel Director, and/or the County Manager. Upon completion of the investigation, the subject recordings must be erased from the surveillance system in accordance with the time periods shown in this section, but the subject recordings may be stored separately with the investigation file or case file in accordance with state and county records retention laws.

H. Surveillance system failures must be documented and reported to the County Manager or his/her designee. Diligence must be taken by the appropriate employee(s) to remedy the system failure promptly. The County Manager or his/her designee must be notified when the remedy is completed.

VI. Viewing Requests

Requests for review of surveillance recordings will be regulated as follows.

A. Law Enforcement and Court Order Requests:

   a. Requests by law enforcement officials to view or obtain surveillance recordings must be presented to the County Manager. If the County Manager is unavailable, the requests will be presented to his/her designee or to the Administrative Officer and/or Personnel Director. Law

enforcement officials may review the recordings, in which case such records would be released only pursuant to a valid court order.

b. In the event of a search warrant, which is executable immediately, the County Manager or his/her designee will comply with the search warrant and consult immediately with the District Attorney's Office.

c. Upon receipt of a subpoena or other court order, the County Manager or his/her designee will consult with the District Attorney's Office to determine if the document is in proper form and that good cause for its issuance in a court of proper jurisdiction is demonstrated. If not, the County Manager or his/her designee will insist any defect be remedied before releasing records.

B. Employee Requests:

a. All viewing request by county employees must be submitted to the County Manager or his/her designee in writing. Request for viewing will be limited to those employees or county officials with a direct interest in the recording as authorized by the County Manager or Emergency Management Director with concurrence by the County Manager. Only a portion of the recoding concerning the subject incident or issue will be made available for viewing.

b. Approval or denial for viewing will be made by the County Manager or his/her designee within 5 business days of the request, and so communicated to the requesting individual.

c. If approved, recordings will be made available for viewing within 5 business days of the decision. All review of the recordings will occur in the presence of the County Manager or his/her designee.

d. To the extent required by law, a written log will be maintained for those viewing video and audio recordings including the date and location of review, reason for review, date the recording was made, and the viewer's written name and his/her signature.

e. Recordings will remain the property of Storey County and may be reproduced only in accordance with applicable law and county policies.

C. Public Disclosure

a. Protection of infrastructure, secure area, and other data from public requests.

b. Confidentiality/privacy issues prohibit the general public from reviewing surveillance recordings that contains information about county employees and public customers. If the county receives a request from a member of the public to inspect surveillance recordings which contains employee or customer information, and the request appears suspicious, the recipient of the request is advised to file a complaint with the Sheriff's Office.

c. All requests for public disclosure of recordings will be presented to the County Manager or his/her designee.

d. A copy of this policy must be shared with members of the public upon request.

e. Actual viewing by third-parties, such as the public or media, will be permitted only at a secure county located as determined by the County Manager or his/her designee, unless otherwise required by law.

VII. Video and Audio Recording Use by Employees

A. Employees are prohibited from operating video recorders or other visual/audio recording devices in areas where confidential personnel information may be compromised. Such areas may include, but are not limited to, areas where there is a reasonable expectation of privacy including, but not limited to, restrooms, locker rooms, clothes changing areas, etc.; the Human Resources Office except for the designated public area therein; and vaults, safes, and other areas where valuable or highly sensitive property or materials are located (e.g., an office vault, safe, or equipment stations); and areas designated by the Emergency Management Director as high security or highly sensitive to exterior threat.

   The County Manager or Administrative Officer and/or Personnel Director should be contacted by any person if there is question as to where video and/or audio recording in any part of the workplace may or may not occur.

B. Employees are prohibited from operating cameras or other visual/audio recording devices at staff meetings where company trade secrets or proprietary business information could be disclosed, except when there exists knowledge and consent of every person in a room or associated with the subject meeting.

C. No employee may photograph or video another employee's personnel record or sensitive identification except as allowed for official business such as in the Human Resources or Comptroller's offices.

D. Employees may record workplace activities when the recording is performed in such a manner not prohibited by law and when the recording does not compromise confidential information as described above.

VIII. Video and Audio Recording by Members of the Public

A. Any member of the public may video and/or audio record within public areas of county property and buildings, and areas visible from public places, including buildings, office areas, work stations, and other areas which are visible from the public place. This activity is sometimes referred by certain members of the public as a "First Amendment Audit".

B. Member of the public are prohibited from video and audio recording within areas not accessible to the public.

C. Each county office must designate a place and/or places in which the public is allowed to access (e.g., front service counter area, seating areas, lobby areas, etc. within each office). These public places must be identified as such by highly visible and conspicuously placed signage (e.g., "employees only beyond this

point", "no public access", etc.). Outdoors areas around buildings and offices where public access is restricted must be posted as such, but those areas may not include public streets, sidewalks, parks, and other spaces open to the public. Outdoor job sites, construction areas, and other such areas must be cordoned off and/or demonstrated clearly as restricted areas. Employee vehicles and equipment are not considered public places and do not need to be marked as such. Private property in which county business may be conducted is not considered a public place for the purpose of this policy.

D. No member of the public video and/or audio recording in accordance with this policy may obstruct, disrupt, or interfere with business; obstruct openings or public access and circulation; physically or verbally harass, bully, intimidate, or disturb employees, vendors, or other persons in the vicinity; or violate any law or county policy. Persons exhibiting such behavior will be asked kindly by county staff to leave the premises. If the person refuses to leave the premises after being asked to do so, the employee will exercise appropriate effort to not escalate the situation with the person, and s/he will promptly contact the Sheriff's Office for assistance.

   Whether or not it is necessary to contact law enforcement, the following guidelines should be followed when a member of the public attempts to video and/or audio record a county employee at the workplace.

   a. Allow the person to conduct the recording within the public place.
   b. Remain verbally and physically calm.
   c. If it is necessary to engage in conversation, respond verbally to the person calmly no matter what his/her demeanor.
   d. Inform the person of the parameters of the immediate public place.
   e. Do not engage in argument with the person.
   f. Do not confront the person physically.
   g. Do not counter-video record the person.
   h. Avoid photographing the person except as necessary to take a photograph that may be provided to law enforcement, emergency management, the department head, and/or county officials. Do not photograph as a mechanism to instigate the person.
   i. Ignore the person as much as possible. Conduct business as usual despite being recorded. Leave the immediate room out of his/her sight if necessary. However, do not leave sensitive information or materials unsupervised.
   j. Attempt to remember features of the person such as facial features, hair and facial hair color, height and build, clothing, and unique features such as tattoos, scars, piercings, etc.
   k. Attempt to obtain the person's vehicle make, model, approximate vintage/year, license plate number, and identifiable features such as bumper stickers, body damage, etc.

l. Report the incident to the department head as soon as possible regardless if the incident was hostile or not. Report the incident to the Emergency Management Director and County Manager if the person appeared to be suspicious or if the person is believed to be a potential future threat to the county, any person, or the community.

RESPONSIBILITY FOR REVIEW: This policy will be reviewed on an annual basis by the Information Technology Director.