



<b>GENERAL SERVICES DEPARTMENT</b> <b>Agency Policy</b>	Number: <b>GSD-008</b>
Subject:  <b>Security Camera Policy</b>	Effective Date: <b>3/21/2016</b>
	Number of Pages: <b>11</b>

**REVISION LOG**

Revision Number	Date	Responsible Party/Author	Comment
Rev.0	08/03/2015	Leo Rodriguez/Jay Hone	New Policy.
Rev.1	03/21/2016	Kimberly Hunt-Brown	Policy number changed to GSD-008 due to duplication error in numbers; header update changed pagination, no textual changes made to document

<b>1.0</b>	<b>Purpose.....</b>	<b>2</b>
<b>2.0</b>	<b>Scope / Applicability / Organizations Affected.....</b>	<b>2</b>
<b>3.0</b>	<b>References .....</b>	<b>2</b>
<b>4.0</b>	<b>Background.....</b>	<b>2</b>
<b>5.0</b>	<b>Definitions .....</b>	<b>2</b>
<b>6.0</b>	<b>Policy Statement.....</b>	<b>4</b>
<b>7.0</b>	<b>Procedures .....</b>	<b>11</b>
<b>8.0</b>	<b>Attachments and Enclosures .....</b>	<b>11</b>
<b>9.0</b>	<b>Approval .....</b>	<b>11</b>

## 1.0 PURPOSE

This policy establishes guidance for the limited use of security cameras systems installed **asa** safety and security measure in state-operated buildings in Santa Fe. The Facilities Management Division (FMD) of the General Services Department (GSD), and tenant agencies of FMD-operated buildings, must balance the public benefits of security camera use against an individual's right to be free of unwarranted intrusion into his or her life. The desired outcome for this policy is to streamline the security camera procedure at FMD for the primary purpose of maintaining building and campus security. Duties and responsibilities of FMD personnel, as well as those of the building proctors and tenant agencies who are involved in the implementation of this policy and its procedures, are defined in this document.

## 2.0 SCOPE/ APPLICABILITY/ ORGANIZATIONS AFFECTED

The primary purpose and use of the content and information recorded by the security camera system installed and maintained by FMD is to protect public safety and property, and to detect or deter, and assist in investigating, criminal activity.

Tenant agencies must be able to demonstrate that any proposed or existing collection of information by a security camera system is authorized, justified and appropriate.

## 3.0 REFERENCES

New Mexico Statutes Annotated (NMSA) 1978 15-3B-4 (as amended, 2001), Chapter 15, Administration of Government, Article 3B, Property Control, Part 4, Division, Duties, Federal Funds

1.13.70 New Mexico Administrative Code (NMAC), Public Records, Performance Guidelines for the Legal Acceptance of Public Records Produced by Information Technology Systems

## 4.0 BACKGROUND

Statutory authority for this policy is based on Paragraph A.7 of 15-3B-4 NMSA 1978, which authorizes FMD to: "make rules for the conduct of all persons in and about buildings and grounds under its jurisdiction **necessary and proper for the safety, care and preservation of the buildings and grounds and for the safety and convenience of the persons while they are in and about the buildings and grounds.**" (Emphasis added.)

## 5.0 DEFINITIONS

**Access Control Specialist:** Individual within the FMD organization who is responsible for physically generating access cards/codes, electronic building access and hard keys to buildings.

**Building Modification Request:** The documentation required for modifications to buildings, including that needed for security camera upgrades not listed in any prior SAUs.

**Building Proctors:** Individuals designated by the agency or department heads that have security responsibilities for the space in a particular building to be responsible for overall building management and maintenance, and who define all levels of personnel access to a particular building or agency. Where appropriate, the building proctor will arrange for each person assigned to that building for daily work to be given access by assigning them an individual access device (i.e., access cards, keys). A building may have more than one building proctor, depending on the building.

**Reception Equipment:** The equipment or device used to receive or record the information collected through a security camera system, including a camera or video monitor or any other video, audio, physical or other mechanical, electronic or digital device. Reception equipment might also be or contain the storage device for the captured information.

**Record:** As described in 1.13.70 NMAC, a record is information preserved by any technique in any medium now known, or later developed, that can be recognized by ordinary human sensory capabilities either directly or with the aid of technology. A record may include, but is not limited to, information captured at a moment in time and preserved upon paper, film, video or audio tape, or by an electronic device such as a digital camera, computer, or a handheld device with recording capability, where the preserved information can later be retrieved in the original captured format, or can be restored to a form comprehensible to a human through the use of human senses (i.e., sight, hearing, touch), or can be retrieved from an electronic or digital medium and made to produce data comprehensible to human senses.

**Security camera System:** Video, physical or other mechanical, electronic, or digital observing or monitoring of open, public spaces (including streets, highways, and parks). In these guidelines, the term security camera system includes an audio device, thermal imaging technology or any other component associated with capturing the image of an individual and storing it for a specific period of time.

**Service Provider:** A vendor or contractor who may design, install, upgrade, maintain, replace, back up on electronic media, store, or remotely diagnose or access the security camera system.

**Space Assignment Understanding (SAU):** Official allocation of building space and the assignment of responsibilities by FMD to a tenant of FMD-operated buildings.

**Storage Device:** A videotape, computer disk or drive, computer server, CD ROM, computer chip or other device used to store the recorded data or visual, audio or other images captured by a security camera system.

## 6.0 POLICY STATEMENT

### 6.1 Implementation

This policy applies to any building, premises or property controlled by the Facilities Management Division of the General Services Department. This policy provides the requirements and guidance needed when developing and approving SAUs and building modification requests related to the installation and use of security camera equipment. This policy also provides the rationale behind why certain **areas** of FMD-operated property and buildings might need to be monitored through the use of an installed security camera system.

### 6.2 Roles and Responsibilities

- 6.2.1 **Building Proctor**- requests security camera equipment upgrades or reorientation of video cameras through building modification requests; requests video recordings for each area of interest by completing a work order request that identifies each specific camera, according to inclusive dates and times, from which recorded material is needed.
- 6.2.2 **FMD Director or Designee** - responsible for oversight and final approval of FMD SAUs and building modification requests.
- 6.2.3 **FMD Environmental Safety and Health Coordinator** - audits the use of security camera equipment in buildings operated by FMD.
- 6.2.4 **FMD Facilities Modification Committee** - authorize security camera upgrades beyond building design.
- 6.2.5 **FMD Facilities Operations Manager** - receives building modification requests and work order requests for video recording; oversees the use and maintenance of security camera equipment and storage devices; serves as primary contact with contractor providing security camera services.
- 6.2.6 **FMD Facilities Operations and Maintenance Bureau Chief**- oversees the assignment of tenant agency/building proctor responsibilities, SAUs, and changes resulting from building modification requests.

### 6.3 Consideration of, and Verifiable Justification for, the Use of Security Cameras

- 6.3.1 For the purposes of this policy, a security camera should only be used on public property, and at entrances, exits, and within passages considered to be public areas on public property.
- 6.3.2 Security cameras may furthermore be justified whenever their use is deemed the most cost-effective way to deter, detect, and investigate risk to the general public or

to public property, or to deter or solve criminal activity.

- 6.3.3 The use of each security camera may be justified on the basis of verifiable, specific reports of incidents of crime, or reports of significant safety concerns, or the value and exposure of new or remodeled construction.

## 6.4 Privacy Implications

- 6.4.1 The benefits of installing and using a security camera must be weighed against the individual's right to be free of unwarranted intrusion into their life by means of video monitoring. Installation and use of a security camera system to provide ongoing monitoring and recording of people moving about during their daily workday must be carefully planned and implemented to ensure that individual rights to privacy, as well as individual rights to a safe and secure workplace, are protected.
- 6.4.2 Privacy implications will be considered as to the effects that the proposed security camera system may have on personal privacy, especially when the location being monitored is internal to a building.
- 6.4.3 Within areas considered to be "private areas":
  - 6.4.3.1 FMD shall not install or use security cameras **as a** standard practice within private areas.
    - a. Any use of security cameras in off-normal conditions, such as those described in this policy, shall first be discussed with the GSD Legal Counsel, appropriate senior management for the affected division, and the FMO Director.
    - b. When supported for use within private areas, technical staff will be directed to maximize privacy protection while achieving the goals of the exception.
  - 6.4.3.2 Some areas where security cameras will not normally be installed or used include, but are not limited to, the following:
    - a. Areas where there is a normal and reasonable expectation for privacy, such as washrooms, change rooms, locker rooms, shower areas, and non-common hallways or residential areas.
    - b. Areas that are specifically designed for the comfort of employees, or where their personal possessions may be securely stored, such as within restricted-access lounges and locker rooms, shall be considered to be private areas under this policy.

- c. Areas that are dedicated to medical, physical, or mental health therapy or treatment shall also be considered to be private areas under this policy.
- 6.4.4 There should be no expectation for personal privacy in areas considered "public areas". Public areas include, but are not limited to:
- 6.4.4.1 External areas that are open and accessible to the general public (e.g., parking lots, transportation platforms, passenger pickup or drop-off areas)
  - 6.4.4.2 Interior common-use areas that may or may not be available to the general public but that are made available to state employees on a non-controlled-access basis (e.g., cafeteria or dining areas, hallways, stairwells and stairways)
  - 6.4.4.3 Parks and sidewalks
  - 6.4.4.4 Building exteriors and loading docks
  - 6.4.4.5 Areas of ingress and egress
  - 6.4.4.6 Public-access areas of state buildings (**e.g.**, lobbies, auditoriums or theaters)
  - 6.4.4.7 Libraries
  - 6.4.4.8 Display areas, such as those in museums or other public buildings, where historical, cultural, educational, or artistic works are exhibited
- 6.4.5 There should be no expectation of privacy in common-use areas of FMD-controlled buildings. Such common-use areas may include, but are not limited to: hallways, stairwells and stairways, lunchrooms, building lobbies or foyers, and meeting areas such as conference rooms or auditoriums. Under the auspices of this policy, those areas of FMD-controlled buildings to which access is restricted to certain state employees, such as chemical or material storage areas, equipment storage areas, and some office areas, should also be considered to be public areas.
- 6.4.6 Consultations should be conducted with relevant stakeholders as to the necessity of and justification for a proposed security camera program.
- 6.4.7 Appropriate signage should be posted to indicate security camera usage.

## **6.5 Video Storage, Access and Wireless Technology Requirements**

- 6.5.1 All storage devices that are not in use shall be stored as follows:
  - 6.5.1.1 All tapes or other storage devices that are not in use should be stored securely inside a locked receptacle located within a controlled-access area.
  - 6.5.1.2 Each storage device that has been used should be dated and labeled with a unique, sequential number or other verifiable symbol.
- 6.5.2 Access to the storage devices will only be made through authorized personnel.
  - 6.5.2.1 A log will be kept of all instances of access to, and use of, recorded material, to enable a proper audit trail.
  - 6.5.2.2 Electronic logs should be kept where records are maintained electronically.
- 6.5.3 Security camera systems using wireless technology should encrypt the wireless transmission of all information.

## **6.6 Use and Retention of Recorded Video**

- 6.6.1 Old storage devices must be securely disposed of in such a way that the information cannot be reconstructed or retrieved. Disposal methods may include overwriting electronic records, shredding, burning or magnetically erasing the information.
- 6.6.2 FMD must control access to stored security camera recordings, and to those areas of FMD-operated buildings where live security cameras are being monitored to ensure that only authorized individuals under certain circumstances are able to view security camera transmissions.
  - 6.6.2.1 Security personnel may view live security video feeds or security video recordings as a routine assignment in the performance of their job duties.
  - 6.6.2.2 FMD should maintain a written list of authorized individuals who, by virtue of their position within FMD, GSD, or the tenant agency, may need to access security camera recordings on a routine basis.
  - 6.6.2.3 The list of authorized individuals should also correlate a list of circumstances (i.e., following report of an incident, to investigate a potential crime) under which each authorized individual can view the captured information.
- 6.6.3 FMD will establish the retention period for information that has not been viewed for law enforcement or public safety purposes, and will ensure that such information is routinely erased or destroyed according to a standard schedule.

- 6.6.4 Law enforcement officials may request security camera recordings if they are investigating an incident involving an FMD-operated building or property, a state building or property, or an incident nearby where the alleged perpetrators or incident might have been caught by installed security cameras.
- 6.6.5 All law enforcement requests for security camera footage shall be considered to be official formal requests, and should be processed in tandem with completion of an FMD record of access.
  - 6.6.5.1 Documentation completed by FMD will contain a cross-reference to any law enforcement incident report number, and will include as an attachment any other legal document furnished by the law enforcement entity at the time of the request (i.e., subpoena).
  - 6.6.5.2 A separate retention period will be established for recorded information that has been requested for a law enforcement or public safety investigation. Captured personal information used for this purpose will be retained for one year following closure of the investigation by the responsible agency.
  - 6.6.5.3 FMD will store and retain storage devices requested for evidentiary purposes until law enforcement authorities release them.
    - d. A storage device release form shall be completed before any storage device is released to the appropriate authorities.
    - e. The form should indicate who took the device and under what authority, when this occurred, and if it will be returned or destroyed after use.
    - f. Retaining and releasing storage devices for evidentiary purposes should be regularly monitored and strictly enforced.

## **6.7 Use of Reception Equipment**

- 6.7.1 Reception equipment such as video cameras, audio-capture or other devices should be installed in public areas where security cameras are appropriate to protect public safety, and to detect, deter, and assist in the investigation of criminal activity.
- 6.7.2 Equipment should be installed in such a way that it monitors only those spaces that have been identified as appropriate for security camera monitoring.
  - 6.7.2.1 Equipment should not monitor the areas where individuals generally have a higher expectation of privacy {e.g., change rooms and public washrooms}.
  - 6.7.2.2 Cameras should not be directed to look through the windows of adjacent buildings.



**6.7.2.3** If cameras are adjustable by operators, adjustment capability should be restricted, if possible, so that operators cannot adjust, zoom or manipulate the camera to monitor spaces that are not intended to be monitored under the security camera program established for that **area**.

6.7.3 FMD should post signs in areas with security cameras to ensure that state employees and the general public will both be given reasonable and adequate notification that they may be in, or entering into, an area where security cameras are or may be in use.

6.7.3.1 Signs should be clear and easy to comprehend, and should be prominently displayed in the areas where security cameras may be operating.

6.7.3.2 Signs should identify someone who can answer questions about the security camera program by including an address, telephone number, or website for contact purposes.

6.7.4 Reception/recording equipment should be in a strictly controlled access area.

6.7.4.1 Only personnel authorized to operate the system, or those properly authorized in writing according to the organization's policy, should have access to the controlled-access area and the reception/recording equipment.

6.7.4.2 Video monitors should never be in a position that enables public viewing.

## **6.8 Security Camera Installation Requests**

6.8.1 Requests for modifications that are made by a building proctor or tenant agency and are specific to the installation of a security camera system are required to include:

6.8.1.1 The rationale and objectives for installing the security camera system or implementing a security camera system upgrade.

6.8.1.2 The use of the system's equipment, including: the location of the reception equipment; which personnel are authorized to operate the system and access the storage devices; the times when security cameras will be in operation.

6.8.1.3 A requirement that the building proctor or tenant agency will comply with this policy and has read and agrees to same, and signs an approved certification form regarding compliance as part of the review of its installation request.

6.8.1.4 A requirement that any agreements between the building proctor or tenant agency and the service providers state that the records dealt with or

created while delivering a security camera program are under FMD's control.

6.8.1.5 A requirement that employees and service providers review and comply with this policy while performing their duties and functions relating to the operation of the security camera system

- Employees will be subject to discipline if they breach the policy or relevant statutes.
- Where a service provider fails to comply with the policy, it should be considered a breach of contract leading to penalties up to and including contract termination .
- Employees of organizations or tenant agencies and employees of service providers will sign written agreements regarding their duties under the policy, including confidentiality.

6.8.1.6 A requirement that the requirements of this policy be incorporated into the appropriate training and orientation programs of organizations or tenant agencies and the service provider. Training programs addressing staff obligations under this policy should be conducted on a regular basis.

6.8.2 The SAU will be reviewed and updated when there is a change or upgrade to the security camera system, or a change in building proctor or Department Head. Conversely, any time an SAU is updated or added, the security system will be reviewed for necessary modifications.

## **6.9 Auditing and Evaluating the Use of a Security Camera System**

6.9.1 The use and security of security camera equipment is subject to audits.

6.9.1.1 The audit should address the tenant agency's compliance with the operational policies and procedures.

6.9.1.2 Any deficiencies or concerns identified by the audit must be addressed immediately.

**6.9.1.3** Tenant agencies should be aware that their activities are subject to audit, and should be aware that they may be called upon to justify their interest in any given **area**.

6.9.1.4 FMD should review and evaluate its security camera program to ascertain whether it is still justified in accordance with this policy.

6.9.2 Reasons to perform an audit of the security camera system might include, but are not limited to, the following:

- An incident is reported related to personnel working in or around the building.
- An incident is reported related to the building, such as vandalism.
- A crime is reported in the **area** and there is a possibility that security cameras might have picked up information that could aid in the investigation.
- To verify that only authorized personnel have been accessing the captured video recording.
- To determine whether a camera angle has been changed from the designated angle.

## 7.0 PROCEDURES

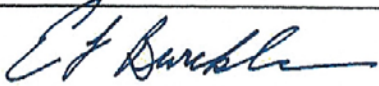
Change orders processed under this procedure will be kept in the formal project files and retained with these files for reference.

## 8.0 ATTACHMENTS AND ENCLOSURES

None.

## 9.0 APPROVAL

Approved by:

  
\_\_\_\_\_  
Edwynn L. Burckle, Secretary, GSD

3/21/2016  
Date