

Guam Power Authority

Standard Operation Procedure

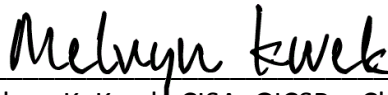
Title/Description: Video Monitoring & Surveillance Guidelines
Procedure No.: SOP-175
Effective Date: 2/13/2025
Supersedes: n/a
Procedure Owner: Safety Division

Prepared by:



Kenneth J. Gutierrez, PSP – Safety & Physical Security Manager

Concurred by:



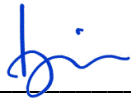
Melvyn K. Kwek, CISA, GICSP – Chief Information Technology Officer

Concurred by:



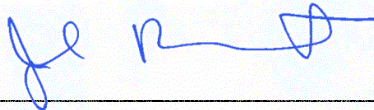
John J. Cruz Jr., P.E. – AGM, Engineering & Technical Services

Concurred by:



Beatrice P. Limtiaco – AGM, Administration

Approved by:



John M. Benavente, P.E. – GENERAL MANAGER

PURPOSE

This policy outlines video surveillance measures designed to ensure the safety and security of Authority personnel and assets, and serve to protect the interest of our utility customers. It is part of various measures of the Authority's overall strategy relative to physical security. Additionally, this policy ensures that a transparent environment exists within the Authority with regard to all video surveillance measures.

SCOPE

This policy shall apply to Guam Power Authority and Guam Waterworks Authority (GWA) employees working within GPA-operated facilities, including the Gloria B. Nelson Public Service Building (GBNPSB), and other facilities housing GPA assets deemed under GPA Physical Security purview. This policy also applies to contracted vendors and members of the public while on Authority property.

DEFINITIONS

Asset: Any tangible or intangible value (*people, property, information*) to the organization.

Camera: Device used for capturing visual images, whether still or moving, in security as part of video surveillance.

Closed Circuit Television (“CCTV”): Also known as Video Surveillance, are video camera technologies used to transmit a signal to a specific place for viewing or recording, but are not publicly distributed.

Covert Cameras: Cameras that are concealed and not readily seen or identifiable as a recording device.

Detection: The act of discovering an attempt (*successful or unsuccessful*) to breach a secured perimeter (*such as scaling a fence, opening a locked window, or entering an area without authorization*).

Event: A noteworthy happening; typically, a security incident, alarm, medical emergency, or similar occurrence.

Physical Security: That part of security concerned with physical measures designed to safeguard people; to prevent unauthorized access to equipment, facilities, material, and documents; and to safeguard them against a security incident.

Physical Security Measure: A device, system, or practice of a tangible nature designed to protect people and prevent damage to, loss of, or unauthorized access to equipment, facilities, material, and information.

Security Incident: An occurrence or action likely to impact assets.

Surveillance: Observation of a location, activity, or person.

Video Surveillance: A surveillance system in which a signal is transmitted to monitors/recording, and control equipment. Includes CCTV and network-based video systems.

Video Surveillance Device: Any item, system, camera, technology device, communications device, or process, used alone or in conjunction with a network, for the purpose of gathering, monitoring, recording, analyzing, or storing an image or images of GPA facilities. Images captured by surveillance cameras may be real-time or preserved for review at a later date. These may include CCTV systems or covert cameras, which have the capability to store images in an electronic format for later viewing.

Video System: support assessment of alarms and allow for review of incidents within the field of view of the various cameras.

Reasonable Expectation of Privacy: a place where a reasonable person would believe that without concern that he or she is being viewed, photographed, filmed or otherwise recorded by an imaging device.

RESPONSIBILITIES

All GPA employees and all affected GWA employees must become familiar with these guidelines. Employees are responsible for reporting any known deviation or circumvention of this policy to their immediate supervisor or manager and ultimately to the Safety Division.

Authorized GPA employees that are tasked to monitor or have access to view recordings shall be held responsible to perform such duties for official GPA business purposes only. A confidentiality statement and Non-Disclosure Agreement (NDA) will be signed for the purposes of their respective duties.

Contracted Security System Operators fall under the purview of the Safety Division, and may be responsible for the monitoring of the video surveillance system. The operators will be trained in the effective, legal, and ethical use of the monitoring equipment, and expectations related to confidentiality. All recording or monitoring will be conducted in a professional, ethical, and legal manner. A confidentiality statement and NDA will be signed by the contracted vendor and each of the operators.

Division Managers shall ensure that employees receive and comply with the policy.

Safety & Physical Security Manager is responsible for the physical security program of the Authority and the overall implementation operation and maintenance of video surveillance and monitoring.

Shall ensure that authorized GPA employees and/or contracted operators conduct official business while monitoring the system. Shall oversee the work of employees, ensuring they are trained and understand the sensitivity and confidentiality of the information and data they are collecting and reviewing.

Shall establishes policies and directs the overall administration of the Video Monitoring and Surveillance program, and shall maintain, secure, and issue all relevant data requests and responses as approved.

Conduct annual audits with the Chief Information Technology Officer (CITO) or designee on the program and review relevant policies for updating.

Information Technology (IT) Division is responsible for the installation and maintenance of the surveillance system servers, remote monitoring system, software (*Operating System and Applications*), updates, patches, server storage, backups and any system expansion.

SURVEILLANCE INSTALLATION/OPERATIONS/MAINTENANCE

GPA may, at any time, conduct video surveillance of any portion of its premises with the only exception of areas with a reasonable expectation of privacy. Video monitoring of designated areas for safety and security purposes will be conducted in a professional, ethical and legal manner.

Any video surveillance device installed, used, monitored, or recorded on or within GPA facilities and properties, and properties with GPA assets shall be reviewed and facilitated through the Safety & Physical Security Manager with IT and Engineering Support for any construction, installation and technological related work.

- A. The Safety & Physical Security Manager is charged with the governance and operations of the video surveillance system and accessories, and has the authority to select, coordinate, operate, manage, and monitor all Authority wide security surveillance systems pursuant to this policy.
- B. The Safety & Physical Security Manager or designee is responsible to establish and maintain approval and operational guidelines concerning the installation and continued use of video surveillance technologies.
- C. The Safety Division will be responsible in the coordination with pertinent Divisions/Sections to ensure that Authority-owned buildings and facilities with video surveillance devices have visible signage indicating that surveillance cameras are in use.

- D. Request for installation of additional or new surveillance cameras, their locations, and purpose must be approved in advance by the Safety & Physical Security Manager or designee with concurrence and overview of the Physical Security Steering Committee. All requests for surveillance camera(s) installation must be approved prior to the purchase of equipment.
- E. Upon approval of the request, the Safety & Physical Security Manager will consult and coordinate with the IT Division regarding the procurement of the necessary equipment and related accessories. All requests for installation of surveillance camera(s) and corresponding hardware and software must be approved prior to the purchase of equipment.
- F. The Safety Division is charged with overseeing the installation and maintenance of the cameras and mounting hardware.
- G. The IT Division is charged with overseeing the installation and maintenance of all related cabinets, switches and equipment, related accessories and software to support surveillance monitoring.
- H. The IT Division is responsible for the annual inspection of all authorized cameras and systems to ensure that they are in proper working condition and meet this policy's requirements. This will insure that preventive maintenance is coordinated and carried out on a determined schedule. They will ensure the maintenance service, repairs and replacement of cameras and equipment of the surveillance system as needed. These inspections will be documented and maintained by IT Division. The Facilities Division and respective Division Managers will also be provided advanced notice of the maintenance scheduled, and to ensure proper clearance, authorization and escort while vendor is on Authority property.

SURVEILLANCE MONITORING

Surveillance Usage. Video surveillance is primarily used to:

- A. Detect activities that call for a security response;
- B. Collect images of an incident for later review and use as evidence, if needed; and
- C. Assist with incident assessment.

Vital to this policy is the use of video equipment to deter crime, assist in response to security issues, and provide information for criminal investigations. With efforts to promote safety, security, and the protection of individuals and assets, monitoring shall include, but are not limited to:

- A. Common areas and areas accessible to and by the public;
- B. Stairwells and hallways;
- C. Building Exits and Entrances;
- D. Perimeters of all authority-owned, rented, or leased property and buildings;
- E. Rooms and areas containing high value equipment and/or information; and
- F. Cash-handling areas where money is exchanged, such as cashier locations, and vaults.

Any video recorded, collected or preserved in any manner is the property of Guam Power Authority and shall not be released to any requestor without the proper approval process as outlined in Section 7 of this policy.

Any diversion of video technology for any purpose other than safety or security (*e.g. monitoring of political or religious activities, personal gain, and employee performance*) is prohibited by this policy.

An individual's and/or a group's behavior may warrant specific monitoring with safety and security in mind. However, no one will be selected for monitoring based on discriminatory criteria such as gender, race, sexual orientation, national origin or disability.

PROHIBITED SURVEILLANCE

The Authority will not carry out and does not condone surveillance of customers, vendors, and/or employees in any of the following areas:

- A. changing rooms;
- B. breastfeeding rooms
- C. restrooms;
- D. shower rooms;
- E. locker rooms;
- F. toilets; or
- G. other bathing facility in the workplace.

Video surveillance monitoring equipment will not be installed in areas where there is a reasonable expectation of privacy. The Authority will not carry out and will not condone any surveillance in these areas.

No video surveillance equipment will be installed for the sole purpose of covertly monitoring employee behavior in the absence of evidence pointing to criminal

behavior involving a particular employee(s). Covert cameras will only be used to aid in suspected criminal investigations within the legal means and processes of the law. Such surveillance will require the written prior approval of the Safety & Physical Security Manager, Legal Counsel, and the General Manager or designees. Video footage may be retrieved if determined to be relevant to an ongoing investigation.

Video surveillance equipment found to be illegally installed without approval, or used in such a manner that violates any portion of this policy or pertinent laws shall be removed and confiscated by the Safety Division. All relevant local and federal law enforcement entities will be called for a full investigation and further pursuit and prosecution of offenders. The Safety Division will conduct and document the investigation. Offender(s) will be subjected to disciplinary action to include the criminal ramification by local and federal legal authorities, as warranted.

ACCESS TO SURVEILLANCE RECORDS

Access to camera systems will be monitored and strictly controlled. This section outlines the protocol for requesting access to surveillance records, as warranted and approved.

All requests for access to surveillance records must be submitted in writing to the Safety Division. The Safety & Physical Security Manager or designee will review the request and make determination for approval or denial based on the nature, implications and severity of the request as it relates to Safety and Security measures.

Upon approval of the request, the Safety Division will coordinate with the IT Division in the retrieval of the requested surveillance recording. The Safety Division will be responsible for the distribution of the requested surveillance record(s) to the requestor.

The Safety Division will maintain a log of all surveillance access requests and information released.

A. The log shall include, at the minimum, the following information:

1. requestor's name and title;
2. date request was received;
3. particular date(s) and time(s) surveillance camera recordings accessed;
4. requestor's acknowledgment that information was received;

5. date of receipt; and
6. Safety Division official who released the surveillance records.

The log is to note and document whether the accessed recordings were relevant to the purpose of the request.

- A. Surveillance records shall only be released to the approved requestor.
- B. Safety Division will remind the requestor of the requirements of this policy and that information shall not be released without prior written approval.
- C. The log documentation shall be retained for at least twenty-four (24) months.

Any surveillance records made as a result of the surveillance review will not be used or disclosed unless:

- A. They are for a legitimate purpose related to employment or business activities or functions.
- B. They are required and are a part of an ongoing investigation.
- C. They are a part of and substantiate an alleged complaint as related to maintaining a safe and secure environment.
- D. They are required to be presented to local and/or federal law enforcement agencies.
- E. They relate to civil or criminal proceedings.
- F. It is necessary in order to avert an imminent threat, violence to persons, hostile work environments or substantial damage to property.

DATA LOG AND STORAGE

Recorded camera images will be retained for at least thirty (30) days by the servers maintained by the IT Division. Records retention may exceed the minimum days. Therefore, all purchased devices must be capable of retaining media for at least this period of time.

A log documenting access to and use of data stored in the Authority's centralized surveillance system will be maintained for a period of twenty-four (24) months by the IT and Safety Division respectively.

Surveillance recordings will be stored in a secure location with access by authorized personnel only.

COMPLIANCE AND REPORTING

Failure to adhere to this policy may result in disciplinary action being taken.

Anyone who has reason to suspect a violation of this policy must promptly report it to their immediate supervisor, their Division Manager and ultimately to the GPA Safety Division.

Policy infringements will be assessed and action taken to remediate the violation accordingly. The severity and/or adverse effect(s) of the infraction(s) on GPA's operation and security will be considered. If offense is found to be deliberate and/or willful, offender may also be held personally liable for damages caused by any violations.

Any person who tampers with or destroys video security equipment will be subject to disciplinary action, and may be personal liability of any associated costs.

Employees or supervisors who fail to report known violations of this policy may also be subject to disciplinary action.