

Georgia Town Policy and Procedure

Effective: 08/01/2023

SUBJECT: Video Surveillance and Physical Access Control Policy

PURPOSE

The purpose of this policy is to ensure that the legal, privacy and financial interests of the Town of Georgia, its tax payers, and staff are maintained while providing guidelines for the administration of video surveillance on or in town property.

POLICY

It is the policy of The Town of Georgia to ensure that video surveillance is done in a professional, ethical, and legal manner consistent with other Town policies and applicable laws.

The administration of this policy is coordinated by the Town of Georgia Selectboard.

DEFINITIONS

Surveillance Camera

Any item, system, camera, technology device, communications device, or process, used alone or in conjunction with a network; or tape, for the purpose of gathering, monitoring, recording or storing an image. Such devices may include but are not limited to: analog and digital surveillance cameras, close circuit television, web cameras, and computerized visual monitoring.

Access Control device: Any device that grants access to a secured building, room and/or area. These devices include and are not limited to: electronic. door strikes, magnetic locks, scan cards, key fobs, etc.

System Administrator(s)

The staff that supports and maintains the information technology network, including the surveillance camera and access control infrastructure. Responsible for retrieval of video and access control logs from software application.

Incident

An incident is defined as an unusual occurrence (unplanned, remarkable, or exceptional) for which a response, in the form of an investigation and/or administrative action is appropriate. An incident is the occurrence of any of the following, (but not limited to), on the property of the Town of Georgia or in connection with the provision of any of its services.

1. Theft.
2. Vandalism.
3. Misconduct.
4. Accidents or Traffic Safety.
5. Compliance Violations.

PROCEDURE

Surveillance cameras may be used and installed in areas where the security of either persons or property is enhanced. Video will be used to accurately record events and provide a means of identifying individuals (staff and non-staff) who may be involved in legal or policy violations. Procedures are outlined below:

Data, storage and archiving

All video surveillance must be archived for a minimum period of 30 days in an appropriate folder identified by the system administrator.

If video surveillance is evidence in an incident, or an event involving an external party, it will be archived for a period of 1 year or longer depending on the resolution of the incident.

Installation Of New Security Cameras

New surveillance cameras can be installed in any area where monitoring is necessary to protect persons or property. It will be at the discretion of the Selectboard to determine these locations, they will consider recommendations from town boards, advisory committees, and town employees. Once installed, new cameras must be inspected, maintained, and monitored in the same manner as other cameras to ensure that they are in operating condition.

Request for Surveillance Video

Anyone who has knowledge, or was involved in, an incident can request that the surveillance video be reviewed by providing the date, time, and location of an incident to the Town Administrator. The request must be approved by the Selectboard and should be made within 30 days of the event. Unique situations will be reviewed and addressed on a case-by-case basis by the Selectboard.

Any law enforcement officer investigating a potential criminal matter may request a copy of the surveillance video. The request shall be reviewed, and if appropriate, approved by the Town Administrator/ Selectboard.

Access Control

The Access Control System has been implemented to enhance the safety, security, and efficiency of our town offices. Access control cards will be issued and maintained by the Town Administrator (or as otherwise designated by the Selectboard) to employees with the appropriate access level needed for their role with the town. Where needed, control access can be quickly turned on or off allowing for easy access for meetings, cleaners, etc. without disruption to parties involved.

Access, Sharing and Release of Video Surveillance

Surveillance video and information contained on video shall not be used, viewed, or disclosed for any purpose without receiving consent from the Selectboard, except as noted below.

Surveillance Video outside of Town Office

The exterior town office cameras were installed with the purpose of being monitored during business hours so that office staff could see who was entering the building. Since there is no line of site to the doors from the clerk's office, viewing of live feeds specifically limited to the outside the town office during normal business hours for these cameras would be permitted to the Town Administrator or additional parties as granted by the Selectboard.

Surveillance Video as Evidence to an Investigation of Public Misconduct

In the event that a video is evidence to public misconduct, the Selectboard must be notified and approve access of the video, including presentation of the video to person(s) involved.

Surveillance Video as Evidence to an Investigation of Employee Misconduct

In the event that a video is evidence to employee misconduct, the Selectboard must be notified and approve access of the video, including presentation of the video to person(s) involved.

Surveillance Video as Evidence to an Investigation of External Matter

In the event that a video is evidence to any external matter, the Selectboard must be notified and approve access of the video, the Selectboard shall make a decision on whether to release the video to external parties.

Surveillance Video as Evidence of a Criminal Matter

In the event that a video is evidence to any criminal matter deemed non-time critical and no immediate or ongoing danger to the public and/or an individual, the Selectboard may approve access of the video and shall make a decision on whether to release the video to a law enforcement (LE) officer. If the criminal matter is an event in which there is an immediate or ongoing danger to the public and/or individual, LE will be able to view applicable video in furtherance of their investigation upon request without immediate Selectboard approval which might not be feasible. The video surveillance system Primary or Secondary Administrator will immediately notify (at a minimum) the Selectboard Chair when LE request viewing access to the video surveillance system. A Selectboard quorum will be required to release a copy of the video to LE if needed.

MAINTENANCE

Upgrades or maintenance of security cameras

All cameras and related equipment are expected to be functional at all times. If a camera is found in need of repair, a request will immediately be sent to the vendor who supports the system. If the cost for repair is above the amount of money budgeted, the Selectboard shall be notified for direction.

Planned Outages

If the video surveillance system needs to be shut down for maintenance or upgrades, every effort should be made to do so during off hours and for a shortest period of time required.

Removal of Security Cameras. Access Control

The Selectboard shall make final decisions on the removal of any equipment. Access control will be vested in the Internet Technology Firm that is serving the town. They will manage the cameras and access to the footage unless the Selectboard designates a different System Admin. They will cooperate with the police if needed as part of an investigation and they will be proactive to prevent access by employees of the Town and to limit opportunities for abuse of the camera footage.

Inspection

A selected System Administrator will be responsible for the inspection and monitoring of the cameras. The cameras must be inspected on a monthly schedule to ensure the system is functioning properly. The process for a proper inspection will be defined by the company or firm that installed the system. A Primary and Secondary System Administrator will be designated annually in March by the Selectboard or as needed throughout the year due to a vacancy in either role.

Cyber Security

The Video Surveillance Administrators will use existing and new industry best practices to protect the integrity of the video camera system from external threats. These will include at minimum:

- *Change the system default password as required
- *Change the system password on a regular basis or when it's suspected that the system has been compromised.
- *Apply software updates regularly as needed for camera system
- *Limit the number of users and physical access to equipment.

*Ensure that the internet provider that supports the camera system maintains up to date firewall integrity and virus protection.

PRIVACY

Protecting Privacy

Surveillance Cameras will not be placed in areas where staff, residents and the public have reasonable expectations of privacy, i.e., bathrooms, changing rooms.

All effort will be made to limit any surveillance to town owned property and buildings. These cameras are intended to capture activities happening on municipal property and there is no intention or desire to record anything that may occur on an adjacent property.

Adopted by the Selectboard on _____ at a publicly warned meeting.

Chair

Vice Chair

Selectboard Member

Selectboard Member

Selectboard Member

