TOWN OF GEORGIA VIDEO SURVEILLANCE & PHYSICAL ACCESS CONTROL POLICY

Adopted [INSERT Date]

PURPOSE

The Town of Georgia ("Town") uses video surveillance equipment in municipal buildings or on municipal property to ensure the safety of the community, staff, and Town property. Any activity captured on the cameras may be recorded and archived and can be used for resolving any Town issues requiring documented evidence.

The purpose of this Video Surveillance and Physical Access Control Policy is to ensure that the legal, privacy and financial interests of the Town of Georgia, its taxpayers, 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 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 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 images. 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 or prevents 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, key pads, etc.

System Administrators: The staff that supports and maintains the information technology network, including the surveillance camera and access control infrastructure. They are 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" includes, but is not limited to, the occurrence or allegation of any of the following on the property of the Town or in connection with the provision of any Town services:

1. Theft.
2. Vandalism.
3. Crime
4. Town Personnel Misconduct.

5. Accidents or Traffic Safety.
6. Compliance Violations.

PROCEDURE

Surveillance Cameras may be used and installed in areas where their presence enhances the security of either persons or property. Video will be used to accurately record events and provide a means identifying individuals (staff and non-staff) who may be involved in incidents, or legal or policy violations. Procedures ae outlined below:

Data, storage and Archiving

All video surveillance will be retained until obsolete, but must be archived for a minimum period of at least 30 days in an appropriate folder identified by a System Administrator.

Any recorded surveillance video that becomes part of a criminal investigation must be retained in accordance with applicable regulatory requirements.

The Town reserves the right to retain recorded surveillance video longer than 30 days if the recorded surveillance video contains recordings of events that are potentially relevant to any actual or potential legal claims involving the Town.

The Town shall retain recorded surveillance video that is relevant to a potential legal claim against the Town upon the Town's receipt of a credible threat of litigation of that potential claim for a period of one day after the statutory limitations period to bring the potential claim has run.

Installation of New Security Cameras

The Selectboard shall determine the locations where new surveillance cameras shall be installed. In exercising its discretion, the Selectboard will consider comments from the public, 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 Review of Surveillance Video

Anyone who was involved in an incident can request that a System Administrator review the surveillance video by providing the date, time, and location of an incident to the Town Administrator. The request should be made within 30 days of the event. Unique situations may be reviewed and addressed on a case-by-case basis by the Selectboard. The Town has no duty to preserve surveillance video related to civil claims that do not involve the Town.

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.

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, controlled 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

When recorded data is accessed, all information pertaining to that access event will be logged, and those logs will be made available to the Town Administrator and the Selectboard monthly, or as requested. Information that will be logged includes, but is not limited to:

1. Date and time of access,
2. The user accessing the system,
3. Whether or not recorded data was exported or saved external to the video surveillance system.

All system access rights, login events, and system activities will be logged with periodic audits to ensure compliance.

No unauthorized recording of video footage through cell phones, portable devices, or any other means is permitted.

Live Surveillance Video of Exterior of Town Office

The exterior Town office cameras were installed with the purpose of being monitored during business hours so that the Town office staff could see who was entering the building since there is no line of sight to the doors from the Town Clerk's office.

The Town Administrator, Public Works Director and additional parties specifically designated by the Selectboard may view live feeds of the cameras showing the exterior of the Town Office during normal business hours for those cameras. All cameras will be checked daily to ensure cameras are working properly. Indoor cameras will not be monitored unless an incident warrants a request for review of surveillance video.

All requests for release of recorded videos shall be handled in accordance with State law. Licensed law enforcement officers will be provided access to recorded videos upon request if the recorded video is within the licensed law enforcement officer's jurisdiction.

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, the System Administrators shall immediately send a repair, work order, or replacement request to the vendor who supports the system. If the cost for repair is above the amount of money budgeted, the Selectboard shall be notified and asked for direction.

Planned Outages

If the video surveillance system needs to be shut down for maintenance or upgrades, reasonable efforts should be taken to do so during off hours and for the shortest period of time necessary.

Removal of Security Cameras. Access Control

The Selectboard shall make final decision on the removal of any equipment. Access control will be vested in the Internet Technology Firm that is serving the Town as the System Administrator. They will manage the cameras and access to the footage unless the Selectboard designates a different System Administrator. 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

~~SA s~~elected System Administrators will be responsible for the inspection and monitoring of the cameras. The cameras must be inspected on a ~~monthly~~ daily schedule to ensure the system is functioning properly. The process for a proper inspection will be defined by the Internet Technology 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 vacancy in either role.

Cyber Security

The System 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:

1. Change the system default password as required.
2. Change the system password on a regular basis or when it's suspected that the system has been compromised.
3. Apply software updates regularly as needed for camera system.
4. Limit the number of users and physical access to equipment.
5. 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, such as bathrooms and/or changing rooms. Reasonable efforts will be made to limit any surveillance to Town-owned property and buildings. The cameras are intended to capture activities happening on municipal property, and there is no intention or desire to record anything that may occur on adjacent property.

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

_____
Chair

_____ Vice Chair

_____ Selectboard Member

_____ Selectboard Member

_____ Selectboard Member