City of Findlay Security Camera Policy

Policy: 20240001
Date in Effect: 11/6/2024

Purpose

The City of Findlay "City" strives to maintain a safe environment for the public and all employees; the City is obligated to protect taxpayer-funded property. Therefore, selected areas are equipped with security cameras that are recording at all times.

The purpose of this policy is to establish rules for the use of security cameras, as well as access to live and recorded images. The City's system shall only be used for the protection and safety of citizens, employees, assets, property, and to identify persons breaking the law or violating City policy, including the City's Rules of Conduct.

Scope

This policy covers all employees, including seasonal, temporary, volunteers, and interns, and visitors to City facilities.

Definitions:

Video recording camera: This type of camera has the ability to record images in an area. May be digital or tape recording.

Video Conference Camera: This type of camera is connected to a personal computer. Used to transfer images of videoconference participant. Not a continuously monitored camera and is activated by the user.

Responsibilities

1. **Adding Cameras:**
    a. Departments seeking the addition of security cameras to their facilities/offices shall work with Computer Services to determine camera types and locations for installations to ensure appropriate coverage. Departments may elect to collaborate with the City Police Department to determine areas that should be covered with surveillance equipment. The department's elected official(s) or their appointed representative shall be responsible for final approval of any new camera installations prior to execution of any of these plans.

i. To maintain uniformity, the Computer Services Department will select cameras from a list of approved vendors. All security camera equipment must comply with current City standards and connect to the City's centralized surveillance system.

b. The department adding the camera will be responsible for the cost of purchasing the physical camera and licenses required to connect the camera to the City camera system. Ongoing annual maintenance costs going forward will be paid by Computer Services.

2. **Delegation of Access:**
   a. Each department's elected official or their appointed representative holds the authority to grant final approval regarding who can access security cameras within their assigned areas as well as the level of access. The following shall be considered:
      i. Access shall be granted only when necessary for the user to undertake their duties, and should be granular to allow the minimum access required (e.g., specific cameras, control PTZ, live or playback, etc.).
      ii. Different access methods are listed below, Computer Services can help the granting authority determine which is best for each use case.
         1. Full local client access (Internal Only)
         2. Web client access (Internal Only)
         3. Mobile device access (Internal and External)
         4. Web client access (Internal and External)
   b. Computer Services staff will be responsible for setting appropriate permissions as requested
      i. Permissions should be audited regularly to confirm appropriate access is granted to City users
3. **Maintenance:**
   Computer Services staff is responsible for overseeing all aspects of maintenance for the security camera system.
   a. Regular Inspections:
      i. Conduct periodic inspections of all security cameras to ensure they are operational and positioned correctly.
      ii. Automated reporting should be configured to alert staff of any loss of functionality on security cameras in the system.
      iii. Conduct physical inspections to ensure no physical damage is present and weather strips are in place if outdoors.
   b. Technical Support and Issue Resolution:
      i. Provide technical support for all security camera systems, including addressing hardware, software, and network issues.
      ii. Use a ticketing system to track and resolve reported issues promptly.
   c. Preventive Maintenance:
      i. Develop a preventive maintenance schedule for routine checks, cleaning camera lenses, and updating firmware/software as needed.

ii. Ensure preventive maintenance activities are documented and performed regularly.

d. Camera Replacement
   i. Computer Services staff will be responsible for tracking the age and viability of all City cameras. They will recommend replacement schedules for aging cameras to the appropriate departments for budgeting purposes.

e. System Testing:
   i. Regularly test the functionality of cameras, including key features like motion detection and night vision.
   ii. Verify that camera coverage meets the security needs of each department and adjust as necessary.

4. Data Privacy and Retention:

a. Data Storage:
   i. Security camera footage should be stored securely, with access limited to authorized personnel.
   ii. Storage systems must comply with applicable data protection laws and regulations. Video storage periods must meet or exceed the State of Ohio's records retention standards

b. Data Retention:
   i. Footage will be retained. For example, footage should be retained for a minimum of 30 days unless required for an investigation or legal purposes.
   ii. Establish procedures for securely deleting footage that is no longer needed.

c. Data Access:
   i. Access to stored footage should be logged and monitored to ensure compliance with access policies.
      1. Access logs should be kept for minimum of 30 days
   ii. Procedures for requesting access to footage for investigative or legal purposes should be clearly outlined.

5. Public Disclosure and Exemptions:

a. Security camera footage is generally considered a public record and may be subject to disclosure under the Ohio Public Records Act upon request. However, certain exemptions under the Ohio Revised Code (ORC) may apply, particularly when the footage involves secure areas or sensitive information.
   i. No footage should be released to the general public without an officially approved Ohio Public Records Act request, taking into consideration the potential exemptions listed below.

b. The following types of footage may be exempt from disclosure under the ORC:
   i. Security Records: Footage from areas classified as secure, where releasing the video could compromise the safety or security of public facilities, infrastructure, or operations. This includes, but is not limited to,

footage that reveals security protocols, access controls, or the layout of sensitive areas. This exemption is covered under ORC § 149.433.

ii. Investigative Records: Footage that is part of an ongoing law enforcement investigation or that could reveal investigatory work product, potentially jeopardizing the investigation or endangering individuals involved. This exemption is covered under ORC § 149.43(A)(1)(h).

iii. Critical Infrastructure: Footage that involves the physical or digital security of critical infrastructure, where disclosure could expose vulnerabilities or pose a risk to public safety. This exemption is also covered under ORC § 149.433.

c. Before denying a public records request based on the above exemptions, the footage in question must undergo a thorough review by legal counsel. This review will ensure that the exemption is appropriately applied and that the decision to withhold the footage is legally sound.

i. Legal counsel will consider the nature of the footage, the potential risks associated with its release, and the relevant statutory exemptions under Ohio law. Only after this review can a determination be made to withhold the footage from public disclosure.

d. If footage is withheld, detailed documentation of the legal reasoning for the exemption must be provided. This documentation should include references to the applicable legal provisions under the Ohio Revised Code and a summary of the risks or concerns that justify the denial.

---

6. Training and Awareness:

e. Provide guidelines for training staff on the appropriate use of security cameras and the policies surrounding them.

f. Training Programs:

i. Implement training programs for all staff with access to security cameras, covering proper use, data protection, and compliance with the policy.

ii. Regularly update training programs to reflect any changes in the policy or technology.

g. User Awareness:

i. Ensure that all employees are aware of the security camera policy and understand their responsibilities.

ii. Use signage and communications to inform staff and visitors that security cameras are in use.

Acceptable Use

The installation or removal of a department's security camera must be coordinated with the department head and Information Systems Manager. Departments shall not install cameras for security purposes on their own.

Reasonable efforts shall be made to safeguard the privacy of citizens and employees. Cameras may be installed in locations where employees and the public would not have an expectation of privacy. Examples include, but are not limited to, common areas of the municipal and other City-owned buildings such as entrances, hallways, court rooms, City council chambers, exterior grounds and parking lots. Cameras will not be installed in areas where employees and the public have a reasonable expectation of privacy, such as inside restrooms. Signs may be posted at the entrances to City buildings or other public facilities informing the public and staff that security cameras are in use.

The Mayor, Service-Safety Director, Police Chief and other authorized personnel may monitor and review security camera live feeds and recordings as needed and appropriate to support investigations and/or to enhance public safety. Department heads may monitor and review security camera live feeds and recordings only of their work areas for purposes of public and employee safety. Other employees with a need to access select security cameras will require approval by the department's elected official or their appointed representative. Computer Services personnel will monitor and review security camera live feeds and recording as needed to troubleshoot and support the camera system, software, and staff.

Access to the archived footage for investigating violations of workplace polices and procedures should go through the Human Resources Department. Access to the archived footage for investigating potential criminal activity is restricted to designated police personnel, with approval from the Police Chief.

Prohibited Conduct

No security cameras, videoconference cameras, or other monitoring devices shall be installed or located upon City property without being properly approved and meeting the standards of this policy. Tampering with, or causing damage to City cameras is also prohibited.

Security cameras are not intended to be used for routinely monitoring staff. However, City management may utilize routine security camera recordings in support of disciplinary proceedings against employees, or in a civil suit or other proceeding involving person(s) whose activities are shown on the recording and relate to the proceeding. No City employee shall share or release security camera footage without following the proper channels outlined in this policy.

Confidentiality, privacy, and security issues prohibit the general public from viewing security camera footage that contains personally identifiable information about employees and citizens, or information that reveals or identifies City security measures. If the City receives a request from the general public to inspect security camera footage, the City will respond accordingly to Ohio public records laws and City policy.

A breach of this policy may result in disciplinary action up to and including dismissal. Any employee who becomes aware of any damage to or tampering with a City security camera, unauthorized disclosure of a video recording, and/or a potential privacy breach has a responsibility to immediately inform the Mayor, Service-Safety Director or Human Resources Director.

Mayor: _____

Service-Safety Director: _____

Human Resources Director: _____