USE OF SURVEILLANCE TECHNOLOGY APM

Purpose: City of Madison agencies have identified a wide variety of legitimate business reasons to use surveillance technology. The primary purpose of this policy is to protect the privacy rights of the public and the collective action rights of City employees. This policy insures there is consistency among all City departments in the use of surveillance technology.

"Surveillance Technology" means any software, electronic device, or system utilizing an electronic device, owned by the City or under contract with the City, designed, or primarily intended, to collect, retain, process, or share audio, electronic, visual, location, thermal, biometric, olfactory or other personally identifiable information for the purpose of surveillance. Surveillance technology includes but is not limited to the following: cell site simulators; automatic license plate readers; gunshot detection systems; facial recognition software; gait analysis software; video cameras that record audio or video and can transmit or be remotely accessed; and unmanned aircraft systems equipped with remote video capabilities.

"Surveillance Technology" does not include the following devices, hardware or software:

1. Office hardware, such as televisions, computers, credit card machines, copy machines, telephones and printers, that are widespread in use by the City;
2. Audio/video teleconference systems;
3. City databases and enterprise systems that contain information , including, but not limited to, human resource, permit, license and business records;
4. City databases and enterprise systems that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology, including payroll, accounting, or other fiscal databases;
5. Information technology security systems, including firewalls and other cybersecurity systems;
6. Systems or databases that capture information where the an individual knowingly and voluntarily consented to provide the information, such as applying for a permit, license or reporting an issue;
7. Physical access control systems, employee identification management systems, and other physical control systems;
8. Infrastructure and mechanical control systems, including those that control or manage street lights, traffic lights, or water or sewer functions;
9. Manually-operated technological devices used primarily for internal City and department communications and are not designed to surreptitiously collect surveillance data, such as radios, cell phones, personal communications devices and email systems;
10. Manually-operated, non-wearable, handheld cameras, audio recorders and video recorders that are not designated to be used surreptitiously and whose function is limited to manually capturing and manually downloading video and/or audio recordings;
11. Devices that cannot record or transmit audio or video or be remotely accessed;

12. Computers, software, hardware or devices used in monitoring the work and work-related activities involving City buildings, employees, contractors and volunteers or used in conducting internal investigations involving City employees, contractors and volunteers;
13. Medical equipment and systems used to record, diagnose, treat, or prevent disease or injury and are used and/or kept in the court of providing City services;
14. Parking Ticket Devices;
15. Equipment used on a temporary basis for investigations and in accordance with City policies;
16. Cameras intended to record activities at City facilities in public areas where the public has been notified per this APM;
17. Cameras intended to record activities at City facilities in nonpublic areas;
18. Police department interview rooms, holding cells, and police department internal security audio/video recording systems; and
19. Police department systems/databases, including but not limited to, records/case management systems, Live Scan, Computer Aided Dispatch (CAD).

Responsibilities:

Department of Information Technology (IT)

Whenever IT is informed by a department that the department plans to purchase, contract for, or consult in the use of new surveillance technology, IT shall review said surveillance technology. If IT does not recommend said use or purchase, IT will contact the department and discuss the concerns or issues. If IT recommends the use of the surveillance technology, IT will provide notice to the Mayor of the intent to use said surveillance technology for approval. IT will notify Common Council Leadership (Council President and Vice-President) of the request and recommendation. The Mayor will inform the department and IT if the surveillance technology is not approved. Upon approval by the Mayor, notification of said surveillance technology will be posted on the City's website and placed on file in the Clerk's Office (sensitive surveillance technology and data that is not suitable for public release is excluded from this requirement).

IT shall, in accordance with APM 4-7 (Policy for Procurement and Disposal of Electronic Products) assist agencies in obtaining surveillance technology that meets the agency's technical requirements and complies with the City's enterprise system technological standards and polices.

IT shall manage network connectivity issues, coordinate problem remediation, maintenance and replacement of devices connected to the enterprise camera system. Agencies that have their own IT and/or facilities maintenance staff capable of maintaining camera devices may provide their own maintenance and problem remediation support.

IT shall design, manage and maintain the network infrastructure to support a City-wide enterprise surveillance camera system. IT shall ensure that the enterprise camera system is capable of complying with all Wisconsin Public Records Law for the capturing, retention and timely production of public records.

Departmental Responsibility

Agencies shall not purchase, create or maintain their own independent enterprise surveillance technology without notification to IT. Departments must notify IT of any planned purchase or contract for the use of new surveillance technology at least 90 days prior to said purchase or use, so that IT has ample time to review the request and make a recommendation to the Mayor.

Departments will insure that signage is posted in public entryways to City buildings, providing notice that surveillance technology is in use.

Departments that choose to use surveillance technology must adopt a written policy on said use. Such written policy will be reviewed by IT and upon approval said policy will be referred to the Mayor's office and placed on the agency's webpage. *See attached template*

Agency policies must address the following considerations:

- The circumstances which necessitate the use of surveillance technology;
- The staff member or position responsible for the account management and administration of the surveillance technology;
- The staff member or position responsible for receiving complaints regarding the department's use of surveillance technology;
- The process for determining roles and access to surveillance technology;
- Provision for a regular audit of employee use/access of surveillance technology;
- The process to insure access to surveillance technology is revoked when the employee no longer has a job related need to said access;
- The personnel responsible for training staff and reviewing staff access and use of the surveillance technology;
- Unless otherwise prohibited by law, the Madison Police Department will be provided with immediate access to all data recordings that may constitute evidence of a crime;
- The time period that recorded audio/video will be retained, in accordance with the Department's record retention policy; and
- Procedures for ensuring that records are not destroyed during the pendency of any public records request, investigation or civil/criminal litigation.

Every agency policy shall comply and each use of surveillance technology will comply will all applicable laws.

The department head (or designee) will conduct an annual review of all surveillance technology in use within the department and insure that all policies are up to date. Departments will insure that all new staff receive training regarding the surveillance technology policies and the ethical use of said surveillance technology. The department head (or designee) will conduct audits of staff utilization of surveillance

technology to insure use is in compliance with applicable policies and with this APM. The department head or designee will review any violations of this policy and insure that appropriate action occurs.

Agencies shall be responsible for the costs of procuring and operating surveillance technology they employ. Agencies shall use their budgeted funds to purchase all new camera devices, equipment, licenses, and services required to install and connect (fiber-optics, point-to-point radios, or any other network connectivity technologies) the devices to the enterprise surveillance technology.

It is recognized that exigency may require the acquisition of, purchase of, or contracting for the use of surveillance technology prior to consultation with IT and mayoral approval. In those instances, the department head will notify IT as soon as is feasible.