USE OF SURVEILLANCE TECHNOLOGY APM 3-17

Purpose: City of Madison Departments have identified a wide variety of legitimate business reasons to use Surveillance Technology. The primary purpose of this policy is to insure consistency among all City Departments in the acquisition and the use of Surveillance Technology. Another purpose is to protect the privacy rights of the public and the rights of City employees to associate.

"City-wide Network" means the City's IT infrastructure which is connected using high speed fiber optic connections which allows City employees to share communications, software, hardware devices, and data and information.

"Department" means any agency, department, or division of the City.

"Sensitive Surveillance Technology Information" means any information about Surveillance Technology that public disclosure of would unreasonably expose or endanger City infrastructure; would adversely impact operations of City agencies; or may not be legally disclosed.

"Surveillance Technology" means any hardware, 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 of members of the public 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 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;

Commented [KK1]: Ledell Zellers: "This APM needs work. Some comments/suggestions/questions below…but needs additional attention."

Commented [KK2]: Ledell Zellers: "This is not clear."

Commented [KK3]: Ledell Zellers: "Shouldn't definitions simply refer to ordinance so they don't get out of sync? Doesn't make sense to me to duplicate them with the possibility there may be changes to one and not the other…"

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 electronic data or be remotely accessed, such as vision-stabilizing binoculars or night vision goggles;
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 nonpublic areas;
17. Police Department interview rooms, holding cells, and Police Department internal security audio/video recording systems; and
18. Police Department records/case management systems, Live Scan, Computer Aided Dispatch (CAD).

All Department request to purchase, acquire or contract for the use of new Surveillance Technology that will connect to the City-wide Network will be referred to the Common Council via the budget process or through a resolution. Departments will use the Request to Purchase Surveillance Technology Form to notify the Information Technology ("IT") Department, the Mayor and Common Council Leadership of any request to purchase, acquire or contract for the use of Surveillance Technology that is not connected to the City-wide Network. If the Mayor and Common Council leadership request that a Department notify residents, the Department will work with IT to create an online form for residents to submit feedback and comments. The Department will hold a public meeting if requested by the Mayor or Common Council Leadership.

Commented [KK4]: Ledell Zellers: "The first two sentences duplicate the ordinance. The third sentence seems to conflict with the ordinance which requires notification on website. Perhaps this should be clarified/expanded/explained."

Roles and Responsibilities:

Department of Information Technology

Whenever Information Technology ("IT") is informed that a Department has obtained approval as outlined above to purchase, acquire or contract for the use of new Surveillance Technology, IT will review the technology. IT shall, in accordance with APM 4-7 (Policy for Procurement and Disposal of Electronic Products) and APM 3-20 (Software Acquisition Policy) assist the Department in obtaining Surveillance

Commented [KK5]: Ledell Zellers: "This is referring to the paragraph immediately preceding?"

Technology that meets the Department's technical requirements and complies with the City's Network technological standards and polices.

For the City-wide enterprise camera system, IT shall manage network connectivity issues, coordinate problem remediation, and oversee maintenance and replacement of devices connected to the enterprise camera system. IT shall design, manage and maintain the network infrastructure to support the system. In coordination with IT, Departments that have staff capable of maintaining camera devices may provide their own maintenance and problem remediation support. It will be the responsibility of IT to 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

Each Department will not purchase, acquire or contract for the use of their own independent Surveillance Technology without approval from the Mayor and Common Council through the processes outlined above. When notifying the Mayor and Common Council of the purchase, acquisition or contract for the use of Surveillance Technology, the Department will provide the following information:

1. A description of the Surveillance Technology, its capabilities and the surveillance data or information it will generate;
2. Who in the Department will be the lead individual responsible for the Surveillance Technology;
3. The training protocols the Department will put in place, which shall minimally include appropriate uses of Surveillance Technology and access to data;
4. The intended location and/or deployment of the Surveillance Technology;
5. How and when the Department will use the Surveillance Technology;
6. How the Surveillance Technology will be captured, including whether it will be by real-time or historical data capture;
7. What is the potential fiscal impact of the Surveillance Technology;
8. Whether the Department has agreements with other entities for the use or access of the Surveillance Technology;
9. How the Surveillance Technology access and use will be shared, managed and monitored;
10. Who within the Department will be using the Surveillance Technology;
11. How the Department will monitor staff access to the Surveillance Technology; and
12. How the surveillance data will be stored, retained and deleted.

Commented [KK6]: Ledell Zellers: "The approval process which is the penultimate paragraph on prior page?"

Commented [KK7]: Ledell Zellers: "data/information" instead of technology

Commented [KK8]: Ledell Zellers: "What does this mean?"

Commented [KK9]: Ledell Zellers: "The" instead of what is the

Commented [KK10]: Ledell Zellers: "and/or resulting data/information"

Commented [KK11]: Ledell Zellers: "and audit"

After the Department has received approval for the purchase, acquisition or contracting for the use of Surveillance Technology, the Department will provide notification of said Surveillance Technology on the Department's website, the Surveillance Technology Master List housed on the Information Technology's Surveillance Technologies webpage(s) and place a copy of said notification on file in the Clerk's Office.

In the event a Department has an immediate opportunity to acquire new Surveillance Technology and it is not feasible to obtain prior approval, the Department may do so. The new Surveillance Technology may not be used until the notification and approval process outlined in this APM has been completed.

However, in the event of an exigent situation requiring the urgent acquisition and use of new Surveillance Technology that is not placed on the City Network a Department may acquire and use Surveillance Technology, without prior approval. The Department will apply for approval within 14 days of such exigent circumstances and will follow the formal approval process described above.

If a Department needs to move a camera location on the City-wide enterprise camera system, or needs to additional camera at a new location or the same location, the Department will notify the Mayor and Common Council Leadership and the Alder of the district of the camera location. If the Mayor, Common Council Leadership and Alder request the Department notify residents, the Department will work with IT to create an online form for residents to submit feedback and comments. The Department will hold a public meeting if requested by the Mayor, Common Council Leadership or the Alder of the district where the camera is located.

Departments will insure that signage is posted in public entryways to City buildings, providing notice that Surveillance Camera Technology is in use.

Every Department will adopt a written policy on the use or Surveillance Technology and shall insure the use of Surveillance Technology complies with all applicable laws. Departments will insure that all new staff receive training regarding the Surveillance Technology policies and the appropriate use of said Surveillance Technology. Department polices will be posted on the Department's website, as well as, on the Information Technology's Surveillance Technologies webpage(s) that will house the Master List. Department policies will include at least the following information:

1. The circumstances which necessitate the use of the Surveillance Technology;
2. The training protocols the Department will utilize;
3. The staff member or position responsible for the account management and administration of the Surveillance Technology;
4. The staff member or position responsible for receiving complaints regarding the Department's use of Surveillance Technology;
5. The process for determining roles and access to Surveillance Technology;
6. The process to insure access to Surveillance Technology is revoked when the employee no longer has a job related need to said access;
7. The personnel responsible for training staff and reviewing staff access and use of the Surveillance Technology;
8. Insuring that the Madison Police Department will be provided with immediate access to all data recordings that may constitute evidence of a crime, unless otherwise prohibited by law;
9. The time period that recorded audio and video will be retained, in accordance with the Department's record retention policy;
10. Insuring that the Surveillance Technology may not be used to visually or audibly monitor the interior of private dwellings where a reasonable expectation of privacy exists, absent a court order or other lawful justification; and
11. Procedures for ensuring that records are not destroyed during the pendency of any public records request, investigation or civil or criminal litigation.

Commented [KK12]: Ledell Zellers: "or changes the originally approved use"

Commented [KK13]: Ledell Zellers: "or" instead of "and"

Commented [KK14]: Ledell Zellers: Add section header "Departmental Policies"

Commented [KK15]: Ledell Zellers: "Ensure" instead of "insure"

Commented [KK16]: Ledell Zellers: "Ensure" instead of "insure"

Commented [KK17]: Ledell Zellers: Replace with "The process for providing"

Commented [KK18]: Ledell Zellers: Replace with "The prohibition of using"

Reporting Process

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. The Department Head or designee will conduct annual audits of staff utilization of Surveillance Technology to insure use is in compliance with applicable policies and APMs. The Department Head or designee will review any violations of this policy and insure that appropriate action occurs.

The Department will provide an annual Surveillance Technology Report to the Common Council. The report will include at least the following information:

1. An inventory of current Surveillance Technology and the applicable policies;
2. How the Department has used its Surveillance Technology;
3. How any surveillance data is being shared with other entities;
4. How well surveillance data management protocols are safeguarding individual information; and
5. Whether the Department has received any complaints or concerns about its Surveillance Technology use.

Commented [KK19]: Ledell Zellers: "Ensure" instead of "insure"

Commented [KK20]: Ledell Zellers: "Ensure" instead of "insure"

Commented [KK21]: Ledell Zellers: "Ensure" instead of "insure"

Commented [KK22]: Ledell Zellers: Add "as required in Ord 23.61(5)"

Commented [KK23]: Ledell Zellers: "Again, why repeat this info in the APM…can't the ordinance simply be referenced?"

Commented [KK24]: Ledell Zellers: Add "and resolution of said complaints"

Sensitive Surveillance Technology Information

Whenever a Department uses Sensitive Surveillance Technology Information it is exempt from all requirements of this APM. However, when legally permissible Departments will submit an explanation of why the Sensitive Surveillance Technology Information is considered sensitive to the IT Director, who will notify the Mayor and Common Council Leadership of the exemption.