*****DRAFT *****

USE OF SURVEILLANCE TECHNOLOGY APM

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 protect the privacy rights of the public and the rights of City employees to associate. This policy insures that there is consistency among all City Departments in the acquisition and 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 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;
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).

Roles and Responsibilities:

Surveillance Review Team (SRT)

The SRT will consist of the Common Council Chief of Staff and a designee from each of the following departments: Mayor's Office, Police, Information Technology, City Attorney, Finance, Civil Rights, Metro, Water Utility, and Traffic Engineering.

All Department requests to purchase, contract for, or consult in the use of new surveillance technology will be sent to the Chief Information Officer who will schedule a SRT meeting. If the SRT does not recommend said use or purchase, the SRT designee will contact the Department and discuss the concerns or issues. If the SRT recommends the use of the surveillance technology, the requesting Department will follow the approval process outlined below.

Department of Information Technology

Whenever Information Technology ("IT") is informed that a Department has obtained approval from the Mayor and the Common Council to purchase or contract for the use of, new Surveillance Technology, IT will need to review said Surveillance 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 Technology that meets the Department's technical requirements and complies with the City's network enterprise system 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

Departments will not purchase, create or maintain their own independent Surveillance Technology without approval from the Mayor and Common Council. Departments must notify the SRT of any planned purchase or contract for the use of new Surveillance Technology at least 120 days prior to said purchase or use, so that the department has ample time to follow the approval process outlined in this APM.

After the Mayor and Common Council have approved the purchase or acquisition of the Surveillance Technology, the Department will provide notification of said Surveillance Technology on the Department's website and place a copy of said notification on file in the Clerk's Office. Sensitive Surveillance Technology and data that is not suitable for public release are excluded from this requirement.

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.

Departments will insure that signage is posted in public entryways to City buildings, providing notice that Surveillance Camera 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 the SRT and posted on the Department's webpage.

Department policies must address the following considerations:

- The circumstances which necessitate the use of Surveillance Technology;
- The training protocols the Department will utilize;
- 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;
- 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;
- 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;
- The time period that recorded audio and video will be retained, in accordance with the Department's record retention policy;

- 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
- Procedures for ensuring that records are not destroyed during the pendency of any public records request, investigation or civil or criminal litigation.

Every Department policy shall comply and each use of Surveillance Technology shall 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, utilizing the Surveillance Annual Review Form. Departments will insure that all new staff receive training regarding the Surveillance Technology policies and the appropriate use of said Surveillance Technology. When feasible, 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.

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 doing so, and will follow the formal approval process described above.

<u>Approvals and Reporting</u>

Approval Process

A description of the Surveillance Technology, its capabilities and the surveillance data or information it will generate.

The Department will provide a Surveillance Technology use policy including, which will include the following:

A surveillance technology use policy including, which will include the following:

a) Who is the lead Department responsible for the Surveillance Technology?
b) The training protocols the Department will put in place, which shall minimally include appropriate uses of surveillance technology and access to data;
c) The intended location and/or deployment of the Surveillance Technology;
d) How and when the Department will use the Surveillance Technology;
e) How the Surveillance Technology will be captured, including whether it will be by real-time or historical data capture;
f) Whether there is the potential that any privacy rights affected by the Surveillance Technology;
g) Identification of groups of people on whom this Surveillance Technology may have a disparate impact, and explanation of the Department's public notification plan for each potentially disparately impacted group; whether the surveillance technology potentially has an impact on any minority groups. What is the potential fiscal impact of the surveillance technology;

h) Whether the Department has agreements with other entities for the use or access of the Surveillance Technology;
i) How the Surveillance Technology access and usage will be shared, managed and monitored;
j) Who will be using the Surveillance Technology?
k) How the surveillance data will be stored, retained and deleted.

Reporting Process

Each Department will conduct an annual review of its Surveillance Technology to ensure compliance and will complete an Annual Surveillance Technology Report.

The Annual Surveillance Technology Report will include:

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;
5. Whether the Department has received any complaints or concerns about its Surveillance Technology use;

The SRT shall will work with Departments to get completed reports which will be submitted to the Chief Information Officer for the Annual Report to the Common Council.