DAYTON POLICE DEPARTMENT
GENERAL ORDER
SURVEILLANCE TECHNOLOGY USE

KAMRAN AFZAL – DIRECTOR AND CHIEF OF POLICE

Rev. 10/22

POLICY STATEMENT

Surveillance operations are essential for criminal investigations and information collection required to develop intelligence. However, covert, and clandestine methods may be neither appropriate nor necessary and, if used, can have associated risks. Surveillance is suitable only for those types of investigations where information of comparable investigative value cannot be obtained by other less intrusive means and is permitted only when reasonable suspicion of criminal activity has been established. It is the policy of this agency to employ surveillance methods only where they can be justified in accordance with principles and operational protocols established in this policy.

This policy is to comply with Revised Code of General Ordinance 34.09 through 34.15 regarding the establishment of a process to approve and regulate new law enforcement surveillance technology.

I. DEFINITIONS

A. *Exigent Circumstances:* The Chief of the Dayton Police Department or their designee's good faith belief that there exists an emergency involving imminent danger of death, serious physical injury to any person, or imminent danger of significant property damage, that requires the use of the Surveillance Technology or the information it provides.

B. *Personal Communication Device:* a cellular telephone that has not been modified beyond stock manufacturer capabilities, a personal digital assistant, a wireless capable tablet or similar wireless two-way communications and/or portable Internet accessing devices, whether procured or subsidized by a City entity or personally owned, that is used in the regular course of conducting City business.

C. *Surveillance Technology*: any device or system designed or used or intended to be used to collect, retain, process, or share audio, electronic, visual, location, thermal, olfactory, or similar information associated with, or capable of being associated with, any specific individual or group of specific individuals by the Department.

Examples of surveillance technologies include but are not limited to: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors; facial recognition software; gait analysis software; surveillance enabled or capable light bulbs or light fixtures; social media monitoring software; video cameras that record audio or video and can transmit or be remotely accessed; software designed to integrate or analyze data from surveillance technology, including surveillance target tracking and predictive policing software based on surveillance.

The enumeration of Surveillance Technology examples in this subsection shall not be interpreted as an endorsement or approval of their use by the Department.

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 in widespread use by City departments and used for routine City business and transactions;

2. City databases and enterprise systems that contain information kept in the ordinary course of City business and do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology, including, but not limited to, human resource, permit, license, business records, payroll, accounting, or other fiscal databases;

3. Information technology security systems, including firewalls and other cybersecurity systems;

4. Physical access control systems, employee identification management systems, and other physical control systems;

5. Infrastructure and mechanical control systems, including those that control or manage streetlights, traffic

lights, electrical, natural gas, or water or sewer functions;

6. Manually operated technological devices used primarily for internal City and department communications and are not designed to surreptitiously collect surveillance data, such as radios, Personal Communication Devices and email systems;

7. Manually operated, non-wearable, handheld cameras, audio recorders and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings;

8. Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision equipment;

9. 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;

10. Medical equipment and systems used to record, diagnose, treat, or prevent disease or injury and are used and/or kept in the ordinary course of providing City services;

11. Parking ticket devices;

12. Photo Enforcement Cameras, provided the cameras and the data collected therefrom are used and maintained solely to enforce traffic laws;

13. Police department interview room, holding cell and police department internal security audio / video recording systems;

14. Police department computer aided dispatch (CAD), records / case management Live Scan, booking, Bureau of Motor Vehicles, Ohio Law Enforcement Administrative Database, 9-1-1 and related dispatch operation or emergency services systems.

15. Technology or tools used to investigate specific criminal incidents where such technology or tools are not readily known to the public and for which the effectiveness of the technology or tool would be compromised by disclosure.

16. Any technology that collects information exclusively on or regarding City employees or contractors.

17. Technology or tools used by Dayton Police Officers solely while they are working as part of an established federal task force.

II. PURPOSE

The purpose and intent of the policy is to formally adopt a process for citizen notification and review of new law enforcement Surveillance Technology before such technology is acquired or used, and to ensure that approved technology is used in accordance with policies that protect citizens' privacy, civil rights, and civil liberties. This process is not intended to discourage the adoption of Surveillance Technology that will make Dayton's citizens more secure. Rather, this policy is intended to:

1. Establish safeguards, including transparency, oversight, approval, and accountability measures to protect civil rights and civil liberties before new Surveillance Technology is acquired or deployed by the Department;

2. Ensure that a public hearing is held before any such new technology is acquired or used by the Department;

3. Establish data reporting measures regarding the use and implementation of Surveillance Technology by the Department;

4. Improve public confidence in law enforcement and new technology and equipment that is approved for use; and

5. Provide mechanisms for continued oversight and annual evaluation.

III. AUTHORIZED USE: The uses that are authorized, and the rules and processes required prior to and associated with such use.

A. Personnel will deploy Surveillance Technology only after receiving training for that technology and for law enforcement purposes only.

IV. DATA COLLECTION: The information that can be collected by the Surveillance Technology, including "open source" data.

A. Only data from Surveillance Technology and open-source data that is necessary for law enforcement purposes, such as gathering evidence, public safety purposes (crowd management, traffic control), or assisting in criminal investigations will be gathered and stored.

V. DATA ACCESS: The category of individual who can access or use the collected information, and the rules and processes required prior to access or use of the information.

A. The following individuals are eligible to view and analyze data collected from surveillance technologies:

1. Senior Command Staff

2. Lieutenants who directly oversee the use of the Surveillance Technology

3. Sergeants who supervise those involved in viewing and analyzing the data collected

4. Officers and detectives who are analyzing the data collected for dissemination to other sworn personnel for law enforcement purposes

VI. DATA PROTECTION: The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms. Nothing in this subsection shall be construed to require the disclosure of information that could reveal vulnerabilities to, or otherwise increase the potential for an attack on an information technology system of the City.

A. Data gathered from the use of Surveillance Technology will be protected in accordance with General Order 1.01-7, Management Information System / KRONOS Timekeeping / Data Security.

VII. DATA RETENTION: The time period, if any, for which information collected by the Surveillance Technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period.

A. Data will be categorized and kept as outlined in the City of Dayton Records Retention Policy.

VIII. MOVING OR DEPLOYMENT OF FIXED SURVEILLANCE TECHNOLOGY

A. Whenever fixed Surveillance Technology is moved or deployed, the Department shall provide notice of the location of the Surveillance Technology with coordination with the Department of Public Affairs and the Police Information Specialist. The Department will attempt to provide notice to Public Affairs as soon as practicable, but at a minimum will require posting the notice on the City of Dayton's website and providing e-mail notice to those that request such notice from the Department of Public Affairs within 72 hours of deploying the Surveillance Technology. The Department will also provide notice through social media. Such notice will not be provided if the Surveillance Technology is being used to investigate specific criminal incidents or the disclosure would otherwise impair a police investigation.

B. Surveillance Technology will only be moved or deployed if it is recommended in a neighborhood Safety Plan and is requested by that neighborhood, or the neighborhoods affected.

IX. PUBLIC ACCESS

A. Requests for information gathered through the use of Surveillance Technology will be handled in accordance with General Order 1.10-8, Public Access to Agency Records.

X. THIRD PARTY SHARING

A. Information gathered from Surveillance Technology will only be shared with other agencies for law enforcement purposes.

XI. TRAINING

A. Officers will receive training on the proper use of the technology before it is deployed

XII. AUDITING AND OVERSIGHT

A. The Inspections and Audits Bureau will conduct a yearly audit of all technology used by the Department to ensure compliance with this policy.

XIII. USE OF UNAPPROVED TECHNOLOGY DURING EXIGENT CIRCUMSTANCES

A. The Chief of Police or their designee may authorize the Department's temporary acquisition or temporary use of Surveillance Technology in exigent circumstances without following the provisions of this Oversight Ordinance before that acquisition or use. If the Department acquires or uses surveillance technology pursuant to this Section, the Department shall:

1. Use the Surveillance Technology to solely respond to the exigent circumstance;

2. Cease using the surveillance technology within thirty (30) days or when the exigent circumstance ends, whichever is sooner. All use must end when the exigent circumstances end;

3. Only keep and maintain data related to the exigent circumstance and dispose of any data that is not relevant to an ongoing investigation;

4. Within thirty (30) days after the end of the exigent circumstances submit a report to the City Manager to be shared with the Commissioners. The report must explain the exigent circumstances, why the technology or equipment was needed to address the exigent circumstances, how the exigent circumstances prevented the Department from following the approval process in this ordinance and describe how the technology or equipment was used. This report shall be promptly posted on the City's website and shall be promptly emailed to all individuals that have filled out a request for notice of the reports within the Department of Public Affairs.

XIV. ANNUAL SURVEILLANCE REPORT

A. The Strategic Planning Bureau Commander will be responsible to complete the Annual Surveillance Report to the City Commission by the end of each fiscal year. It will include the following mandatory items:

1. A general description of how the Surveillance Technology was used, including general locations and neighborhoods where technology or equipment was deployed;

2. A general description of whether and how often data acquired through the use of the Surveillance Technology was shared with outside entities, the type(s) of data and general justification for the disclosure(s);

3. A summary of community complaints about the Surveillance Technology item;

4. The results of any internal audits required by the Surveillance Use Policy and information about violations of the Surveillance Technology Use policy;

5. Information including crime statistics, where applicable, that help the Commission assess whether the Surveillance Technology has been effective at achieving its identified purposes;

6. An analysis of any discriminatory or other adverse impacts the use of the surveillance technology may have had on the public's civil rights and civil liberties, including but not limited to those guaranteed by the First, Fourth, and Fourteenth Amendments to the United States Constitution and the Ohio Constitution; and

7. Total costs, to the extent possible, including personnel, maintenance, and other ongoing costs, for the Surveillance Technology and anticipated funding for the technology as needed; and

8. Any requested modifications to the Surveillance Technology Use Policy applicable to the item; and

9. Aggregate information concerning technology or tools exempted pursuant to Revised Code of General Ordinances §34.10(5)(a)(15).

XV. SURVEILLANCE IMPACT REPORT

A. The Strategic Planning Bureau Commander will be responsible to complete the Surveillance Impact Report. It will include the following mandatory items:

1. Information describing the Surveillance Technology and how it works;

2. Information on the proposed purpose(s) and use(s) for the Surveillance Technology; along with any existing independent evaluations demonstrating that the Surveillance Technology can help achieve that purpose;

3. If applicable, the location(s) where it may be deployed and crime statistics for such location(s);

4. The known fiscal costs for the Surveillance Technology, including initial purchase, personnel and other known ongoing costs, and any current or potential sources of funding;

5. A description of any possible adverse impacts the use of the Surveillance Technology may have on civil rights and liberties, and

   a. The safeguards that will be implemented to prevent these impacts; and
   b. The potential uses of the Surveillance Technology that will be expressly prohibited.

6. A presentation of the surveillance technology will be presented to presidents from community groups that may be impacted by the technology. A description of the technology and a survey will be sent out in the Patrol Operations District newsletters. Any comments or input from the community groups will be included in the Surveillance Impact Report. A separate presentation will be made to the neighborhood groups that will be directly impact by the technology.

   The Strategic Planning Bureau will coordinate with the Community Engagement Officers for all community engagement activities. The presentations will be given by Community Engagement Officers, Dayton Police personnel familiar with the technology, and/or vendors that provide the technology. Any questions or concerns about the technology will be addressed by those giving the presentation.

Groups to be contacted include:

- College Hill Neighborhood Association
- Dayton View Historic Association
- Dayton View Triangle Neighborhood Association
- Fairview Neighborhood Association
- Five Oaks Neighborhood Association
- Greenwich Village Neighborhood Association
- Hillview Neighborhood Association
- Jane Reece Neighborhood Association
- McPherson Town Historic Society
- Northern Hills Neighborhood Association
- Northwest Priority Board
- Riverdale Neighborhood Association
- Salem Avenue Business Association
- Sandalwood Park Neighborhood Association
- Carillon Business Association
- Carillon Civic Council
- Edgemont Neighborhood Coalition
- Madden Hills Neighborhood Association
- Pineview Neighborhood Association
- Residence Park Neighborhood Association
- Southwest Priority Board
- Westwood Collaborative Network
- Wright-Dunbar Village Neighborhood Association
- Wayne Avenue Twin Towers Association
- Twin Towers Neighborhood Association
- Old North Dayton Neighborhood Association
- Greater Old North Dayton Business Association
- Walnut Hills Neighborhood Association
- East End Community Services
- Forest Ridge Neighborhood Association
- Burkhardt Springfield Neighborhood Association
- Huffman Historical Neighborhood Association
- St. Anne's Hill Neighborhood Association
- Walnut Hills Neighborhood Association
- Belmont Business Association
- Gander Road Neighborhood Association
- Belmont/Hearthstone Neighborhood Association
- McCook Field Neighborhood Association
- South Park Neighborhood Association
- Linden Heights Neighborhood Association
- Patterson Park Neighborhood Association
- Dayton Unit NAACP
- Latino Connection

7. Whether use or maintenance of the Surveillance Technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis.