**City of Somerville Surveillance Technology Use Policy**

This Surveillance Technology Use Policy (the "Policy") is issued on _____ (the "Effective Date") by the Mayor of the City of Somerville (the "City") pursuant to Chapter 10 Article III, Section 10.64 of the Somerville Code of Ordinances (the "Ordinance"). The Ordinance provides for the regulation of the City's use or acquisition of Surveillance Technology for the collection, use, and retention of Surveillance Data as defined in Section 10.62 of the Ordinance. Any City Department Head, as defined below, whose department uses or anticipates acquiring or using Surveillance Technology or Surveillance Data, is required to comply with the Ordinance and this Policy. The goal of this Policy is to balance the capacity of Surveillance Technology to improve the delivery of City services with the importance of maintaining individual(s)' civil rights and civil liberties.

## I. Definitions

All capitalized terms in this Policy shall have the meaning given to them in the Ordinance with the exception of the below-defined terms.

A. **Department Head** shall mean the Department Head of any City department which uses or anticipates acquiring or using Surveillance Technology or Surveillance Data.
B. **Compliance Officer** shall mean a person assigned by a Department Head to keep and maintain records on the acquisition and use of Surveillance Technology or Surveillance Data by that City department, including records on access to Surveillance Data, to ensure that the requirements of the Ordinance and this Policy are followed.

## II. Oversight

The Department Head of each City department which currently possesses, uses or anticipates seeking to acquire or use Surveillance Technology shall submit to the Mayor the name of a designated Compliance Officer assigned by the Department Head to keep and maintain records on the acquisition and use of Surveillance Technology or Surveillance Data by that City department, including records on access to Surveillance Data to ensure that the requirements of the Ordinance and this Policy are followed.

The Department Head or Compliance Officer for that City department shall be responsible for internal record keeping on the acquisition and use of Surveillance Technology or Surveillance Data by that City department, including records on access to Surveillance Data, to ensure compliance with the Ordinance and this Policy.

The name and contact information for each Compliance Officer, and the department they represent, shall be made publicly available on the City's website.

### 1. Process for Approval and Authorizing Use of Surveillance Technology and Surveillance Data

A. The Department Head of any department that uses, or proposes to acquire or use, Surveillance Technology or Surveillance Data, shall submit to the Mayor the following documents required by the Ordinance:

i. **Surveillance Technology Impact Report(s)** (Ordinance Section 10.65), in the form provided in Appendix A attached hereto, submitted for each proposed acquisition, or use of Surveillance Technology; and, if approved by the Mayor's office, submitted to the City Council for approval.
ii. **Annual Surveillance Report(s)** (Ordinance Section 10.66), in the form provided in Appendix B attached hereto, submitted annually by the Mayor to the City Council covering the prior

calendar year. The first such report, describing all existing Surveillance Technologies and Surveillance Data is due to the City Council 12 months after the effective date of the ordinance. Thereafter, the report will be due to the City Council by May 31 of each year. The annual report shall note the department's Compliance Officer and shall include a disclosure of any agreements made in the previous year with any non-city entities that may include acquiring, sharing, or otherwise using surveillance technology or the surveillance data it provides (Ordinance Section 10.66(b)(9)).

iii. **Technology-Specific Surveillance Use Policy(ies)** (Ordinance Section 10.65), in the form provided in Appendix C attached hereto, submitted for each proposed acquisition or use of Surveillance Technology not already covered under this Policy, and, if approved by the Mayor's office, submitted to the City Council for approval. All Technology-Specific Surveillance Use Policies shall be consistent with the provisions set forth in this Policy as it may be amended from time to time. To the extent there is a conflict between this Policy and a Technology-Specific Surveillance Use Policy, this Policy shall govern.

B. When providing any of the above reports, a Department Head should pay particular attention to the impacts the use of the Surveillance Technology has on marginalized communities in the City, including, but, not limited to, communities of color. For any disparity that exists, the Department Head shall explain their understanding as to why the disparity exists and how the Department Head intends to address the disparity.

C. A Surveillance Technology Impact Report and, where applicable, a Technology-Specific Use Policy approved by City Council shall be an accurate documentation of the scope of the approved use of the particular Surveillance Technology.

D. If any employee, agent, or contractor of any City department becomes aware of any inaccuracies concerning the use of Surveillance Technology or Surveillance Data that is collected by a department's Surveillance Technology other than as outlined in that City department's Surveillance Technology Impact Report for that technology, that employee, agent, or contractor is required to immediately report the collection of such Surveillance Data or use of such Surveillance Technology to the department's Compliance Officer, the Department Head, the Mayor, the City Solicitor, or the Personnel Director.

E. City Departments may seek, but may not accept, funds for Surveillance Technology without approval from the City Council, provided that the City shall notify the City Council of the funding application at the time it is submitted, and shall include in this notification the deadline of the funding opportunity and details regarding the nature of the surveillance technology for which funding is sought, pursuant to Ordinance Section 10.65.

F. City Departments may not acquire, use, or enter into an agreement to acquire, share or otherwise use, Surveillance Technology or Surveillance Data without prior approval from the City Council, pursuant to Ordinance Section 10.65(a), unless exempted or excepted from the requirements pursuant to Section 10.63.

2. **Permissible Purposes and Authorized Uses for Surveillance Technology in All City Departments**

A. The Surveillance Technology Impact Report for each proposed Surveillance Technology shall indicate the purpose(s) the Surveillance Technology will be used for. Examples of purposes that the City considers to be generally consistent with this Policy include but are not limited to:

i. Identifying and preventing threats to persons and property and preventing injury to

persons or significant damage to property;

ii. Identifying, apprehending, and prosecuting criminal offenders;
iii. Gathering evidence of violations of any law in criminal, civil, and administrative proceedings;
iv. Providing information to emergency personnel;
v. Documenting and improving performance of City employees;
vi. Executing financial transactions between the City and any individual engaged in a financial transaction with the City;
vii. Preventing waste, fraud, and abuse of City resources;
viii. Maintaining the safety and security of City employees, students, customers, and City-owned or controlled buildings and property;
ix. Enforcing obligations to the City;
x. Operating vehicles for City business;
xi. Analyzing and managing service delivery;
xii. Communicating among City employees, with citizens, or with third parties; and
xiii. Surveying and gathering feedback from constituents.

B. The use of any Surveillance Technology by the City is subject to Mayoral and City Council approval as provided in the Ordinance Section 10.65 and this Policy. The Mayor and the City Council may approve the use of any Surveillance Technology for a purpose not listed herein, provided that the purpose is disclosed in the Surveillance Technology Impact Report and, if applicable, Technology-Specific Use Policy, submitted for approval; and provided, further that such purpose and use is consistent with this Policy.

C. Use of any Surveillance Technology for any purpose not permitted by the Ordinance is prohibited.

D. Use of Surveillance Technology for the purpose of monitoring people on the basis of a) protected First Amendment activity or association or b) any protected class including race or ethnicity, is strictly prohibited.

3. **Data Collection.**

Surveillance Technology produces Surveillance Data upon which the City relies for governmental functions. It is the policy of the City to ensure that the Surveillance Technology it uses collects no more Surveillance Data than is necessary to achieve the specific, authorized purposes of that particular Surveillance Technology, and that any such Surveillance Data is accurate and up to date. It is the policy of the City to ensure that any and all Surveillance Data is collected for specified, explicit, and authorized purposes, and is not to be further processed in a manner incompatible with those purposes.

4. **Data Access.**

City employees may only have access to Surveillance Data when such access is necessary for their official duties. The Department Head or Compliance Officer of each City department shall report to the Information Technology Department ("ITD"), the Mayor and the City Solicitor, the name of each employee, contractor, or other agent that requires access to Surveillance Data. The Department Head or Compliance Officer shall state the specific Surveillance Data to which each individual may have access. The City may, at any time, with or without notice to the individual, terminate any individual's access to Surveillance Technology or Surveillance Data.

To the extent technically possible, the City shall create an automated record each time Surveillance Data is accessed, including the time and date and, if possible, the reason for the access.

5. **Data Protection.**

No Surveillance Data shall be stored, accessed, or transmitted without proper encryption, access and password controls, and access-oversight approved by the City's Chief Information Officer or their designee in ITD. Each City department's Compliance Officer shall complete and submit to ITD a list of each type of Surveillance Technology currently used by that department, the Surveillance data it collects, the staff who have access to the Surveillance Data, and the purpose for which it is used as required under Section II. 2(A). ITD shall ensure that proper procedures are in place to protect all Surveillance Data. In the event that any department is, in the judgment of ITD, unable to implement the security measures necessary to adequately protect Surveillance Data, ITD shall immediately contact the Mayor and the City Solicitor and propose additional measures to protect Surveillance Data from inadvertent or unauthorized disclosure.

6. **Data Retention.**

Surveillance Data shall not be maintained any longer than is necessary to achieve its approved purpose(s), provided that the City shall retain Surveillance Data for the periods required by the Massachusetts Public Records Law, G.L. c. 66, § 10, the Massachusetts Municipal Records Retention Schedule, or any other applicable laws or regulations.

Exceptions to the Massachusetts Municipal Records Retention Schedule may be requested from the Commonwealth by the City Solicitor at the request of a Department Head as follows:

A. A Department Head may seek exceptions for a particular type of Surveillance Data by seeking the exception explicitly in a Surveillance Technology Impact Report or Technology-Specific Surveillance Use Policy; or
B. A Department Head may seek an exception for a particular type of Surveillance Data from the Mayor on a case-by-case basis.
C. All exceptions and the reasons therefor shall be included in a department's Annual Surveillance Report.

7. **Public and Third-Party Access.**

The City shall comply with its obligations pursuant to the Massachusetts Public Records Law, (G. L. c. 4, § 7 cl. 26, and G. L. c. 66, § 10 *et seq*.) and any other applicable law, regulation, or order of a court or state or federal administrative agency of competent jurisdiction that requires the disclosure of particular Surveillance Data.

The City's intent is to make as much information as possible available to the public without compromising the privacy of any Identifiable Individual(s), as defined in Section 10.62 of the Ordinance. The City shall, to the extent possible and permitted in accordance with applicable laws and regulations, anonymize, aggregate, and/or geomask Surveillance Data where necessary to protect the privacy of Identifiable Individuals. While some data may not on its own reveal the personal information of Identifiable Individuals, when combined with other data it may reveal information that would otherwise be exempt from disclosure by law. In the event that a City employee suspects that the release of data would present such a risk, the employee shall report that risk to the Department Head or the Compliance Officer for that employee's department and the Department Head or the Compliance Officer shall contact the Mayor and City Solicitor requesting a legal opinion from the City Solicitor as to whether the data is exempt from disclosure under the Public Records Law or other applicable law or regulation.

Surveillance Data may only be accessed by authorized City employees, as described in Section II. 4, and may only be distributed to third parties in accordance with this section of this Policy. However, any department may share Surveillance Data with the Police Department under Exigent Circumstances.

8. **Training.**

Upon beginning employment or within a reasonable time after commencing employment, any City employee or City contractor who will be involved in the collection of Surveillance Data or use of Surveillance Technology shall be given a copy of the Surveillance Ordinance and this Policy for their review and shall be trained by their Department Head, supervisor, or other appropriate person assigned to conduct such trainings in ensuring that the activities to be performed by that staff or contractor comply with the Surveillance Ordinance and this Policy.

9. **Use of Surveillance Technology in Exigent Circumstances**

The Police Department and the Fire Department may temporarily acquire or use Surveillance Technology in Exigent Circumstances, provided that, within 90 days following the end of those Exigent Circumstances (unless the 90-day deadline is extended pursuant to the ordinance), any such acquisition or use is reported and a Surveillance Technology Impact Report, and, if necessary, a technology-specific surveillance use policy regarding that surveillance technology is submitted to the City Council; and the surveillance technology is described in the next Annual Surveillance Report submitted to the City Council pursuant to Section 10.63(c) of the Ordinance following the end of those Exigent Circumstances. The Chief of Police may, pursuant to Section 10.63(c)(3), redact any public documents submitted under this Ordinance to the extent required to comply with an order by a court of competent jurisdiction, or to exclude information that, in the reasonable discretion of the Chief of Police, if disclosed, would materially jeopardize an ongoing investigation or otherwise represent a significant risk to public safety and security provided, however, that any information redacted pursuant to this paragraph will be released in the next annual surveillance report following the point at which the reason for such redaction no longer exists.

10. **Use of Surveillance Technology Requiring a Warrant**

The Somerville Police Department shall comply with all applicable laws relative to obtaining a warrant or other court-ordered permission prior to using Surveillance Technology or collecting Surveillance Data; and this policy shall not be interpreted to authorize any use of Surveillance Technology or Surveillance Data absent such warrant or court-ordered permission otherwise required by law. For each Surveillance Technology, information regarding when a warrant is required will be included in the Surveillance Technology Impact Report and, if applicable, Technology-Specific Use Policy.

## III. Video Surveillance Technology, Data and Use by the Police Department

It is the purpose of this section to provide general procedures for video surveillance operations conducted by the Somerville Police Department ("SPD"), to establish control processes and procedures to ensure the protection of individuals' civil rights, and to ensure the efficiency and the effectiveness of SPD video surveillance operations. All such operations conducted pursuant to this section shall be in compliance with the Ordinance and this Policy.

The City provides, operates and maintains video surveillance equipment in an attempt to create a safe and secure environment as well as to protect the health, safety and welfare of all those who live, work, visit and transact business within the City. Video Surveillance operations are essential for crime prevention, scene reconstruction and evidence gathering. It is a key resource which aids the Somerville Police and other municipal officials to secure vulnerable sites by producing real time views of both crime scenes and emergency scenes and by allowing Somerville Police command staff and senior municipal city personnel to manage the City's response in an efficient and timely manner.

### 1. Video Surveillance Equipment Location

Video surveillance equipment is located in publicly disclosed locations throughout the City at the direction of the Chief of Police to assist the Somerville Police Department in detecting and deterring crime and acts of terrorism, safeguarding against potential threats to Homeland Security, managing emergency response situations (including

natural and manmade disasters) and assisting other City Officials with the provision of municipal services. The Department anticipates that there are times when it will be deemed necessary for video surveillance equipment to be placed in undisclosed locations. Video surveillance equipment that is placed in an undisclosed location will be used on a temporary basis for investigations where information of comparable investigative value cannot be obtained by other less intrusive means. Such video surveillance equipment shall only be permitted to be placed in undisclosed locations when:

A. Exigent circumstances exist.
B. Reasonable suspicion of criminal activity has been established.
C. A lawfully issued search warrant has been obtained.
D. The Chief of Police determines that compelling circumstances in the public's interest warrants use of certain technology.

It is the policy of the Somerville Police Department to employ surveillance methods in accordance with principles and operational protocols established in the Ordinance and this Policy.

**2. Procedure**

A. The Somerville Police Department by and through its Chief of Police is solely responsible for the day-to-day operation and management of the City's Video Surveillance System including:

I. Storage
II. Maintenance and access
III. Reproduction of the monitored images
IV. The maintenance of evidentiary chains of custody for civil and criminal court actions

B. It shall be the responsibility of the Chief of Police to assign Somerville Police personnel to operate the Video Surveillance System, including but not limited to:

I. Monitoring the camera feeds
II. Managing the inventory control
III. Managing access to the camera feeds
IV. Reproducing and distributing of any electronic media (i.e., CDs, DVDs)
V. Ensuring the chain of custody of such imaging for the evidentiary purposes in civil and criminal court actions
VI. Archiving the recorded information in accordance with the provisions of established policy

C. It shall be the responsibility of the Chief of Police to ensure that the Video Surveillance System is operated within the guidelines of the Ordinance, this Policy, and any applicable intergovernmental agreements, and in accordance with all other department policies, rules and regulations.

D. The Chief of Police shall enforce the Video Surveillance Regulations and shall act as the Department Head for all disciplinary and enforcement actions for violations of these Surveillance Regulations by Somerville Police Personnel.

E. The Chief of Police shall secure any licenses or other agreements to install each camera. The Chief of Police shall monitor the status of each license or other agreement.

**3. The Video Surveillance System**

A. Video surveillance equipment shall consist of City-owned video cameras along with Homeland Security video cameras. The particular type of cameras installed at a location shall be determined by and at the sole discretion of

the Chief of Police or their designee, in coordination with their Command Staff and other governmental agencies, if applicable. The Video Surveillance System shall be accessed remotely through a web- based virtual private network (VPN) connection. The Chief of Police shall limit access to authorized users only.

B. Camera Markings: Except for cameras operated on a temporary basis pursuant to this Policy, cameras shall be marked in a conspicuous manner prior to installation and operation. The City of Somerville Police Department logo shall be affixed to the pole so as to inform the general public that the camera is monitoring and recording. The absence or lack of markings shall not affect the ability of the city or any other agency or person to use the images obtained by any particular monitoring device.

C. Camera Log: The Administrative Captain shall create and maintain a Camera Log of all cameras that are placed in service. The Camera Log shall document when each camera was originally placed into service and shall document each occasion any such camera was taken out of service for maintenance and/or repair. This Camera Log shall also document the date and time each camera was visually inspected (see below).

D. Monthly Visual Inspection: The Administrative Captain shall designate an individual to be responsible to conduct a visual inspection of each camera on a monthly basis and shall document the visual condition of each camera, the condition of the Somerville Police Department markings, and the condition of any signage and lighting in the area of the camera. An entry of each inspection shall be entered into the Camera Log. A notation shall be made in the log that each camera continues to be marked in a conspicuous manner so as to notify the public of its operation.

E. No Sound Recordings: The cameras record images only and do not capture or record sound.

F. No Fake Cameras: Each camera installed is an authentic camera capable of surveillance and recording images. No fake cameras will be installed for any purpose.

**4. Operation of Video Surveillance System**

A. The Video Surveillance System shall be operational twenty-four (24) hours a day, seven (7) days a week. Each camera is designed to transmit its signal wirelessly to a Digital Video Recorder ("DVR") which is located within the Somerville Police Department. The primary monitoring devices shall be located in the office of the Officer in Charge located on the first floor of Police Headquarters. The Officer in Charge, their designee and authorized department personnel are allowed to monitor the feed from the video cameras.

**5. Use Restrictions**

A. The Department operates the Video Surveillance System on behalf of the City of Somerville, to aid in the prevention of incidents of terrorism, suppression of crime, public safety concerns, quality of life issues, municipal research and to aid City officials and the Somerville Police Department in managing their respective missions. Each video surveillance technology shall be used in accordance with the corresponding Surveillance Technology Impact Report.

B. The Video Surveillance System shall be used to view only what is in the general public's view. Monitoring anything that would be deemed an invasion of privacy is prohibited. For purposes of this policy, public view is defined as anything that may be viewed from a vantage point that is accessible to the general public where an individual would not have a reasonable expectation of privacy. As an example, a citizen may have a reasonable expectation of privacy in the interior of their home where they could not be viewed from a public area with normal sight.

C. Any mechanically enhanced view into private property where there is a reasonable expectation of privacy is prohibited. Exceptions to this prohibition may only exist in the case of a search warrant, court order, or where

exigent circumstances are present pursuant to the Ordinance. In the event that a camera is utilized for one of the listed exigencies, a complete narrative shall be filed in an Incident and/or Arrest Report documenting the reason(s) the camera was used for this purpose. A copy of the report shall be forwarded to the Chief of Police for their review.

Nothing in this section shall prohibit the use of a camera's pan-tilt-zoom capacity in compliance with this section and the Ordinance.

**6. Maintenance of the Video Surveillance System**

A. Inventory: The Somerville Police shall retain an updated list of all cameras, their locations and specifications.

B. Maintenance: The Somerville Police will retain a Camera Log documenting the inspections of each camera and the service and/or repairs to each camera.

**7. Organization and Personnel**

A. The Chief of Police, or their designee, is responsible for the day-to-day management and operation of surveillance equipment. The Police Chief shall assign the personnel responsible for the management of its inventory and its maintenance. The Officer in Charge of each Patrol Shift, or their designee, shall be directly responsible for the operation, manipulation and monitoring of Video Surveillance during their shift until their replacement has logged into the system.

B. Training: The Chief of Police, or their designee, shall ensure that all department personnel successfully complete training as required by the Ordinance and this Policy, and training which the Chief of Police deems necessary to successfully operate and monitor Video Surveillance Equipment.

C. Superior Officers and Detectives shall receive training in the operation of the system, including but not limited to, logging on, angle manipulation (pan, tilt, zoom), and retrieving archive video. Patrol Officers shall receive training in the location of all cameras and familiarization with the overall system.

**8. Administrative Captain Duties and Responsibilities**

A. All requests for copies of recorded images from the Video Surveillance System by police department or court personnel (e.g., prosecutors, probation officers) shall be made to the Administrative Captain or their designee by completing and submitting a Video Surveillance Request Form.

B. To facilitate requests made by police officers or court personnel as outlined above, the Administrative Captain or their designee shall follow the procedures as outlined below.

C. The Administrative Captain or their designee shall be responsible for the creation and proper upkeep of all maintenance and inventory logs for the operation of the Video Surveillance System.

D. The Administrative Captain or their designee shall act as the principal liaison with other federal, state, law enforcement and municipal agencies to ensure the execution and delivery of any interagency or inter-municipal agreements which may be required for the operation of Video Surveillance and for any interagency or inter-municipal coordination efforts.

E. The Administrative Captain or their designee shall create, keep and maintain the Image Log noting the Property Number, Arrest and/or Incident Number, Date of Request, Date of Recording and Request Form Control Number. The Image Log maintains a list of those image recordings requested in civil matters pursuant to either subpoena or public records requests pursuant to M.G.L. Chapter 66 Section 10 as well as requests for tapes made in the course

of conducting criminal investigations. [83.2.2]

**9. Data Storage**

A. The Video Surveillance System shall store all recorded images from every camera for a period of thirty (30) days. The System shall be configured to automatically purge and write over any images at the end of this 30-day period.

**10. Reproduction (Archive Video)**

A. The Somerville Police will reproduce such images pursuant to the Public Records Law of Massachusetts; M.G.L. c. 66 Section 10. The Somerville Police will also reproduce images pursuant to normal police procedures for investigations and the handling of evidence.

B. Any private citizen (other than court personnel) requesting a copy of any portion of a Surveillance Recording shall make their request in writing by completing the DVD Image request form or emailing videorequests@police.somerville.ma.us and forwarding it to the Administrative Captain. In the alternative, such a request can be sent directly to the Records Access Officer in the City of Somerville who will provide a response to this request. The Administrative Captain shall submit said form to the City of Somerville Law Department for final approval.

C. Upon receiving a DVD Image request form, and receiving authorization from the City of Somerville Law Department, the Administrative Captain or their designee shall make two (2) copies of each requested image. One copy is to be produced and submitted to the requesting party. The second copy is to be kept together with the Image Log.

D. Any requests for archive video by police and/or court personnel shall be made directly to the Administrative Captain by utilization of a DVD Image request form. The Administrative Captain or their designee shall make two (2) copies of each requested image. One copy is to be produced and submitted to the requesting officer/investigator/assistant district attorney. The second copy is to be kept together with the Image Log.

E. All CDs for private citizens as well as for evidentiary purposes shall contain a ReadMe File with instructions for downloading.

F. For quick access, a Video Investigative File may be created at the special request of the investigating officer to share between law enforcement agencies. This type of image Video Investigative File may not be used for evidentiary purposes.

**11. Retention**

A. The Somerville Police shall maintain one (1) copy of all recordings and requests for recordings in a manner consistent with the Somerville Police Department rules and regulations, its evidentiary policies and in such a manner so as to be consistent with maintaining the chain of custody for evidentiary materials.

B. The Somerville Police shall retain all images/recordings pursuant to the Massachusetts Public Records Laws. In the event that a reproduced image or recording is subject to both the Somerville Police Evidentiary Policies and the Massachusetts Public Record Laws, the Somerville Police Department shall retain the reproduced images/recordings in a manner consistent with both policies. In the event the Somerville Police Evidence Policy and the Massachusetts Public Record Laws conflict as to the duration of retention, the reproduced images/recording shall be held in accordance with the longer required duration.

IV. **Amendments.**

This Policy may be amended from time to time by the Mayor, provided that any proposed amendment shall be submitted to the City Council for approval.

**APPENDIX A: SURVEILLANCE TECHNOLOGY IMPACT REPORT**

| | |
|---|---|
| **Department or Division:** | |
| **Compliance Officer (name and position):** | |
| **Submitted by:** | |
| **Date:** | |
| **Surveillance Technology:** | |

Please identify the purpose(s) of the proposed surveillance technology. Check all that apply.

- ☐ Identifying and preventing threats to persons and property and preventing injury to persons or significant damage to property
- ☐ Identifying, apprehending, and prosecuting criminal offenders
- ☐ Gathering evidence of violations of any law in criminal, civil, and administrative proceedings
- ☐ Providing information to emergency personnel
- ☐ Documenting and improving performance of City employees
- ☐ Executing financial transactions between the City and any individual engaged in a financial transaction with the City
- ☐ Preventing waste, fraud, and abuse of City resources
- ☐ Maintaining the safety and security of City employees, students, customers, and City-owned or controlled buildings and property
- ☐ Enforcing obligations to the City
- ☐ Operating vehicles for City business
- ☐ Analyzing and managing service delivery
- ☐ Communicating among City employees, with citizens, or with third parties
- ☐ Surveying and gathering feedback from constituents
- ☐ Other (Describe): _____
    - If the surveillance technology is used for a purpose not listed above, does the purpose comply with the surveillance use policy? ___ Yes ___ No

1. Information describing the surveillance technology and how it works:

In addition to describing the technology and how it works, please describe:

a. Authorized use – the uses that are authorized, the rules and processes required before that use, and the uses that are prohibited (10.64.b.2):

b. Training – the training, if any, required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, including whether there are training materials (10.64.b.9):

2. Information on the proposed purpose(s) for the surveillance technology (10.64.b.1):

3. Information describing the kind of surveillance the surveillance technology is going to conduct and what surveillance data is going to be gathered (10.64.b.3):

In addition, please describe the following as it relates to surveillance data:

a. Data access – the individuals who can access or use the collected surveillance data, and the rules and processes required before access or use of the information (10.64.b.4):

b. Data protection – the safeguards that protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms; (10.64.b.5)

c. Data retention – the time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason that retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period has elapsed, and the conditions that must be met to retain information beyond that period (10.64.b.6):

d. Public access – if and how collected surveillance data can be accessed by members of the public, including criminal defendants (10.64.b.7):

e. Third-party data-sharing – if and how other city or non-city entities can access or use the surveillance data, including any required justification and legal standard necessary to do so, and any obligation(s) imposed on the recipient of the surveillance data (10.64.b.8):

4. The location(s) it may be deployed and when:

5. A description of the privacy and anonymity rights affected and a mitigation plan describing how the department's use of the equipment will be regulated to protect privacy, anonymity, and limit the risk of potential abuse:

6. The potential impact(s) on privacy in the city; the potential impact on the civil rights and liberties of any individuals, communities or groups, including, but not limited to, communities of color or other marginalized communities in the city, and a description of whether there is a plan to address the impact(s):

7. An estimate of the fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding:

8. An explanation of how the surveillance use policy will apply to this surveillance technology and, if it is not applicable, a technology-specific surveillance use policy:

In addition, please describe the following

a. Oversight – the mechanisms to ensure that the surveillance use policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the surveillance technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy (10.64.b.10):

**APPENDIX B: CITY OF SOMERVILLE ANNUAL SURVEILLANCE REPORT**

| | |
|---|---|
| **Division or Unit (if applicable):** | |
| **Compliance Officer:** | |
| **Submitted by:** | |
| **Date:** | |
| **Surveillance Technology:** | |

1. A description of how surveillance technology has been used, including whether it captured images, sound, or information regarding members of the public who are not suspected of engaging in unlawful conduct:

2. Whether and how often data acquired through the use of the surveillance technology was shared with local, state, and federal, the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure:

3. A summary of community complaints or concerns about the surveillance technology, if any:

4. The results of any internal audits, any information about violations of the surveillance use policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the city:

5. Whether the surveillance technology has been effective at achieving its identified purpose:

6. The number of public records requests received by the city seeking documents concerning surveillance technology approved during the previous year:

7. An estimate of the total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known:

8. Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the city are disproportionately impacted by the deployment of the surveillance technology:

**9.** A disclosure of any new agreements made in the past 12 months with non-city entities that may include acquiring, sharing, or otherwise using surveillance technology or the surveillance data it provides:

**APPENDIX C: TECHNOLOGY-SPECIFIC SURVEILLANCE USE POLICY FORM (ONLY TO BE USED FOR NEW TECHNOLOGIES NOT ADDRESSED IN THE SURVEILLANCE USE POLICY)**

| | |
|---|---|
| **Division or Unit (if applicable):** | |
| **Compliance Officer:** | |
| **Submitted by:** | |
| **Date:** | |
| **Surveillance Technology:** | |

1. **Purpose**: the specific purpose(s) for the surveillance technology:

2. **Authorized use:** the uses that are authorized, the rules and processes required before that use, and the uses that are prohibited:

3. **Data collection:** the surveillance data that can be collected by the surveillance technology:

4. **Data access:** the individuals who can access or use the collected surveillance data, and the rules and processes required before access or use of the information:

5. **Data protection:** the safeguards that protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms:

6. **Data retention:** the time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason that retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period has elapsed, and the conditions that must be met to retain information beyond that period:

7. **Public access:** if and how collected surveillance data can be accessed by members of the public, including criminal defendants:

8. **Third-party data-sharing:** if and how other city or non-city entities can access or use the surveillance data, including any required justification and legal standard necessary to do so, and any obligation(s) imposed on the recipient of the surveillance data:

9. **Training:** the training, if any, required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, including whether there are training materials:

10. **Oversight:** the mechanisms to ensure that the surveillance use policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the surveillance technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for