COUNCIL POLICY CITY OF CHULA VISTA			
SUBJECT: PRIVACY PROTECTION AND TECHNOLOGY TRANSPARENCY POLICY	**POLICY NUMBER**	**EFFECTIVE DATE**	**PAGE**
			1 OF 7
ADOPTED BY: 2022-XXX		**DATED:**	
AMENDED BY: N/A			

BACKGROUND

The City of Chula Vista uses many technology systems to effectively and efficiently deliver public services. Technology available to the City has expanded from more simple tools, such as email and spreadsheets, to more complex systems that involve the automated collection and analysis of a broad range of data, including Sensitive Personal Information. Emerging technologies tend to involve the collection or generation of large amounts of data that can later be processed or analyzed. As the scope of City use of data and technology has grown, risks to individual privacy have become more apparent. As the City continues to explore new ways to use technology, the community has expressed a desire for greater levels of transparency and public engagement in decision-making around City acquisition and use of certain technologies impacting privacy.

PURPOSE

This policy has multiple purposes:

- To safeguard the security, accuracy, and control of access to City data and technology systems
- To protect the civil rights and civil liberties of Chula Vista community members, including rights to privacy
- To ensure that expert advice and community input is included as part of City decision-making involving the acquisition and use of privacy-impacting technology
- To protect against the waste of taxpayer funds
- To promote transparency in the acquisition and use of privacy-impacting technology by the City
- To build and maintain public trust in the City and its use of technology to deliver public services

POLICY

1. Definitions:
   1.1. **Acquire**: to obtain, purchase, lease, rent, borrow, create, develop, or accept in donation
   1.2. **Exigent Circumstances**: Circumstances where, based upon a good faith belief, one or more of the following conditions exists: an emergency involving danger of death or serious physical injury to any individual, or imminent danger of significant property damage or monetary loss to any individual or organization, or an imminent threat to an individuals' civil liberties or rights.
   1.3. **General Technology**: Any electronic device, software program, or hosted software solution that does not meet the definition of Sensitive Technology or Surveillance Technology.
   1.4. **Sensitive Personal Information**: Information that reveals a person's social security number, driver's license information, state identification card, passport number, military identification number, financial account numbers, debit card number, credit card number, account log-in credentials, IP address, email address, phone number, home address, precise geolocation at a given time, biometric information, contents of email, contents of mail, contents of text

messages, ethnic origin, racial origin, genetic data, medical information, health information, immigration status, philosophical beliefs, political opinions, religious beliefs, sexual orientation, union membership, or membership in any other private organization, in each case to which a person has a reasonable expectation of confidentiality or privacy. For purposes of this definition and this policy, Sensitive Personal Information **does not include** information recorded, obtained or disclosed as a part of an active criminal investigation, a lawful judicial hearing or process, or in accordance with other legal or statutory requirements.

1.5. **Sensitive Technology**: Any electronic device, software program, or hosted software solution owned or operated by the City that generates or collects Sensitive Personal Information, but which is not designed or intended to be used for surveillance.

For the purposes of this definition and this policy, Sensitive Technology **does not include** the following:

- Standard office technology such as email systems, copy machines, telephone networking systems, or broadly available consumer software such as Microsoft Office applications
- IT infrastructure only intended to manage backend or operational data.
- Technology solely intended to manage the Sensitive Personal Information of City employees, such as payroll, employment applications, health and retirement benefits.
- Technology solely intended to manage the internal administrative functions of the City, such as case management systems and revenue collection and billing systems.

1.6. **Surveillance** or **surveil:** To observe the movements, behavior, or actions of identifiable individuals, or to gather information that can readily be connected to identifiable individuals (for example, an automated license plate reader program), for purposes of analysis in accordance with a program or plan, without the knowledge and consent of the observed individuals. Observations that are incidental or part of a focused, ongoing investigation shall not be considered surveillance for the purposes of this definition and this policy.

1.7. **Surveillance Technology:** Any electronic device, software program, or hosted software solution owned or operated by the City that is designed or primarily intended to be used for the purpose of Surveillance.

For the purposes of this definition and this policy, Surveillance Technology **does not include** the following:

- Cameras installed on City property solely for the purpose of maintaining the security of that property.
- Cameras installed solely to protect the physical integrity of City infrastructure, such as sewers and storm drains.
- Technology that monitors only City employees in the performance of their City functions.
- Public safety officer body-worn cameras.

2. Privacy and Technology Advisory Commission
   2.1. The City will establish an advisory commission referred to herein as the Privacy and Technology Advisory Commission ("PTAC") responsible for carrying out a broad range of advisory duties described in this policy. In general, PTAC duties shall include (a) reviewing and advising on City technology use policies, Surveillance Technology impact reports, annual reports, procurement standards for agreements involving Sensitive or Surveillance Technology, and (b) facilitating public discussion of important issues related to privacy and City technology.
   2.2. The PTAC should include (but not be limited to) members who have the following perspectives:
   - Experts in emerging technologies and systems
   - Financial auditors and certified public accountants
   - Attorneys, legal scholars, and recognized academics with expertise in privacy and/or civil rights
   - Members of organizations that focus on government transparency or individual privacy
   - Representatives from equity-focused organizations
   - Public safety professionals
   - Individuals with experience or expertise in the functions of local government

3. Support from Privacy and Technology Experts
   3.1. The City Manager shall seek the advice of one or more City staff members or consultants with privacy and technology expertise ("PT Advisor"), as appropriate, for the following purposes:
   - Provide training and guidance to City staff on privacy issues
   - Serve as an advisor or liaison to the PTAC
   - Perform internal audits and monitor compliance with City privacy and technology use policies;
   - Coordinate with external privacy auditors when applicable;
   - Assist in the evaluation of new technology acquisitions for potential privacy issues

4. Use policies:
   4.1. The City Manager shall establish a process for determining whether a particular technology is classified as General Technology, Sensitive Technology, or Surveillance Technology. Such process may include review by an internal group of designated City staff and/or the PT Advisor.
   4.2. The City Manager shall create one written use policy that applies to all General Technology. The City Manager shall also create use policies covering each Sensitive Technology or Surveillance Technology. Where City Council approval of any technology acquisition is required, the related use policy shall be presented to the City Council for its consideration at the time of the requested approval as provided in Section 6, below.
   4.3. Every use policy for a Sensitive Technology or Surveillance Technology shall include the

following information: (a) City purpose and objectives for acquiring and deploying the technology, (b) range of authorized uses and users, (c) protocols for data collection, access, protection, retention, management, and sharing (including sharing among City departments), (d) technology maintenance protocols, (e) training requirements, and (f) provisions for auditing and oversight.

4.4. Use policies shall be reviewed and updated by the City Manager from time to time, as appropriate, with input from the PT Advisor. Use policy reviews, and updates as necessary, should occur at any time there is a significant change in the function or purpose of the subject technology, or there are material changes in applicable laws or best practices.

4.5. The order in which use policies are created or updated for existing Sensitive or Surveillance Technologies shall be determined by the City Manager, with input from the PT Advisor. Such determinations shall be made based on a consideration of the technology's potential data security risks and adverse impacts on individual privacy.

4.6. All use policies must be consistent with federal, state, and local laws and shall be reviewed by the City Attorney for legal compliance.

5. Surveillance Technology impact reports (STIR)

5.1. Prior to acquiring a Surveillance Technology, the acquiring City Department shall draft a Surveillance Technology impact report (STIR) for that technology subject to the review and approval of the City Manager. Departments should solicit input from the PT Advisor for assistance in developing such reports. Where City Council approval of any technology acquisition is required, the related STIR report shall be presented to the City Council for its consideration at the time of the requested approval as provided in Section 6, below.

5.2. Surveillance Technology impact reports should, at a minimum, (a) evaluate the potential for disproportionate adverse impacts on certain groups or parts of the community, (b) where such impacts exist, identify, where feasible, specific measures to mitigate those impacts; (c) evaluate the potential for adverse impacts on the security of data storage and access controls within city systems, particularly with respect to Sensitive Personal Information; (d) where such impacts exist, identify, where feasible, specific measures to mitigate those impacts; (e) evaluate the potential financial impacts on the City budget, including current or potential sources of funding; (f) describe potential alternatives to the technology and explain why those alternatives were not chosen.

5.3. The City should update a STIR as appropriate, any time there is a significant change in the function or purpose of the subject technology, any time there are material changes in applicable laws or best practices, or in the event of any other material change that could have an impact on data security or privacy interests.

6. Surveillance Technology acquisition process:

6.1. Any City Department intending to acquire Surveillance Technology shall, prior to acquisition, obtain City Council approval of the acquisition, along with the associated use policy and STIR.

City departments shall include a summary of comments and recommendations from the PTAC in their report to the City Council.

6.2. City Departments shall, prior to seeking City Council approval for the acquisition of Surveillance Technology, present the applicable use policy and STIR to the PTAC for their input and recommendations. If the PTAC does not act within 60 days of receiving the acquisition proposal from a City Department, the department may proceed to City Council without their recommendation.

6.3. When soliciting proposals for Surveillance Technology, the City shall require respondents to provide information regarding any previous security breaches.

6.4. All Surveillance Technology acquisitions shall be procured by written agreement, approved as to form by the City Attorney, containing in substantial form the data security and privacy provisions described in this policy.

7. Transparency in the use of Sensitive and Surveillance Technology:

7.1. City Manager's Report to the PTAC. The City Manager shall provide a report at least once every two years to the PTAC regarding the status of City use of Surveillance Technology. To the extent feasible and applicable, the report shall include, at a minimum, the following information for the applicable time period: (a) how Surveillance Technologies have been used, (b) how frequently have the technologies been deployed, including material usage patterns changes (if any) over time; (c) if and how often has data from Surveillance Technology been shared with other entities, and whether any of that data included Sensitive Personal Information; (d) an evaluation of whether Surveillance Technology is having a disproportionate adverse impact on certain groups or geographic areas of the City; (e) an evaluation of the effectiveness of any identified mitigation measures; (f) a summary of the total annual costs for the use of Surveillance Technology; and (g) a summary of any incidents involving unauthorized releases of Sensitive Personal Information.

7.2. Public Space Signage. Where feasible, signs should be posted to notify and disclose the use of Sensitive or Surveillance Technology at public facilities or within City rights of way. For example, if surveillance cameras are added to a park, signs should be posted near the entrance(s) to the park notifying visitors that they are under video surveillance.

7.3. City Website. The City shall post to the City website, in a manner that is easy to find and understand, the following information:

- A list of Sensitive and Surveillance Technologies that have been acquired within the last fiscal year
- A list of Sensitive and Surveillance Technologies the City currently uses
- Use policies for all Sensitive and Surveillance Technologies
- STIRs for all Surveillance Technologies
- The City Records Retention Schedule

8. Data Collection, Retention, Sharing, Management

8.1. The City shall not sell or allow unauthorized third-party access to Sensitive Personal Information.

8.2. The City shall ensure that all technology agreements involving the collection or storage of data that may include Sensitive Personal Information contain appropriate provisions, approved by the City Attorney, with input from the PT Advisor, that prohibit vendors from selling or allowing unauthorized access to data owned by the City except as necessary to provide the contracted service to the City.

8.3. The City shall ensure that agreements related to the acquisition or use of Sensitive or Surveillance Technology include a clause that allows the City to terminate the agreement for cause in the event the vendor violates any restriction on the sale or sharing of data or otherwise violates individual privacy protections.

8.4. The City shall seek to minimize the amount of Sensitive Personal Information departments collect when providing services so that the only data collected is the data necessary to provide the service.

8.5. The City Clerk shall ensure that the Records Retention Schedule reflects where Sensitive Personal Information is held by the City and how long that information is retained.

8.6. The requirements of this section **do not apply** to (a) any disclosure of data that is required by law, including without limitation the Public Records Act and Political Reform Act; or (b) in the discretion of the City Manager, the sharing of information necessary to support routine and necessary government operations or administration. Examples include: transferring 9-1-1 calls, transferring criminal records, transferring public health data to county or state public health agencies, sharing medical data with external parties for billing purposes, sharing employment information for verification or compliance purposes, and sharing data required for grant program compliance.

9. Information security

9.1. The City shall establish a cyber roadmap that protects Sensitive Personal Information from being exploited by unauthorized sources.

9.2. The City shall disclose unauthorized releases of Sensitive Personal Information to affected individuals as soon as practicable, subject to all applicable state and federal laws.

10. Exceptions

10.1. Interagency Task Force Activities. City staff assigned to interagency task force activities are exempt from the requirements related to acquisition and use of Sensitive and Surveillance Technology solely to the extent of their duties and work related to their assignment to the interagency task force.

10.2. Exigent Circumstances. City departments may temporarily acquire or use Surveillance Technology and the data derived from that use in a manner not expressly allowed by an existing use policy only in a situation involving exigent circumstances. If City departments acquire or use unapproved Surveillance Technology in a situation involving exigent circumstances, they

shall report the use of the technology and the justifications for using the technology in writing to the City Manager at the conclusion of the exigent circumstances. When the exigent circumstances end, the department will immediately cease using the technology and dispose of any data not directly relevant to an ongoing investigation or the exigent circumstances. If the department intends to continue using the technology after the end of the exigent circumstances, they must seek approval as outlined in Section 6 of this policy.

10.3. City Access to Private Video Feeds. The City will work with the PTAC to further develop this policy as it pertains to privately owned video feeds provided to the City by private individuals or organizations.

10.4. Waivers. The City Manager or City Council as appropriate may waive elements of this policy in the event of exigent circumstances or other circumstances that make compliance impossible or infeasible.

11. Training, Compliance and Enforcement of the Policy and Compliance with Laws.

11.1. The City Manager, with input from the City Attorney and the PT Advisor, will be responsible for interpreting and overseeing City compliance with the terms of this policy. Oversight shall include (a) requiring City employee compliance with the policy as a condition of employment; and (b) assuring that City employees or individuals who report the suspected improper use of Sensitive Technology or Surveillance Technology shall be protected from retaliation in employment.

11.2. The City does not intend by adopting this policy to grant any third party the right to enforce this policy against the City or any individual City employee and there shall be no private right of action created hereby.

11.3. All City activities conducted pursuant to the terms of this policy, including, without limitation, all data collection, retention, sharing, and management activities, shall be conducted in a manner that is consistent with all applicable federal, state, and local laws, including, without limitation, laws governing the collection, storage and disclosure of Sensitive Personal Information, and the protection of individual civil rights and liberties. In the event that there is a conflict between this policy and applicable laws, the applicable laws shall govern.

11.4. Where necessary or appropriate, with the input of the PT Advisor, the City shall provide training to key City departments and staff to ensure they are equipped to recognize and manage potential data privacy issues and perform their role and function.