

Chula Vista Technology and Privacy  
Advisory Task Force

**Supplementary Documents for  
Policy Recommendations**

## **Appendix A: Definitions**

## Definitions

1. “Annual Technology Report” means a written report concerning a specific technology that generates Sensitive Personal Information that includes all the following: (Source: San Diego TRUST pg.3)

- a. A description of how the technology was used, including the type and quantity of data gathered or analyzed by the technology;
- b. Whether and how often data acquired through the use of the technology was shared with internal or external entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s) except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the City;
- c. Where applicable, a description of the physical objects to which the technology hardware was installed without revealing the specific location of such hardware; for technology software, a breakdown of what data sources the technology was applied to;
- d. Where applicable, a description of where the technology was deployed geographically, by each Police Area in the relevant year;
- e. A summary of community complaints or concerns about the technology, and an analysis of its Use Policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall consider whether, and to what extent, the use of the technology disproportionately impacts certain groups or individuals;
- f. The results of any internal audits or investigations relating to technology, any information about violations or potential violations of the Use Policy, and any actions taken in response. To the extent that the public release of such information is prohibited by law, City staff shall provide a confidential report to the City Council regarding this information to the extent allowed by law;
- g. Information about any data breaches or other unauthorized access to the data collected by the technology, including information about the scope of the breach and the actions taken in response, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the City;
- h. A general description of all methodologies used to detect incidents of data breaches or unauthorized access, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the City;

- I. Information, including crime statistics, that helps the community assess whether the technology has been effective at achieving its identified purposes;
  - i. Statistics and information about Public Records Act requests regarding the relevant subject technology, including response rates, such as the number of Public Records Act requests on such technology and the open and close date for each of these Public Records Act requests;
  - j. Total annual costs for the technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year; and
  - k. Any requested modifications to the Use Policy and a detailed basis for the request.
- 2. “City” means any department, unit, program, and/or subordinate division of the City of Chula Vista as provided by Chapter XXXX of the Chula Vista Municipal Code. (Source: CV Municipal Code Sec. 210.01.01 paragraph C; San Diego TRUST pg.6)
- 3. “City staff” means City personnel authorized by the City Manager or appropriate City department head to seek City Council Approval of Technology That Generates Sensitive Personal Information in conformance with this Chapter. (Source: San Diego TRUST pg.7)
- 4. “Community meeting” means a publicly held meeting that is accessible, noticed at least seventy-two hours in advance in at least two languages, for the purpose of educating communities, answering questions, and learning about potential impacts of the technology on disadvantaged groups. (Source: CV City Charter pg.7; San Diego TRUST pg.7)
- 5. “Continuing agreement” means a written agreement that automatically renews unless terminated by one or more parties. (Source: CV City Charter pg.7; San Diego TRUST pg.7)
- 6. “Exigent circumstances” means a City department’s good faith belief that an emergency involving imminent danger of death or serious physical injury to any individual requires the use of a technology that generates Sensitive Personal Information that has not received prior approval by City Council. (Source: CV City Charter pg.7; San Diego TRUST pg.7)
- 7. “Facial recognition technology” means an automated or semi-automated process that assists in identifying or verifying an individual based on an individual’s face. (Source: CV City Charter pg.7; San Diego TRUST pg.7)
- 8. “Individual” means a natural person. (Source: CV City Charter pg.7; San Diego TRUST pg.7)
- 9. “Personal communication device” means a mobile telephone, a personal digital assistant, a wireless capable tablet and a similar wireless two-way communications and/or portable internet-accessing device, whether procured or subsidized by a City entity or personally owned, that is used in the regular course of City business. (Source: CV City Charter pg.8; San Diego TRUST pg.8)

10. “Police area” refers to each of the geographic districts assigned to a Chula Vista Police Department captain or commander and as such districts are amended from time to time. (Source: CV City Charter pg.8; San Diego TRUST pg.8)

11. “Privacy Impact Assessment” means an analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis (Source: National Institute of Standards and Technology Computer Security Resource Center)

12. “Privacy Risk” means the likelihood that individuals will experience problems resulting from data processing, and the impact should they occur. (Source: National Institute of Standards and Technology Computer Security Resource Center)

13. “Sensitive personal information” will reflect the California Privacy Rights Act (CPRA) (Source: 1798.140) definition of personal information which defines the term to include:

- (1) personal information that reveals:
  - (A) a consumer’s social security, driver’s license, state identification card, or passport number;
  - (B) a consumer’s account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
  - (C) a consumer’s precise geolocation;
  - (D) a consumer’s racial or ethnic origin, religious or philosophical beliefs, or union membership;
  - (E) the contents of a consumer’s mail, email and text messages, unless the business is the intended recipient of the communication;
  - (F) a consumer’s genetic data; and
- (2)
  - (A) the processing of biometric information for the purpose of uniquely identifying a consumer;
  - (B) personal information collected and analyzed concerning a consumer’s health;or
  - (C) personal information collected and analyzed concerning a consumer’s sex life or sexual orientation.

14. “Surveillance” (or “spying”) means to observe or analyze the movements, behavior, data, or actions of individuals. Individuals include those whose identity can be revealed by data or combinations of data, such as license plate data, images, IP addresses, user identifications, unique digital identifiers, or data traces left by the individual. (Source: CV City Charter pg.8)

15. “Surveillance technology” means any software (e.g., scripts, code, Application Programming Interfaces), electronic device, or system utilizing an electronic device used, designed, or primarily intended to observe, collect, retain, analyze, process, or share audio, electronic, visual,

location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group. It also includes the product (e.g., audiovisual recording, data, analysis, report) of such surveillance technology. Examples of surveillance technology include, but are not limited to the following: cell site simulators (Stingrays); automated license plate readers; gunshot detectors (ShotSpotter); drone-mounted data collection; facial recognition software; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; video cameras that can record audio or video and transmit or be remotely accessed. It also includes software designed to monitor social media services or forecast and/or predict criminal activity or criminality, and biometric identification hardware or software. “Surveillance technology” does not include devices, software, or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology beyond what is set forth below or used beyond a purpose as set forth below: (Source: CV City Charter pg.8; San Diego TRUST pg.8)

- a. Routine office hardware, such as televisions, computers, credit card machines, badge readers, copy machines, and printers, that is in widespread use and will not be used for any public surveillance or law enforcement functions related to the public;
- b. Parking Ticket Devices (PTDs) used solely for parking enforcement-related purposes, including any sensors embedded in parking sensors to detect the presence of a car in the space;
- c. Manually-operated, non-wearable, handheld digital 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;
- d. Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;
- e. Manually-operated technological devices used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems;
- f. City databases 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;
- g. Medical equipment used to diagnose, treat, or prevent disease or injury, provided that any information obtained from this equipment is used solely for medical purposes;
- h. Police department interview room cameras;
- i. City department case management systems;

- j. Personal Communication Devices that have not been modified beyond stock manufacturer capabilities in a manner described above;
- k. Surveillance technology used by the City solely to monitor and conduct internal investigations involving City employees, contractors, and volunteers; and,
- l. Systems, software, databases, and data sources used for revenue collection on behalf of the City by the City Treasurer, provided that no information from these sources is shared by the City Treasurer with any other City department or third-party except as part of efforts to collect revenue that is owed to the City.

16. “Technology Impact Report” means a publicly-posted written report for each Technology that Generates Sensitive Personal Information including, at a minimum, the following: (Source: CV Charter pg.11; San Diego TRUST pg.11)

- a. Description: Information describing the technology and how it works, including product descriptions from manufacturers;
- b. Purpose: Information on the proposed purposes(s) for the technology;
- c. Location: The physical or virtual location(s) it may be deployed, using general descriptive terms, and crime statistics for any location(s);
- d. Impact: An assessment of the Use Policy for the particular technology and whether it is adequate in protecting civil rights and liberties and whether the technology was used or deployed, intentionally or inadvertently, in a manner that may disproportionately affect marginalized communities;
- e. Mitigations: Identify specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each identified impact;
- f. Data Types and Sources: A list of all types and sources of data to be collected, analyzed, or processed by the technology, including open source data, scores, reports, logic or algorithm used, and any additional information derived therefrom;
- g. Data Security: Information about the controls that will be designed and implemented to ensure that adequate security objectives are achieved to safeguard the data collected or generated by the technology from unauthorized access or disclosure;
- h. Fiscal Costs and Sources: The forecasted, prior, and ongoing fiscal costs for the technology, including initial purchase, personnel, and other ongoing costs, and any past, current or potential sources of funding;
- i. Third-Party Dependence: Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor at any time;

j. Alternatives: A summary of all alternative methods (whether involving the use of a new technology or not) considered before deciding to use the proposed technology, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate;

k. Track Record: A summary of the experience (if any) other entities, especially government entities, have had with the proposed technology, including, if available, quantitative information about the effectiveness of the proposed technology in achieving its stated purpose in other jurisdictions, and any known adverse information about the technology such as unanticipated costs, failures, or civil rights and civil liberties abuses, existing publicly reported controversies, and any court rulings in favor or in opposition to the technology; and

l. Public engagement and comments: A description of any community engagement held and any future community engagement plans, number of attendees, a compilation of all comments received and City departmental responses given, and City departmental conclusions about potential neighborhood impacts and how such impacts may differ as it pertains to different segments of the community that may result from the acquisition of the technology.

17. “Technology that generates ‘Sensitive Personal Information’” includes “Surveillance technology” and other technology that presents “Privacy Risks”

18. “Use Policy” means a publicly-released and legally-enforceable policy for use of a Technology that Generates Sensitive Personal Information that at a minimum specifies the following: (Source: CV Charter pg.13; San Diego TRUST pg.13)

a. Purpose: The specific purpose(s) that the technology is intended to advance;

b. Use: The specific uses that are authorized, and the rules and processes required prior to such use;

c. Data Collection: The information that can be collected, captured, recorded, intercepted, or retained by the technology, as well as data that might be inadvertently collected during the authorized uses of the technology and what measures will be taken to minimize and delete such data. Where applicable, any data sources the technology will rely upon, including open source data, should be listed;

d. Data Access: The job classification of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information;

e. Data Protection: The safeguards that protect information from unauthorized access, including logging, encryption, and access control mechanisms;

- f. Data Retention: The time period, if any, for which information collected by the 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;
- g. Public Access: A description of how collected information can be accessed or used by members of the public, including criminal defendants;
- h. Third Party Data Sharing: If and how information obtained from the technology can be used or accessed, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;
- i. Training: The training required for any individual authorized to use the technology or to access information collected by the technology;
- j. Auditing and Oversight: The procedures used to ensure that the Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy; and
- k. Maintenance: The procedures used to ensure that the security and integrity of the technology and collected information will be maintained.

## **Appendix B: Information Security Policy**

Note: The task force is attaching the following information security policy model, drafted by task force member Charles Walker, as a sample resource to assist City staff in developing a comprehensive information security policy. This policy model is an incomplete working draft and has not been fully vetted by the task force.

## Recommended City Information Security Policies

**PURPOSE:** To provide guidelines with regard to the responsibility of every City of Chula Vista (City) employee who accesses Data and information in electronic formats and to provide for the security of that Data and to restrict unauthorized access to such information.

**POLICY:** Electronic Data is important to the City assets that must be protected by appropriate safeguards and managed with respect to Data stewardship. This policy defines the required Electronic Data management environment and classifications of Data, and assigns responsibility for ensuring Data and information privacy and security at each level of access and control.

**SCOPE AND APPLICABILITY:** This policy applies to all City personnel and affiliated users with access to City Data.

### **DEFINITIONS:**

***Affiliated Users:*** Vendors and guests who have a relationship to the City and need access to City systems.

***Application or App:*** A software program run on a computer or mobile device for the purpose of providing a business/academic/social function.

***Cloud:*** An on-demand availability, geographically dispersed infrastructure of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the end user. Clouds may be limited to a single organization (Private Cloud), or be available to many organizations (Public Cloud). Cloud-computing providers offer their “services” according to three standard models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

***Confidential Data:*** Data that are specifically restricted from open disclosure to the public by law are classified as Confidential Data. Confidential Data requires a high level of protection against unauthorized disclosure, modification, transmission, destruction, and use. Confidential Data include, but are not limited to:

- Medical Data, such as Electronic Protected Health Information and Data protected by the Health Insurance Portability and Accountability Act (HIPAA);
- Investigation. Only investigation data and information within the following broad categories is to be considered Confidential Data:
  - Active Investigations;
  - Activity that is covered by a fully executed non-disclosure agreement (NDA);
  - Information, data, etc., that is proprietary or confidential (whether it belongs to an internal investigator or an outside collaborator), regardless of whether it is subject to an NDA;
  - Information or data that is required to be deemed confidential by state or federal law (e.g., personally identifying information about research subjects, HIPAA or FERPA protected information, etc.); and
  - Information related to an allegation or investigation into misconduct.
- Information access security, such as login passwords, Personal Identification Numbers (PINs), logs with personally identifiable Data, digitized signatures, and encryption keys;

- Primary account numbers, cardholder Data, credit card numbers, payment card information, banking information, employer or taxpayer identification number, demand deposit account number, savings account number, financial transaction device account number, account password, stock or other security certificate or account number (such as Data protected by the Payment Card Industry Data Security Standard) ;
- Personnel file, including Social Security Numbers;
- Library records;
- Driver's license numbers, state personal identification card numbers, Social Security Numbers, employee identification numbers, government passport numbers, and other personal information that is protected from disclosure by state and federal identity theft laws and regulations.

**Data Classifications:** All Electronic Data covered by this policy are assigned one of three classifications:

- Confidential
- Operation Critical
- Unrestricted

**Data Custodian:** Persons or departments providing operational support for an information system and having responsibility for implementing the Data Maintenance and Control Method defined by the Data Steward.

**Data Maintenance and Control Method:** The process defined and approved by the Data Steward to handle the following tasks:

- Definition of access controls with assigned access, privilege enablement, and documented management approval, based on job functions and requirements.
- Identification of valid Data sources
- Acceptable methods for receiving Data from identified sources
- Process for the verification of received Data
- Rules, standards and guidelines for the entry of new Data, change of existing Data or deletion of Data
- Rules, standards and guidelines for controlled access to Data
- Process for Data integrity verification
- Acceptable methods for distributing, releasing, sharing, storing or transferring Data
- Acceptable Data locations
- Providing for the security of Confidential Data and Operation Critical Data
- Assuring sound methods for handling, processing, security and disaster recovery of Data
- Assuring that Data are gathered, processed, shared and stored in accordance with the City privacy statement **(to be written)**.

**Data Steward:** The persons responsible for City functions and who determine Data Maintenance and Control Methods are Data Stewards.

**Electronic Data/Data:** Distinct pieces of information, intentionally or unintentionally provided to the City in a variety of administrative, academic and business processes. This policy covers all Data stored on any electronic media, and within any computer systems defined as a City information technology resource.

**Mobile Computing Devices:** Information technology resources of such devices include, but are not limited to, laptops, tablets, cell phones, smart phones, and other portable devices.

**Operation Critical Data:** Data determined to be critical and essential to the successful operation of the City as a whole, and whose loss or corruption would cause a severe detrimental impact to continued operations. Data receiving this classification require a high level of protection against accidental distribution, exposure or destruction, and must be covered by high quality disaster recovery and business continuity measures. Data in this category include Data stored on Enterprise Systems such as Data passed through networked communications systems. Such Data may be released or shared under defined, specific procedures for disclosure, such as departmental guidelines, documented procedures or policies.

**City Provided Data Systems:** Information technology resources, as defined and described by the City and used for the storage, maintenance and processing of City Data.

**Unrestricted Data:** Information that may be released or shared as needed.

**Usage/Data Use:** Usage and Data Use are used interchangeably and are defined as gathering, viewing, storing, sharing, transferring, distributing, modifying, printing and otherwise acting to provide a Data maintenance environment.

## **PROCEDURES:**

### **1. Data Stewardship**

Data Stewards are expected to create, communicate and enforce Data Maintenance and Control Methods. Data Stewards are also expected to have knowledge of functions in their areas and the Data and information used in support of those functions. The Chief Information Officer(CIO) is ultimately accountable for the Data management and stewardship of all the City data. The CIO may appoint others in their respective areas of responsibility.

### **2. Data Maintenance and Control Method**

Data Stewards will develop and maintain Data Maintenance and Control Methods for their assigned systems.

When authorizing and assigning access controls defined in the Data Maintenance and Control Methods involving Confidential Data and Operation Critical Data, Data Stewards will restrict user privileges to the least access necessary to perform job functions based on job role and responsibility.

If the system is a City Provided Data System, City Technology Services will provide, upon request, guidance and services for the tasks identified in the Data Maintenance and Control Method.

If the system is provided by a Public Cloud, the Data Steward must still verify that the Data Maintenance and Control Method used by the Public Cloud provider meets current City technology standards **(to be written)?**. Further, ongoing provisions for meeting current City technology and security standards **(to be written)?** must be included in the service contract.

Review of Public Cloud solutions must include City Technology Services and City Attorney prior to final solution selection and purchase.

Use of personal equipment to conduct City business must comply with all guidance provided by City policies **(to be written)?**.

### **3. Data Custodianship**

Data Custodians will use Data in compliance with the established Data Maintenance and Control Method. Failure to process or handle Data in compliance with the established method for a system will be considered a violation of the City policies.

### **4. Data Usage**

In all cases, Data provided to the City will be used in accordance with the Privacy Statement **(to be written)** Software solutions, including SaaS solutions, are selected to manage Data and are procured, purchased and installed in conjunction with City (to be written)

Data will be released in accordance with City (to be written). Requests for information from external agencies (such as Freedom of Information Act requests, subpoenas, law enforcement agency requests, or any other request for Data from an external source) must be directed to the City Attorney and processed in accordance with existing policies.

Standards for secure file transmissions, or Data exchanges, must be evaluated by the CIO when a system other than a City Provided Data System is selected or when a Public Cloud is utilized. Specific contract language may be required. The City Attorney must be consulted regarding such language.

Unencrypted authorization and Data transmission are not acceptable.

Communication of Confidential Data via end-user messaging technologies (i.e., email, instant messaging, chat or other communication methods) is prohibited

### **5. Storing Data**

Data cannot be stored on a system other than a City Provided Data System without the advance permission of the Data Steward and demonstrated legitimate need.

Data should be stored in encrypted formats whenever possible. Confidential Data **must** be stored in encrypted formats. Encryption strategies should be reviewed with City Technology Services in advance to avoid accidental Data lockouts.

Data cannot be stored on a City-provided Computing Device unless the device is encrypted without the advance permission of the Data Steward and demonstrated legitimate need.

Data must be stored on devices and at locations approved by Data Stewards. If information technology resources (computers, printers and other items) are stored at an off-campus location, the location must be approved by Data Stewards prior to using such resources to store City Data.

Technology enables the storage of Data on fax machines, copiers, cell phones, point-of-sale devices and other electronic equipment. Data Stewards are responsible for discovery of stored Data and removal of the Data prior to release of the equipment.

When approving Mobile Computing Device Usage, Data Stewards must verify that those using Mobile Computing Devices can provide information about what Data was stored on the device (such as a copy of the last backup) in the event the device is lost or stolen.

In all cases, Data storage must comply with City retention policies. Data Usage in a Public Cloud system must have specific retention standards **(to be written)?** written in the service contract. The City Attorney must be consulted regarding such language.

Provisions for the return of all City Data in the event of contract termination must be included in the contract, when Data is stored on a Public Cloud. The City Attorney must be consulted regarding such language. Current security standards **(to be written)?** (such as controlled access, personal firewalls, antivirus, fully updated and patched operating systems, etc.) will be evaluated when a system other than a City Provided Data System is selected and must be covered in contract language. The City Attorney must be consulted regarding such language.

Data stored on Mobile Computing Devices must be protected by current security standard methods (such as controlled access, firewalls, antivirus, fully updated and patched operating systems, etc.). City standard procedures **(to be written)** for the protection and safeguarding of Confidential Data and Operation Critical Data must be applied equally and without exception to City Provided Data Systems, Mobile Computing Devices and systems other than City Provided Data Systems, such as Public Cloud solution.

## 6. Systems and network Data

Systems and network Data, generated through systems or network administration, logs or other system recording activities, cannot be used, or captured, gathered, analyzed or disseminated, without the advance permission of the Chief Information Officer.

## 7. Value of Data

In all cases where Data are to be processed through a Public Cloud, the following assessment must be done: The value of the Data must be determined in some tangible way.

Signature approval from the Data Steward's division vice president or appropriate party with the ability to authorize activity at the level of the value of the Data must be obtained.

## 8. Sanctions

Failure to follow the guidelines contained in this document will be considered inappropriate use of a City information technology resource and therefore a violation of the City policy **(to be written)**.

## 9. Data Security Breach Review Panel

A Data Security Breach Review Panel (Panel) comprised of the following members will be established:

- Chief Information Officer

- Chief of Police
- City Attorney
- Chief Privacy Officer

#### **10. Data Loss Prevention Software**

Define granular access rights for removable devices and peripheral ports and establish policies for users, computers and groups, maintaining productivity while enforcing device security

#### **11. Audits**

All City owned equipment is subject to audit for unauthorized storage of regulated data. Devices authorized to store regulated data are subject to audits as deemed necessary by the CIO. Reasonable prior notification of an audit will be provided. Audit results are handled confidentially by Information Security staff and are reported to the CIO in aggregate.

#### **12. Mobile Devices**

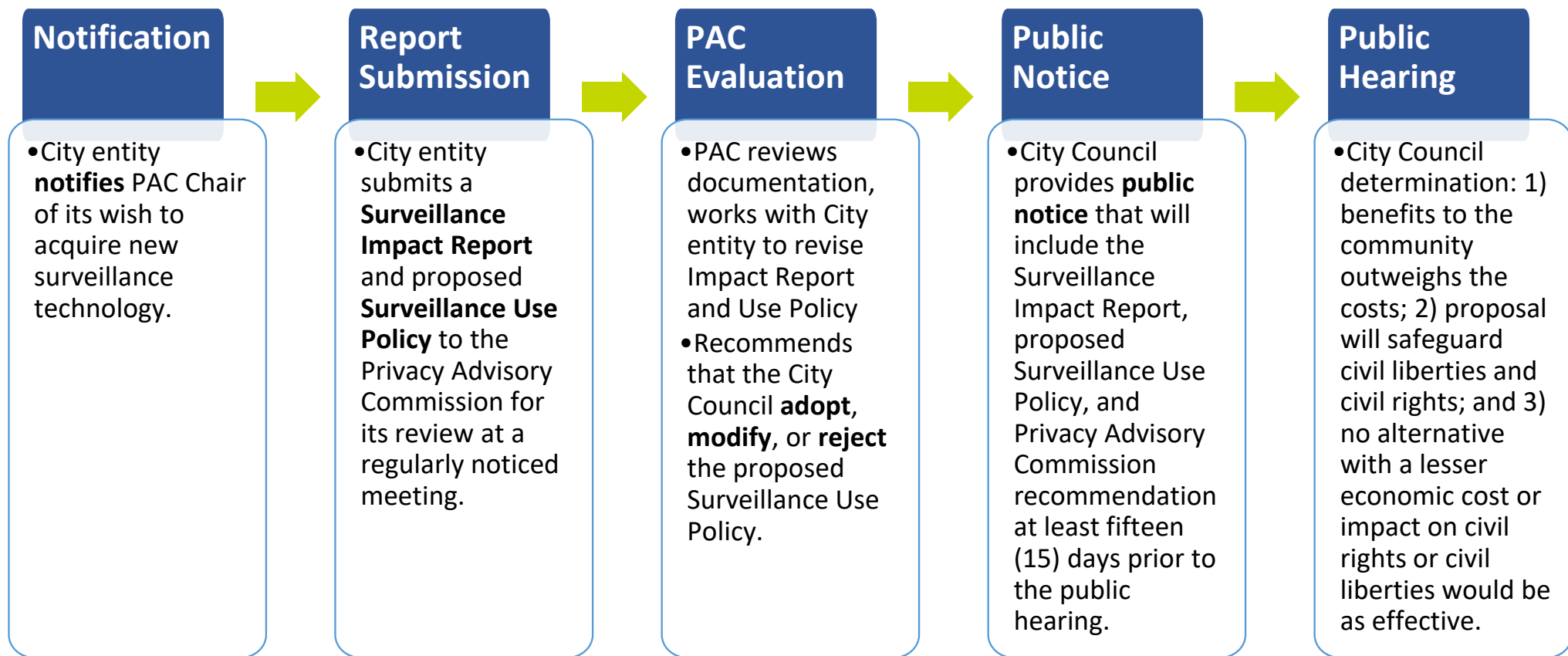
City owned mobile equipment will be exclusively allowed on the City's primary network and use two factor authentication. All personal devices must use "guest" access if provided.

## **Appendix C: Public Disclosure and Review Process**

Note: The task force is attaching this excerpt from a slide presentation that describes the City of Oakland's process for acquiring new surveillance technology. The diagram was not developed by the task force and does not correspond exactly to the process recommended by the task force for the City of Chula Vista; however, it provides a useful illustration of the general order of review intended by the task force for Chula Vista.

# How does the Surveillance Ordinance work in practice?

Process for city to acquire or use a surveillance technology



## **Appendix D: Sample Ordinances**

Note: The task force is attaching the following draft ordinances submitted by community members in recognition of the role they played in helping to shape the task force's recommendations. The inclusion of these draft ordinances is not an endorsement by the task force, as the task force did not review these draft ordinances with the same level of diligence as the final task force recommendations. The draft ordinances are focused on surveillance, which the task force considers to be one part of the broader subject area of privacy and security. The task force encourages the City to continue seeking community feedback and also reviewing similar models, such as the recently adopted San Diego TRUST ordinance.

# Surveillance & Community Safety Ordinance

(Revised - July 15, 2022)

## ORDINANCE ADDING CHAPTER XXXX TO THE CHULA VISTA MUNICIPAL CODE ESTABLISHING RULES FOR THE CITY'S ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY

WHEREAS, the City of Chula Vista ("City") takes great public pride in its status as a Welcoming City and as a Smart City; and

WHEREAS, smart public safety decisions and the protection of all community members require that municipalities ensure public debate and community involvement in decisions about whether to acquire or use surveillance technology; moreover, that real public safety requires that residents have a voice in these decisions; and

WHEREAS, across the U.S. cities that have adhered to a "privacy bill of rights" approach are able to win public support in implementing the technology with proper safeguards in place to build trust. Alternatively, cities that implement new technology in secrecy, without oversight, without policy, and without broad and inclusive public input have found themselves facing scrutiny, lawsuits, and voter referendums to ban certain technologies.

WHEREAS, the City Council finds it is essential to have an informed public debate as early as possible about decisions related to the City's acquisition and use of surveillance technology; and

WHEREAS, the City Council finds that, while the use of surveillance technology may threaten the privacy of all citizens, throughout history, surveillance efforts have been used to intimidate and oppress certain communities and groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation or political perspective; and

WHEREAS, while acknowledging the significance of protecting the privacy of citizens, the City Council finds that surveillance technology may also be a valuable tool to bolster community safety and aid in the investigation and prosecution of crimes; and

WHEREAS, the City Council finds that surveillance technology includes not just technology capable of accessing non-public places or information (such as wiretaps) but also may include technology which aggregates publicly available information, because such information, in the aggregate or when pieced together with other information, has the potential to reveal a wealth of detail about a person's familial, political, professional, religious, or sexual associations; and

WHEREAS, the City Council finds that no decisions relating to the City's use of surveillance technology should occur without strong consideration being given to the impact such technologies may have on civil rights and civil liberties, including those rights guaranteed by the California and United States Constitutions; and

WHEREAS, the City Council finds that any and all decisions regarding if and how the City's surveillance technologies should be funded, acquired, or used should include meaningful public input and that public opinion should be given significant weight in policy decisions; and

WHEREAS, the City Council finds that legally enforceable safeguards, including robust transparency, oversight, and accountability measures, must be in place to protect civil rights and civil liberties before any City surveillance technology is deployed; and

WHEREAS, the City Council finds that if a surveillance technology is approved, data reporting measures must be adopted that empower the City Council and public to verify that mandated civil rights and civil liberties safeguards have been strictly adhered to.

NOW, THEREFORE, the City Council of the City of Chula Vista does ordain as follows:

## **Section I. Establishment**

A. This Ordinance shall be known as the *Surveillance and Community Safety Ordinance*.

B. *Chula Vista Municipal Code Chapter XXXX*, is hereby added as set forth below:

### **Chapter XXXX. REGULATIONS ON CITY'S ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY**

#### **C. Definitions**

1. "Annual Surveillance Report" means a written report concerning a specific surveillance technology that includes all the following:
  - a. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology;
  - b. Whether and how often data acquired through the use of the surveillance technology was shared with internal or external entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s) except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the City;
  - c. Where applicable, a description of the physical objects to which the surveillance technology hardware was installed without revealing the specific location of such

hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to;

- d. Where applicable, a description of where the surveillance technology was deployed geographically, by each Police Area in the relevant year;
- e. A summary of community complaints or concerns about the surveillance technology, and an analysis of its Surveillance Use Policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall consider whether, and to what extent, the use of the surveillance technology disproportionately impacts certain groups or individuals;
- f. The results of any internal audits or investigations relating to surveillance technology, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response. To the extent that the public release of such information is prohibited by law, City staff shall provide a confidential report to the City Council regarding this information to the extent allowed by law;
- g. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the City;
- h. A general description of all methodologies used to detect incidents of data breaches or unauthorized access, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the City;
- i. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes;
- j. Statistics and information about Public Records Act requests regarding the relevant subject surveillance technology, including response rates, such as the number of Public Records Act requests on such surveillance technology and the open and close date for each of these Public Records Act requests;
- k. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the surveillance technology in the coming year; and
- l. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.

2. “City” means any department, unit, program, and/or subordinate division of the City of Chula Vista as provided by Chapter XXXX of the Chula Vista Municipal Code.
3. “City staff” means City personnel authorized by the City Manager or appropriate City department head to seek City Council Approval of Surveillance Technology in conformance with this Chapter.
4. “Community meeting” means a publicly held meeting that is accessible, noticed at least seventy-two hours in advance in at least two languages, for the purpose of educating communities, answering questions, and learning about potential impacts of surveillance technology on disadvantaged groups.
5. “Continuing agreement” means a written agreement that automatically renews unless terminated by one or more parties.
6. “Exigent circumstances” means a City department’s good faith belief that an emergency involving imminent danger of death or serious physical injury to any individual requires the use of surveillance technology that has not received prior approval by City Council.
7. “Facial recognition technology” means an automated or semi-automated process that assists in identifying or verifying an individual based on an individual’s face.
8. “Individual” means a natural person.
9. “Personal communication device” means a mobile telephone, a personal digital assistant, a wireless capable tablet and a similar wireless two-way communications and/or portable internet-accessing device, whether procured or subsidized by a City entity or personally owned, that is used in the regular course of City business.
10. “Police area” refers to each of the geographic districts assigned to a Chula Vista Police Department captain or commander and as such districts are amended from time to time.
11. “Surveillance” (or “spying”) means to observe or analyze the movements, behavior, data, or actions of individuals. Individuals include those whose identity can be revealed by data or combinations of data, such as license plate data, images, IP addresses, user identifications, unique digital identifiers, or data traces left by the individual.
12. “Surveillance technology” means any software (e.g., scripts, code, Application Programming Interfaces), electronic device, or system utilizing an electronic device used, designed, or primarily intended to observe, collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group. It also includes the product (e.g., audiovisual recording, data, analysis, report) of such surveillance technology. Examples of surveillance technology include, but are not limited to the following: cell site simulators (Stingrays); automated license plate readers; gunshot detectors (ShotSpotter); drone-mounted data collection;

facial recognition software; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; video cameras that can record audio or video and transmit or be remotely accessed. It also includes software designed to monitor social media services or forecast and/or predict criminal activity or criminality, and biometric identification hardware or software.

“Surveillance technology” does not include devices, software, or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology beyond what is set forth below or used beyond a purpose as set forth below:

- a. Routine office hardware, such as televisions, computers, credit card machines, badge readers, copy machines, and printers, that is in widespread use and will not be used for any public surveillance or law enforcement functions related to the public;
- b. Parking Ticket Devices (PTDs) used solely for parking enforcement-related purposes, including any sensors embedded in parking sensors to detect the presence of a car in the space;
- c. Manually-operated, non-wearable, handheld digital 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;
- d. Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;
- e. Manually-operated technological devices used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems;
- f. City databases 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;
- g. Medical equipment used to diagnose, treat, or prevent disease or injury, provided that any information obtained from this equipment is used solely for medical purposes;
- h. Police department interview room cameras;
- i. City department case management systems;
- j. Personal Communication Devices that have not been modified beyond stock manufacturer capabilities in a manner described above;

- k. Surveillance technology used by the City solely to monitor and conduct internal investigations involving City employees, contractors, and volunteers; and,
  - l. Systems, software, databases, and data sources used for revenue collection on behalf of the City by the City Treasurer, provided that no information from these sources is shared by the City Treasurer with any other City department or third-party except as part of efforts to collect revenue that is owed to the City.
14. "Surveillance Impact Report" means a publicly-posted written report including, at a minimum, the following:
- a. Description: Information describing the surveillance technology and how it works, including product descriptions from manufacturers;
  - b. Purpose: Information on the proposed purposes(s) for the surveillance technology;
  - c. Location: The physical or virtual location(s) it may be deployed, using general descriptive terms, and crime statistics for any location(s);
  - d. Impact: An assessment of the Surveillance Use Policy for the particular technology and whether it is adequate in protecting civil rights and liberties and whether the surveillance technology was used or deployed, intentionally or inadvertently, in a manner that may disproportionately affect marginalized communities;
  - e. Mitigations: Identify specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each identified impact;
  - f. Data Types and Sources: A list of all types and sources of data to be collected, analyzed, or processed by the surveillance technology, including open source data, scores, reports, logic or algorithm used, and any additional information derived therefrom;
  - g. Data Security: Information about the controls that will be designed and implemented to ensure that adequate security objectives are achieved to safeguard the data collected or generated by the surveillance technology from unauthorized access or disclosure;
  - h. Fiscal Costs and Sources: The forecasted, prior, and ongoing fiscal costs for the surveillance technology, including initial purchase, personnel, and other ongoing costs, and any past, current or potential sources of funding;

- i. Third-Party Dependence: Whether use or maintenance of the surveillance technology will require data gathered by the surveillance technology to be handled or stored by a third-party vendor at any time;
  - j. Alternatives: A summary of all alternative methods (whether involving the use of a new technology or not) considered before deciding to use the proposed surveillance technology, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate;
  - k. Track Record: A summary of the experience (if any) other entities, especially government entities, have had with the proposed technology, including, if available, quantitative information about the effectiveness of the proposed surveillance technology in achieving its stated purpose in other jurisdictions, and any known adverse information about the surveillance technology such as unanticipated costs, failures, or civil rights and civil liberties abuses, existing publicly reported controversies, and any court rulings in favor or in opposition to the surveillance; and
  - l. Public engagement and comments: A description of any community engagement held and any future community engagement plans, number of attendees, a compilation of all comments received and City departmental responses given, and City departmental conclusions about potential neighborhood impacts and how such impacts may differ as it pertains to different segments of the community that may result from the acquisition of surveillance technology.
15. "Surveillance Use Policy" means a publicly-released and legally-enforceable policy for use of the surveillance technology that at a minimum specifies the following:
- a. Purpose: The specific purpose(s) that the surveillance technology is intended to advance;
  - b. Use: The specific uses that are authorized, and the rules and processes required prior to such use;
  - c. Data Collection: The information that can be collected, captured, recorded, intercepted, or retained by the surveillance technology, as well as data that might be inadvertently collected during the authorized uses of the surveillance technology and what measures will be taken to minimize and delete such data. Where applicable, any data sources the surveillance technology will rely upon, including open source data, should be listed;

- d. **Data Access:** The job classification of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information;
- e. **Data Protection:** The safeguards that protect information from unauthorized access, including logging, encryption, and access control mechanisms;
- f. **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;
- g. **Public Access:** A description of how collected information can be accessed or used by members of the public, including criminal defendants;
- h. **Third Party Data Sharing:** If and how information obtained from the surveillance technology can be used or accessed, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;
- i. **Training:** The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology;
- j. **Auditing and Oversight:** The procedures used to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the surveillance 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 legally enforceable sanctions for violations of the policy; and
- k. **Maintenance:** The procedures used to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

## **Section II. Privacy Advisory Commission ("Commission") Notification and Review Requirements**

### *A. Commission Notification Required Prior to City Solicitation of Funds and Proposals for Surveillance Technology.*

1. City staff shall notify the Chair of the Commission by written memorandum along with providing a Surveillance Use Policy and a Surveillance Impact Report prior to:

- a. Seeking or soliciting funds for surveillance technology, including but not limited to applying for a grant;
  - b. Soliciting proposals with any entity to acquire, share or otherwise use surveillance technology including the information it provides; or
  - c. Formally or informally facilitating in a meaningful way or implementing surveillance technology in collaboration with other entities, including City ones.
2. Upon notification by City staff, the Chair of the Commission shall place the item on the agenda at the next Commission meeting for discussion and possible action. At this meeting, City staff shall present the Commission with evidence of the need for the funds or equipment, or shall otherwise justify the action City staff will seek Council approval for pursuant to Section III.
3. The Commission may make a recommendation to the City Council by voting for approval to proceed, by objecting to the proposal, by recommending that the City staff modify the proposal, or by taking no action.
4. If the Commission votes to approve, object, or modify the proposal, City staff may proceed and seek City Council approval of the proposed surveillance technology initiative pursuant to the requirements of Section III. City staff shall present to City Council the result of the Commission's review, including any objections to the proposal.
5. If the Commission does not make its recommendation on the item within 90 calendar days of notification to the Commission Chair, City staff may proceed and seek City Council approval of the proposed Surveillance Technology initiative pursuant to the requirements of Section II.

*B. Commission Review and Approval Required for New Surveillance Technology Before City Council Approval*

1. Prior to seeking City Council approval under Section III, City staff shall submit a Surveillance Impact Report and a Surveillance Use Policy for the proposed new surveillance technology initiative to the Commission for its review at a publicly noticed meeting. The Surveillance Impact Report and Surveillance Use Policy must address the specific subject matter specified for each document as set forth in Section I.
2. The Commission shall approve, modify, or reject the proposed Surveillance Use Policy. If the Commission proposes that the Surveillance Use Policy be modified, the Commission shall propose such modifications to City staff. City staff shall present such modifications to the Commission for approval before seeking City Council approval under Section III.
3. Prior to submitting the Surveillance Impact Report, City staff shall complete one or more community meetings in each City Council district where the proposed surveillance

technology is deployed, with opportunity for public comment and written response. The City Council may condition its approval of the proposed surveillance technology on City staff conducting additional community engagement before approval, or after approval as a condition of approval.

4. The Commission shall recommend that the City Council adopt, modify, or reject the proposed Surveillance Use Policy. If the Commission proposes that the Surveillance Use Policy be modified, the Commission shall propose such modifications to City staff. City staff shall present such modifications to City Council when seeking City Council approval under Section III.

5. If the Commission does not make its recommendation on a presented item within 90 days of notification to the Commission Chair pursuant to Section II, City staff may seek City Council approval of the item.

6. City staff seeking City Council approval shall schedule for City Council consideration and approval of the proposed Surveillance Use Policy, and include Commission recommendations, at least fifteen (15) days prior to a mandatory, properly noticed, germane public hearing. Approval may only occur at a public hearing.

#### *C. Commission Review Requirements for Existing Surveillance Technology Before Seeking City Council Approval*

1. Prior to seeking City Council approval for existing City surveillance technology used by the City under Section III, City staff shall submit a Surveillance Impact Report and Surveillance Use Policy for each existing surveillance technology to the Commission for its review, and for the public's review, at least fifteen (15) days prior to a publicly noticed meeting, so the public can prepare for and participate in the Commission meetings. The Surveillance Impact Report and Surveillance Use Policy shall address the specific subject matters set forth for each document in Section I.

2. Prior to submitting the Surveillance Impact Report, City staff shall complete one or more community meetings in each City Council district where the proposed surveillance technology is deployed with opportunity for public comment and written response. The City Council may condition its approval on City staff conducting additional outreach before approval, or after approval as a condition of approval.

3. Prior to submitting the Surveillance Impact Report and proposed Surveillance Use Policy as described above, City staff shall present to the Commission, and for public review, a list of all surveillance technology possessed and/or used by the City.

4. The Commission shall rank the surveillance technology items in order of potential impact to civil liberties to provide a recommended sequence for items to be heard at Commission meetings. The Commission shall take into consideration input from City

staff on the operational importance of the surveillance technology in determining the ranking to allow such matters to be heard in a timely manner.

5. Within sixty (60) days of the Commission's action in Section II(C)(4), and continuing every month thereafter until a Surveillance Impact Report and a Surveillance Use Policy have been submitted for each item of the list, City staff shall submit at least one (1) Surveillance Impact Report and one (1) proposed Surveillance Use Policy per month to the Commission for review, generally beginning with the highest ranking surveillance technology items as determined by the Commission.

6. If the Commission does not make its recommendation on any item within 90 days of submission to the Commission Chair, City staff may proceed to the City Council for approval of the item pursuant to Section III.

### **Section III. City Council Approval Requirements for New and Existing Surveillance Technology**

A. City staff shall obtain City Council approval prior to any of the following:

1. Accepting local, state, or federal funds, or in-kind or other donations for surveillance technology;

x2. Acquiring new surveillance technology, including but not limited to procuring such technology without the exchange of monies or consideration;

3. Using existing surveillance technology, or using new surveillance technology, including the information the surveillance technology provides, for a purpose, in a manner, or in a location not previously approved by the City Council pursuant to the requirements of this ordinance; or

4. Entering into a continuing agreement or written agreement with to acquire, share or otherwise use surveillance technology or the information it provides, including data-sharing agreements.

5. Notwithstanding any other provision of this section, nothing herein shall be construed to prevent, restrict or interfere with any person providing evidence or information derived from surveillance technology to a law enforcement agency for the purposes of conducting a criminal investigation or the law enforcement agency from receiving such evidence or information.

B. *City Council Approval Process*

1. After the Commission notification and review requirements in Section II have been met, City staff seeking City Council approval shall schedule a date for City Council consideration of the proposed Surveillance Impact Report and proposed Surveillance

Use Policy, and include Commission recommendations, at least fifteen (15) days prior to a mandatory, properly-noticed, germane public hearing. Approval may only occur at a public hearing.

2. The City Council shall only approve any action as provided in this Chapter after first considering the recommendation of the Commission, and subsequently making a determination that the benefits to the community of the surveillance technology outweigh the costs; that the proposal will safeguard civil liberties and civil rights; and that, in the City Council's judgment, no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.

3. For Approval of existing surveillance technology for which the Commission does not make its recommendation within ninety (90) days of review as provided for in Section II: if the City Council has not reviewed and approved such item within four (4) City Council meetings from when the item was initially scheduled for City Council consideration, the City shall cease its use of the surveillance technology until such review and approval occurs.

#### *C. Surveillance Impact Reports and Surveillance Use Policies as Public Records*

1. Unless otherwise provided in this Ordinance, Surveillance Impact Reports and Surveillance Use Policies are public records.
2. City staff shall make all Surveillance Impact Reports and Surveillance Use Policies, as updated from time to time, available to the public as long as the City uses the surveillance technology in accordance with its request pursuant to Section II.
3. City staff shall post all Surveillance Impact Reports and Surveillance Use Policies to the City's website with an indication of its current approval status and the planned City Council date for action.

### **Section IV. Use of Unapproved Surveillance Technology during Exigent Circumstances**

A. City staff may temporarily acquire or use surveillance technology and the data derived from that use in a manner not expressly allowed by a Surveillance Use Policy only in a situation involving exigent circumstances.

B. If City staff acquires or uses a surveillance technology in a situation involving exigent circumstances, City staff shall:

1. Immediately report in writing the use of the surveillance technology and its justifications to the City Council and the Commission;
2. Use the surveillance technology solely to respond to the exigent circumstances;
3. Cease using the surveillance technology when the exigent circumstances end;

4. Only keep and maintain data related to the exigent circumstances and dispose of any data that is not relevant to an ongoing investigation or the exigent circumstances; and
5. Following the end of the exigent circumstances, report the temporary acquisition or use of the surveillance technology for exigent circumstances to the Commission in accordance with Section II of this ordinance at its next meeting for discussion and possible recommendation to the City Council.

C. Any surveillance technology acquired in accordance with exigent circumstances shall be returned within thirty (30) calendar days following when the exigent circumstances end, unless City staff initiates the process set forth for the use of the surveillance technology by submitting a Surveillance Use Policy and Surveillance Impact Report for Commission review within this 30-day time period. If City staff is unable to meet the 30-day deadline, City staff shall notify the City Council, who may grant an extension. In the event that City staff complies with the 30-day deadline or the deadline as may be extended by the City Council, City staff may retain possession of the surveillance technology, but may only use such surveillance technology consistent with the requirements of this Ordinance.

## **Section V. Oversight Following City Council Approval**

### *A. Annual Surveillance Report*

1. For each approved surveillance technology item, City staff shall present a written Annual Surveillance Report for the Commission to review within one year after the date of City Council final passage of such surveillance technology and annually thereafter as long as the surveillance technology is used.
2. If City staff is unable to meet the annual deadline, City staff shall notify the Commission in writing of staff's request to extend this period, and the reasons for that request. The Commission may grant a single extension of up to sixty (60) calendar days to comply with this provision.
3. After review of the Annual Surveillance Report by the Commission, City staff shall submit the Report to the City Council.
4. The Commission shall recommend to the City Council: (a) that the benefits to the community of the surveillance technology in question outweigh the costs and that civil liberties and civil rights are safeguarded; (b) that use of the surveillance technology cease; or (c) propose modifications to the corresponding Surveillance Use Policy that will resolve any identified concerns.
5. If the Commission does not make its recommendation on the item within 90 calendar days of submission of the Annual Surveillance Report to the Commission Chair, City staff may proceed to the City Council for approval of the Annual Surveillance Report.

### *B. Summary Of All Requests And Recommendations And City Council Determination*

1. In addition to the above submission of any Annual Surveillance Report, City staff shall provide in its report to the City Council a summary of all requests for City Council approval pursuant to Section III for that particular surveillance technology and the pertinent Commission recommendation, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval.

2. Based upon information provided in the Annual Surveillance Report and after considering the recommendation of the Commission, the City Council shall revisit its “cost benefit” analysis as provided in Section III(B)(2) and either uphold or set aside the previous determination. Should the City Council set aside its previous determination, the City’s use of the surveillance technology must cease. Alternatively, City Council may require modifications to a particular Surveillance Use Policy that will resolve any concerns with the use of a particular surveillance technology.

## **Section VI. Enforcement**

### *A. Violations of this article are subject to the following remedies:*

1. Any material violation of this Ordinance, or of a Surveillance Use Policy promulgated pursuant to this Ordinance, constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in the Superior Court of the State of California to enforce this Ordinance. An action instituted under this paragraph shall be brought against the City of Chula Vista and, if necessary, to effectuate compliance with this Ordinance or a Surveillance Use Policy (including to expunge information unlawfully collected, retained, or shared thereunder), any other governmental agency with possession, custody, or control of data subject to this Ordinance, to the extent permitted by law.

2. Any person who has been subjected to the use of surveillance technology in material violation of this Ordinance, or of a material violation of a Surveillance Use Policy, or about whom information has been obtained, retained, accessed, shared, or used in violation of this Ordinance or of a Surveillance Use Policy promulgated under this Ordinance, may institute proceedings in the Superior Court of the State of California against the City of Chula Vista and shall be entitled to recover actual damages (but not less than liquidated damages of \$1,000 or \$100 per day for each day of violation, whichever is greater).

3. A court may award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under paragraphs A(1) and A(2) under Section VI above.

## **Section VII. Contract for Surveillance Technology**

### *A. Contracts and agreements for surveillance technology*

1. It shall be unlawful for the City to enter into any contract or other agreement for surveillance technology that conflicts with the provisions of this Ordinance. Any conflicting provisions in any such contract or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable. Any amendment or exercise of any option to any contract to obtain or use surveillance technology shall require City staff to comply with the provisions of this Ordinance.
2. To the extent permitted by law, the City shall publicly disclose all of its surveillance contracts, including any and all related non-disclosure agreements, if any, regardless of any contract terms to the contrary.

## **Section VIII. Whistleblower Protections**

A. Neither the City nor anyone acting on behalf of the City may take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment, including but not limited to discriminating with respect to compensation, terms and conditions of employment, access to information, restrictions on due process rights, or civil or criminal liability, because:

1. The employee or applicant was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of a surveillance technology or surveillance data based upon a good faith belief that the disclosure evidenced a violation of this Ordinance; or
2. The employee or applicant was perceived to, about to, had assisted in or had participated in any proceeding or action to carry out the purposes of this Ordinance.

B. It shall be grounds for disciplinary action for a City employee or anyone else acting on behalf of the City to retaliate against another City employee or applicant who makes a good-faith complaint that there has been a failure to comply with any Surveillance Use Policy or administrative instruction promulgated under this Ordinance.

C. Any employee or applicant who is injured by a violation of this Section may institute a proceeding for monetary damages and injunctive relief against the City in any court of competent jurisdiction.

## **Section IX. Review of Existing Surveillance Use Policies and Adoption as Ordinances**

A. Surveillance technology is considered existing if the City possessed, used, or has a contract in force and effect for the use of surveillance technology, or any resulting data, on the effective date of this Ordinance.

B. The requirement for City staff to present a list of all existing surveillance technology and, once ranked, to seek monthly Commission review and approval for the use of existing surveillance technology shall begin within sixty (60) days after the effective date of this Ordinance.

C. As per Section II, City staff shall return to City Council with an ordinance or ordinances for adoption and codification under the Chula Vista Municipal Code of all Surveillance Use Policies, but only after proper Commission and City Council review of any Surveillance Use Policies for existing surveillance technology, and with a 15-day public notice period in each instance to allow the public to prepare and participate in the meetings.

## **Section X. Severability**

If any portion of this Ordinance, or its application to any person or circumstance, is for any reason held to be invalid, unenforceable or unconstitutional, by a court of competent jurisdiction, that portion shall be deemed severable, and such invalidity, unenforceability or unconstitutionality shall not affect the validity or enforceability of the remaining portions of the Ordinance, or its application to any other person or circumstance. The City Council of the City of Chula Vista hereby declares that it would have adopted each section, sentence, clause or phrase of this Ordinance, irrespective of the fact that any one or more other sections, sentences, clauses or phrases of the Ordinance be declared invalid, unenforceable or unconstitutional.

## **Section XI. Construction**

The City Council of the City of Chula Vista intends this Ordinance to supplement, not to duplicate or contradict, applicable state and federal law and this Ordinance shall be construed in light of that intent.

## **Section XII. Effective Date**

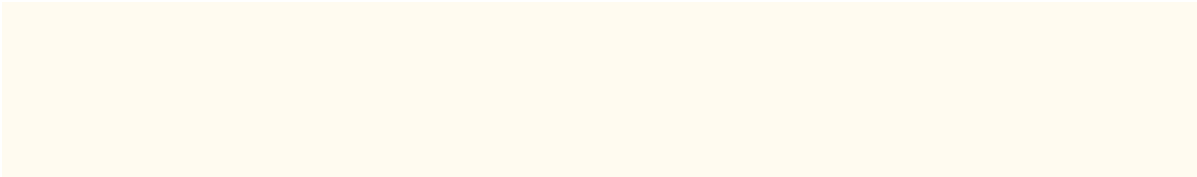
This Ordinance shall take effect and be in force on the thirtieth day after its final passage.

## **Section XIII. Publication**

The City Clerk shall certify to the passage and adoption of this Ordinance and shall cause the same to be published or posted according to law.

Presented by

Approved as to form by



# Privacy Advisory Commission Ordinance

(Revised - July 15, 2022)

ORDINANCE NO. \_\_\_\_\_

## ORDINANCE OF THE CITY OF CHULA VISTA ESTABLISHING THE CHULA VISTA PRIVACY ADVISORY COMMISSION PROVIDING FOR THE APPOINTMENT OF MEMBERS THEREOF, AND DEFINING THE DUTIES AND FUNCTIONS OF SAID COMMISSION

WHEREAS, the Chula Vista City Council (City Council) finds that the use of surveillance technology is important to protect public health and safety, but such use must be appropriately monitored and regulated to protect the privacy and other rights of Chula Vista residents and visitors, and

WHEREAS the City of Chula Vista (the City) has been building on a detailed Smart City Strategic Action Plan since 2017 with limited opportunity for community input, oversight or control; and

WHEREAS Chula Vista seeks to maintain its designation by Welcoming America as a certified Welcoming City, City Council strives to comply with the criteria in the Welcoming Standard, in particular, relevant criteria relating to “Safe Communities”, “Equitable Access”, and “Civic Engagement”; and

WHEREAS, the City Council recognizes the use of open data associated with surveillance technology offers benefits to the City, but those benefits must also be weighed against the costs, both fiscal and civil liberties; and

WHEREAS, the City Council recognizes that surveillance technology may be a valuable tool to support community safety, investigations, and prosecution of crimes, but must be balanced with the individual’s right to privacy, it also; and

WHEREAS, the City Council recognizes that privacy is not just a personal matter; there are societal consequences to privacy degradation over time as well as societal benefits with increased trust and transparency; and

WHEREAS, the City Council finds that surveillance technology includes not just technology capable of accessing non-public places or information, but also may include technology that aggregates publicly-available information, which, in the aggregate or when

pieced together with other information, has the potential to reveal details about a person's familial, political, professional, religious, or intimate associations; and

WHEREAS, the City Council recognizes that government surveillance may chill associational and expressive freedoms; and

WHEREAS, the City Council recognizes that data from surveillance technology can be used to intimidate and oppress certain groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective; and

WHEREAS, the City Council finds that safeguards, including robust transparency, oversight, and accountability measures, must be in place to protect civil rights and civil liberties before City surveillance technology is deployed; and

WHEREAS, the City Council finds that decisions regarding if and how the City's surveillance technologies should be funded, acquired, or used should include meaningful public input; and

WHEREAS, on January 18, 2022, City Council unanimously approved creation of a "Technology and Privacy Advisory Task Force" to draft policy and recommendations to be presented to the City Council for consideration, and further requested that the City Administration prepare a "Citywide Technology Oversight Policy"; and

WHEREAS, the said Technology and Privacy Advisory Task Force recommends creation of a new permanent citizen advisory board known as the "Privacy Advisory Commission" to advise the Mayor and City Council on transparency, accountability, and public deliberation in the City's acquisition and usage of surveillance technology and data; and

WHEREAS, Article VI, Section 600 of the City Charter reserves to the City Council the authority to create boards and commissions by ordinance, and to prescribe their function, powers, duties, membership, appointment, terms, qualifications, eligibility, reimbursements for expenses, if any;

NOW THEREFORE the City Council of the City of Chula Vista does hereby ordain as follows:

## **Section I. Establishment**

### ***A. Establishment and Appropriations***

Pursuant to Article VI of the Charter of the City of Chula Vista, there is hereby created a Chula Vista Privacy Advisory Commission (hereinafter referred to as the "Privacy Commission" or "Commission"). Appropriations of funds sufficient for the efficient and proper functioning of the Privacy Commission shall be included in the annual budget by the City Council.

### *B. Purpose and Intent*

It is the purpose and intent of the City Council to establish a Privacy Commission to serve as an advisory body to the Mayor and City Council on policies and issues related to privacy and surveillance. The Commission will provide advice intended to ensure transparency, accountability, and public deliberation in the City's acquisition and use of surveillance technology.

### *C. Definitions*

For purposes of this ordinance, all words defined in the CVMC Chapter XXXX, known as the Chula Vista Surveillance and Community Safety Ordinance, have the same meaning herein.

### *D. Membership*

The Privacy Advisory Commission shall consist of nine (9) members, who shall serve without compensation. At least six (6) members shall be Chula Vista residents. Members shall be appointed by the City Council.

### *E. Qualifications of Members*

All members of the Privacy Advisory Commission shall be persons who have a demonstrated interest in privacy rights through work experience, civic participation, and/or political advocacy.

The City Council shall appoint the nine (9) members from the following representative areas of organization interest, expertise, and background:

1. At least one attorney or legal scholar with expertise in privacy or civil rights, or a representative of an organization with expertise in privacy or civil rights;
2. One auditor or certified public accountant;
3. One computer hardware, software, or encryption security professional;
4. One member of an organization that focuses on open government and transparency or an individual, such as a university researcher, with experience working on open government and transparency; and
5. At least four (4) members from equity-focused organizations serving or protecting the rights of communities and groups historically subject to disproportionate surveillance, including communities of color, immigrant communities, religious minorities, and groups concerned with privacy and protest.

Member qualifications and eligibility shall be in accordance with Chula Vista Charter Article VI, Section 602, and CVCM Section 2.25.030. No member shall have a state law-prohibited financial interest, employment, or policy-making position in any commercial or for-profit facility, research center, or other organization that sells data products, surveillance equipment, or otherwise profits from recommendations made by the Privacy Advisory Commission.

### *F. Terms*

Pursuant to Article VI, Section 602 of the City Charter, members shall be appointed by motion of the City Council adopted by at least three affirmative votes. The members thereof shall serve for a term of four (4) years and until their respective successors are appointed and confirmed. Members shall be limited to a maximum of two (2) consecutive terms and an interval of two (2) years must pass before a person who has served two (2) consecutive terms may be reappointed to the body upon which the member had served.

Initial members shall be appointed in staggered terms by lot. For the initial appointments, three (3) members shall be appointed to an initial term that will expire on June 30, 2023, and two (2) members shall be appointed to an initial term that will expire on June 30 of each subsequent year. Initial appointments to a term of two years or less shall not have the initial term count for purposes of the eight-year term limit.

#### *G. Rules*

The Commission shall hold regular meetings as required by ordinance of the City Council, and such special meetings as such commissions may require. All proceedings shall be open to the public.

At the first regular meeting, and subsequently at the first regular meeting of each year following the first day of July of every year, members of the Privacy Advisory Commission shall select a chairperson and a vice chairperson.

The Commission shall adopt rules for the government of its business and procedures in compliance with the law. The Commission rules shall provide that a quorum of the Privacy Advisory Commission is five people.

Pursuant to Article VI, Section 603 of the City Charter, the Commission shall have the same power as the City Council to compel the attendance of witnesses, to examine them under oath and to compel the production of evidence before it.

## **Section II. Privacy Advisory Commission: Duties and Functions**

#### *A. Duties and Functions*

The Privacy Advisory Commission shall:

1. Provide advice and technical assistance to the City on best practices to protect resident and visitor privacy rights in connection with the City's acquisition and use of surveillance technology.
2. Conduct meetings and use other public forums to collect and receive public input on the above subject matter.
3. Review Surveillance Impact Reports and Surveillance Use Policies for all existing and new surveillance technology and make recommendations prior to the City seeking solicitation of funds and proposals for surveillance technology.
4. Submit annual reports and recommendations to the City Council regarding:

- a. The City's use of surveillance technology; and
- b. Whether new City surveillance technology privacy and data retention policies should be developed, or existing policies should be amended.
- c. Provide analysis to the City Council of pending federal, state, and local legislation relevant to the City's purchase and/or use of surveillance technology.
- d. The Privacy Advisory Commission shall make reports, findings, and recommendations either to the City Manager or the City Council, as appropriate. The Commission shall present an annual written report to the City Council. The Commission may submit recommendations to the City Council following submission to the City Manager.

#### *B. Meetings and Voting*

The Commission shall meet at an established regular interval, day of the week, time, and location suitable for its purpose. Such meetings shall be designated regular meetings. Other meetings scheduled for a time or place other than the regular day, time and location shall be designated special meetings. Written notice of special meetings shall be provided to the Commission members, and all meetings of the Commission shall comport with any City or State open meetings laws, policies, or obligations.

The Commission shall, in consultation with the City Manager, establish bylaws, rules and procedures for the conduct of its business by a majority vote of the members present. Voting shall be required for the adoption of any motion or resolution. Any action by the Commission shall be approved by a majority of members present, provided a quorum exists.

#### *C. Staff*

Staff assistance may be provided to the Board as determined by the City Manager, pursuant to his or her authority under the Charter to administer all affairs of the City under his or her jurisdiction.

### **Section III. Severability**

If any portion of this Ordinance, or its application to any person or circumstance, is for any reason held to be invalid, unenforceable or unconstitutional, by a court of competent jurisdiction, that portion shall be deemed severable, and such invalidity, unenforceability or unconstitutionality shall not affect the validity or enforceability of the remaining portions of the Ordinance, or its application to any other person or circumstance. The City Council of the City of Chula Vista hereby declares that it would have adopted each section, sentence, clause or phrase of this Ordinance, irrespective of the fact that any one or more other sections, sentences, clauses or phrases of the Ordinance be declared invalid, unenforceable or unconstitutional.

## **Section IV. Construction**

The City Council of the City of Chula Vista intends this Ordinance to supplement, not to duplicate or contradict, applicable state and federal law and this Ordinance shall be construed in light of that intent.

## **Section V. Effective Date**

This Ordinance shall take effect and be in force on the thirtieth day after its final passage.

## **Section VI. Publication**

The City Clerk shall certify to the passage and adoption of this Ordinance and shall cause the same to be published or posted according to law.

Presented by:

Approved as to form by