Chula Vista Technology and Privacy Advisory Task Force
Summary of Policy Recommendations
DRAFT VERSION – August 25, 2022

Note: To facilitate discussion and review, the policy recommendations are numbered in this document. There is no particular order or significance to the numbering scheme or the section headings in this draft.

Privacy Advisory Board

1. The City should establish a Privacy Advisory Board responsible for carrying out a broad range of advisory duties.
    a. The Board's duties are described throughout this document, including:
        i. Holding regular meetings that are open to the public, including opportunities for public comment in English and other languages.
        ii. Reviewing Use Policies for privacy-impacting technologies and making recommendations on changes
        iii. Reviewing data sharing agreements.
        iv. Reviewing new technology-related contracts.

2. The Privacy Advisory Board should have nine members, at least two-thirds of whom are Chula Vista residents.
    a. Chula Vista residents should comprise a super-majority of Board members because residents experience the impacts of City decisions on privacy and technology to a much greater degree than non-residents do.
    b. The purpose of allowing non-residents to serve on the Board is to recognize that non-residents also experience the impacts of City decisions on privacy and technology, especially if they work, own a business, or attend school in Chula Vista. Additionally, non-residents may have valuable expertise or perspectives that should be included on the Board.
    c. There is no requirement to include non-residents on the Board.

3. Privacy Advisory Board members will be selected through a combination of City staff review, community review, and City Council review.
    a. Members of the Board should be selected through a process that includes review and vetting by both City staff and by community leaders, similar to the process used to appoint members of the Technology and Privacy Advisory Task Force.
    b. All members of the Board must be approved by a majority vote of the City Council pursuant to the City Charter.
    c. The purpose of involving community leaders in the selection process for some members is to ensure that Board membership is not exclusively determined by City staff or elected officials.

4. Selections to the Board should reflect the City's diversity in terms of race, gender, and age.

All Board members shall be persons who have an interest in privacy rights as demonstrated by work experience, civic participation, and/or political advocacy.

No member may be an elected official.

No member may have a financial interest, employment, or policy-making position in any commercial or for-profit facility, research center, or other organization that sells surveillance equipment or profits from decisions made by the Board.

Each of the following perspectives should be represented by at least one member of the Board:

a. A resident of Council District 1
b. A resident of Council District 2
c. A resident of Council District 3
d. A resident of Council District 4
e. A technology professional with expertise in emerging technologies and systems (this perspective should be represented by three members of the board)
f. A professional financial auditor or Certified Public Accountant (CPA)
g. An attorney, legal scholar, or recognized academic with expertise in privacy and/or civil rights
h. A member of an organization that focuses on government transparency or individual privacy
i. A representative from an equity-based organization or a member of the Human Relations Commission.
j. A former member of the Technology and Privacy Advisory Task Force (only applies to the first year of appointments)

Chief Privacy Officer

5. The City should hire a full-time Chief Privacy Officer responsible for carrying out a broad range of duties related to privacy.
    a. Until a full-time Chief Privacy Officer can be budgeted and hired, the duties of the Chief Privacy Officer should be carried out by the Chief Information Security Officer.
    b. The Chief Privacy Officer should report to the City Manager to ensure they are accountable to City Council and the voters of Chula Vista.
        i. A minority of task force members believes the Chief Privacy Officer should report to the City Attorney to ensure they are accountable to the voters of Chula Vista.
    c. The Chief Privacy Officer's responsibilities include, but are not limited to:
        i. Provide regular training sessions and guidance to City staff on privacy issues.
        ii. Serve as the primary City staff liaison to the Privacy Advisory Board, including:
            1. Managing agendas and coordinating meetings

2. Managing the selection process for Privacy Advisory Board members
3. Assisting in the preparation and presentation of technology Use Policies for Board review

iii. Performing internal audits and ensuring compliance with data retention standards and use policies, and coordinating with external privacy auditors when applicable
iv. Evaluating new technology acquisitions for potential privacy issues

Use Policies

6. The City should create written Use Policies that govern the use of each privacy-impacting technology and the data generated by those technologies.
    a. Each policy should clearly state the purpose of the technology, who will be allowed to access the technology, how the technology can be used, what kind of data the technology generates, how that data can be used, how that data is protected, and the retention period for that data.

7. Use Policies should be drafted by the applicable department in consultation with the Chief Privacy Officer, then reviewed by the Privacy Advisory Board.
    a. Departments will use a template created by the Chief Privacy Officer.

8. Use Policies should be reviewed annually and updated if necessary. Use policies should also be reviewed and updated any time there is a significant change in the function or purpose of the technology.

9. Due to the large number of use policies that may need to be created or updated, the Chief Privacy Officer and Privacy Advisory Board will perform an analysis that prioritizes current and future technologies based on the impact and risks to individual privacy. Based on the results of this analysis, use policies will be reviewed for the highest-ranked technologies first.
    a. Facial recognition technology, other biometric systems, surveillance systems, and systems that use machine learning algorithms should be a top priority for Board review.

Data Retention and Data Sharing

10. The City should never sell the data it collects nor allow third parties working on behalf of the City to sell or use data owned by the City except as necessary to provide the contracted service to the City.

11. Internal data-sharing between City Departments should be subject to a review process that includes approval by the City Manager and periodic review by the Chief Privacy Officer and Privacy Advisory Board.
    a. The purpose of this policy recommendation is to ensure there is a clear understanding of how data is being used and shared between departments, and to

prevent situations where there is uncertainty around how data is being used, such as in the case of the informal data-sharing that occurred between Engineering and the Police Department regarding traffic signal camera feeds.

12. External data-sharing between the City and third parties must be approved through a formal, auditable process that includes the Chief Privacy Officer and Privacy Advisory Board.
    a. The purpose of this policy recommendation is to prevent situations like the sharing of ALPR data with law enforcement agencies that should not have had access to it.
    b. The review should ensure that personal information is not being shared and that the data has been repackaged and de-identified to minimize the possibility of privacy violations.

13. The City Records Retention Schedule should be re-organized and expanded to include information on what personal data is collected and when that data will be deleted.
    a. As part of these updates, the Records Retention schedule should be presented in a format that provides a category for data type in addition to the existing categories.
    b. The Chief Privacy Officer should collaborate with the City Clerk to lead this process.

14. The City should establish a more formal process for ensuring that personal data is being deleted according to the Use Policies established for that data.

15. The City should establish a policy that it will not collect personal data unless it is absolutely necessary to provide the core service.
    a. The Chula Vista Public Library's approach to personal data is a model that should be followed citywide. Personal data is only collected and retained for the period necessary to provide the service. For example, the library keeps a record of an item checked out by an individual borrower only until that item is returned, at which point data related to that transaction is deleted.
    b. To ensure compliance with this policy, the Chief Privacy Officer should randomly sample Departments or data sets to review on a periodic basis.

16. Where possible, the City should anonymize, remove, or de-identify data that relates to a person.
    a. It must be understood and acknowledged that anonymization strategies will not completely protect individuals from having their identities reverse-engineered from otherwise anonymized datasets, but these strategies are still valuable in mitigating risks to individual privacy.

17. The role of the City's Data Governance Committee should be more clearly defined and communicated to the public.
    a. The City should ensure that the work of the Data Governance Committee is consistent with the City's adopted privacy policies and with the role or recommendations of the Privacy Advisory Board.

Transparency and Oversight

18. City staff should provide the public with full disclosures about what technologies have been acquired, what data is being collected, and how that data is being used.
    a. These disclosures should happen in a variety of ways, including on the City's website, through email newsletters, social media, and in printed communications mailed to residents.
    b. These disclosures should address what data is being collected, what department is collecting it, how it is being used, who has access to it, how long it is retained, etc.
    c. Where feasible, signs should be posted to notify and disclose surveillance technology. For example, if surveillance cameras are added to parks, signs should be posted notifying visitors that they are under video surveillance.
    d. The City should hold public forums, educational seminars, and other types of community events to ensure the public is informed and has an opportunity to hold the City accountable for how privacy-impacting technologies are being used.
    e. All public disclosures related to technology, data, and privacy should be provided with adequate time for public review before any meeting. The 72-hour standard is not sufficient for the public to review and consider new information, especially when that time period coincides with weekends and holidays.

19. Information about privacy and technology that is provided on the City website should be easy to find and easy to understand.
    a. Links to disclosures should be provided on each Department's page within the City website.
    b. The City's "smart city" webpages should have their own navigational tab or section on the City website, rather than being contained under the Business / Economic Development section.

20. Contracts with technology vendors should be easy for the public to find and review.
    a. This should include information about the status of existing contracts, including upcoming renewal or termination dates.

21. Data breaches should be publicly disclosed as soon as possible.
    a. Notification should happen within 24 hours of the data breach being confirmed.
    b. Notification should occur through a wide range of communications channels, including social media, news media, and the City website.

22. Residents should have the opportunity to opt-out or have their data deleted if it was provided voluntarily to the City and is not needed for City operations.
    a. It is understood that individuals will not be able to opt-out of certain types of data collection, such as a drone responding to 9-1-1 calls, or medical data being retained following a emergency medical service call.

Procurement

23. All contracts with privacy implications must be presented to the City Council, regardless of whether they meet standard purchasing and contracting thresholds that typically trigger City Council review.

24. Prior to City Council presentation, contracts with privacy implications must be reviewed by the Chief Privacy Officer and the Privacy Advisory Board. The evaluation provided by the Chief Privacy Officer and the Privacy Advisory Board must be included as part of the report presented to City Council.

25. When acquiring new technology systems, the Chief Information Security Officer and Chief Privacy Officer should prepare an assessment of the technology's potential impact on the City's information security and detail any mitigation strategies. This assessment should be provided to the Privacy Advisory Board and the City Council at the same time as any other documents provided for review, such as the contract for the technology (Item 24) and the technology's proposed Use Policy (Item 7).

26. The City may not enter into any agreement that prohibits the City from publicly acknowledging that it has acquired or is using a particular technology. Nondisclosure agreements are acceptable only to extent that they protect a vendor's proprietary information without prohibiting the City's acknowledgement of a relationship with the vendor.

27. Contracts should include a clause of convenience that allows the City to terminate the agreement in the event the vendor violates any restriction on the sale or sharing of data or otherwise violates individual privacy protections.

28. Technology contracts should require that vendors provide the City with the capability to audit or review who has accessed what information.
    a. These access reports should be provided at pre-designated intervals to City staff or third-party auditors.

29. City staff should be provided with additional training to assist in recognizing potential data privacy issues in contracts.
    a. Key staff to receive additional training includes the Chief Privacy Officer, Chief Information Security Officer, City Attorney staff, and purchasing and contracting staff.

30. Changes in the ownership of a privacy-impacting technology that has already been reviewed by the Privacy Advisory Board should trigger a new review by the Privacy Advisory Board.

Information Security

31. Establish a comprehensive information security policy that addresses procedures for maintaining and controlling access to data and articulates the roles and responsibilities of data stewards and data custodians.
    a. An outline of such a policy has been developed by the Information Security subcommittee of this Task Force and will be submitted as part of this recommendation.
    b. The policy should make clear that only City-owned mobile equipment using two-factor authentication should be allowed to connect to the City's primary network. Any personal devices connecting to the City's network must use restricted "guest" access.
    c. The policy should provide for audits of all City-owned equipment to protect against unauthorized storage of regulated data.
    d. The policy should require data security breaches to be reviewed and addressed by an established panel that includes the Director of Information Technology Services, the Chief Information Security Officer, the Chief of Police, the City Attorney, and the Chief Privacy Officer.
    e. The policy should require that data is stored and transmitted in encrypted formats whenever possible and prohibit the communication of confidential data through end-user messaging technologies such as email, instant messaging, chat, or other communication methods.
    f. The policy should specifically address mobile computing devices, including recovery of data in the event a mobile computing device is lost or stolen.

Additional Comments

The Task Force has received multiple public comments regarding the methodology used to conduct the public opinion survey and focus groups. The Task Force encourages City staff and City Councilmembers to consider the potential for bias in the results of the public opinion research, particularly as described in the letter from Dr. Norah Shultz of San Diego State University, which was provided as part of the August 15 Task Force meeting agenda.

Appendix A: Definitions
DRAFT – August 25, 2022

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;

i. 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;

j. 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

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

(l) 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.

12. “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.

13. “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.

Information Security Subcommittee Report
August 15, 2022
Members: Charles Walker and Carlos De La Toba

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.