Acceptable Use Policy

Committee on Information Technology

PURPOSE AND SCOPE

The purpose of this policy is to protect City and County of San Francisco employees, partners, and departments from illegal or damaging actions by individuals, through intentional or unintentional means, by outlining the acceptable use of all City-owned or leased computer equipment. Inappropriate use of equipment exposes the City to risks including virus attacks, compromise of network systems and services, breach of confidentiality, and legal liability.

This policy applies to all employees, interns, volunteers, or any other City workers, contractors and vendors, and to any person or agency with access to City computers. This policy applies to all equipment owned or leased by the City.

POLICY STATEMENT

Departments are responsible for the enforcement of this policy with respect to their own employees.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, hardware, software, operating systems, storage media, network accounts providing electronic mail, Web browsers, and file transfer protocols, are the property of the City and County of San Francisco. These systems are provided for City business purposes only.

CCSF's Employee Handbook may be found at http://sfdhr.org/employee-handbook

POLICY REQUIREMENTS

General Use and Ownership

Data created and/or stored on City systems remains the property of the City and County of San Francisco. There is no guarantee of confidentiality of information stored on any network device belonging to the City.

The City's Employee Handbook clearly states the City's computer networks, computer systems, telephones, cell phones, fax machines and other City property are to be used for City business purposes only. The handbook sections "Use of City and County Property for Business Purposes Only" and "Computers and Data Information Systems" state, in relevant part:

- Authorized employees or contractors may monitor equipment, systems, and network traffic at any time for security, network maintenance and policy compliance purposes. Typically, monitoring will be done by departmental IT staff or the Department of Technology.
- The City reserves the right to conduct audits on a periodic basis to ensure compliance with this policy.

COIT Policy Dates

Approved: September, 2009
Next Review Date: FY 2017-18

- The City reserves the right to forensically or otherwise examine City-owned electronic devices, including but not limited to computer systems, networks, telephone systems and cell phones.

The complete CCSF Employee Handbook is at http://sfdhr.org/employee-handbook

Use of Personally Owned Devices

Employees may use personally-owned devices to access City networks, subject to the following:

- Using personally-owned devices to conduct City business

  Prior to accessing the City network to conduct City business using a personally owned device, employees must obtain permission from their appointing officers or designees. Access to City networks is limited to City business only, and subject to all City-wide and departmental monitoring systems and policies, including but not limited to the prohibition of discrimination and harassment in the workplace.

  The City's networks are City property and therefore fall under the Employee Handbook sections mentioned in section 3.1 of this document.

- Using personally-owned devices to conduct personal business

  Employees may use their personally owned devices to access City networks designated for public or guest access to conduct personal business during defined rest or meal periods, and subject to any applicable departmental limitations and other City policies, including but not limited to confidentiality, conflict of interest, general conduct, harassment, and discrimination.

Security and Proprietary/Confidential Information

Information contained on the Internet/Intranet/Extranet-related systems may be proprietary or confidential, as defined by the City or department confidentiality guidelines. An example of proprietary information may be a specific software application. Examples of confidential information may include, but are not limited to: employee medical information, employee personal data, vendor and bidder information, attorney/client correspondence, examination and job application materials, and other data. Employees may or may not have access to proprietary and/or confidential information, depending on the business need for access to this type of information.

Authorized users are assigned network accounts based on defined business needs. These accounts are called User Level Accounts. Each employee's access to specific types of information is defined in his or her User Level Account. All employees, regardless of level of access, should take all necessary steps to prevent disclosure of any proprietary and/or confidential information to anyone not authorized to access this information.

In the event a City employee receives a request for information, including requests submitted under the Public Records Act and/or Sunshine Ordinance, the employee must work with his or her department's designee to ensure that in fulfilling requests they do not release any proprietary and/or confidential data to the public.

Enforcement

Violators of this policy may be subject to appropriate disciplinary action, up to and including termination of employment and/or legal action.

Citywide Cybersecurity Policy

Committee on Information Technology

The City and County of San Francisco (City) is dedicated to building a strong cybersecurity program to support, maintain, and secure critical infrastructure and data systems. The following policy is intended to maintain and enhance key elements of a citywide cybersecurity program.

PURPOSE AND SCOPE

The COIT Cybersecurity Policy lays the foundation for the City's Cybersecurity Program as a whole and articulates executive level support for the effort. Cybersecurity operations across the City are in different stages of deployment. The Cybersecurity Policy supports the City's Cybersecurity Program established to:

- protect our connected critical infrastructure
- protect the sensitive information placed in our trust
- manage risk
- continuously improve our ability to detect cybersecurity events
- contain and eradicate compromises, restoring information resources to a secure and operational status
- ensure risk treatment is sufficient and in alignment with the criticality of the information resource
- facilitate awareness of risk to our operations within the context of cybersecurity

The requirements identified in this policy apply to all information resources operated by or for the City, and County of San Francisco and its departments, and commissions. Elected officials, employees, consultants, and vendors working on behalf of the City and County of San Francisco are required to comply with this policy.

POLICY STATEMENT

The COIT Cybersecurity Policy requires all departments to:

1. Appoint a Departmental Information Security Officer (DISO) to coordinate cybersecurity efforts. Larger Departments may appoint a Chief Information Security Officer (CISO) to recognize the increased scope of responsibility.
2. Adopt a cybersecurity framework as a basis to build their cybersecurity program. The City recommends adopting the National Institute of Standards and Technology (NIST) Cybersecurity Framework as a methodology to secure information resources.
3. Support cyber incident response as needed in accordance with Emergency Support Function 18 (ESF-18) Unified Cyber Command.
4. Conduct and update, at least annually, a department cybersecurity risk assessment. Departments with dedicated Risk Management staff may elect to integrate cybersecurity risk management into the department's Risk Management program.
5. Develop and update, at least annually, department cybersecurity requirements to mitigate risk and comply with legal and regulatory cybersecurity requirements. Department will develop and adopt cybersecurity requirements that should be equivalent to or greater than the citywide security requirements.
6. Participate in citywide cybersecurity forum meetings.

COIT Policy Dates

Approved: November 21, 2019
Next Review Date: FY 2020-2021

CYBERSECURITY FRAMEWORK

The Cybersecurity Policy requires all departments to adopt a cybersecurity framework to guide their operations.

In order to adequately protect information resources, systems and data must be properly categorized based on information sensitivity and criticality to operations. A risk-based methodology standardizes security architecture, creates a common understanding of shared or transferred risk when systems and infrastructure are connected, and makes securing systems and data more straightforward.

The NIST framework provides five elements to a cybersecurity program:

Function	Description
Identify	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
Protect	Develop and implement appropriate safeguards to ensure delivery of infrastructure services.
Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
Respond	Develop and implement appropriate activities to respond to a cybersecurity event.
Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services impaired by a cybersecurity event.

Departments, in consultation with the City Chief Information Security Officer (CCISO), may choose alternatives to the NIST Cybersecurity Framework. However, all departments shall implement or consume central standards and services from their respective framework, such as access control and management, risk assessment and management, awareness and training, and data classification.

CYBERSECURITY RISK ASSESSMENT

As defined in NIST Special Publication 800-30, "Guide for Conducting Risk Assessments," risk assessment is the process of identifying, estimating, and prioritizing information security risks.[1] Assessing risk requires the careful analysis of threat and vulnerability information to determine

[1] ISO 31000 "Risk Management – Guidelines" is another framework for risk assessment.

the extent to which circumstances or events could adversely impact an organization [i.e. City departments] and the likelihood that such circumstances or events will occur.

The purpose of risk assessment is to inform decision makers and support risk responses by identifying:

i. relevant threats to [departments]
ii. vulnerabilities both internal and external to [departments]
iii. impact (i.e., harm) to [departments] that may occur given the potential for threats exploiting vulnerabilities
iv. likelihood that harm will occur

The end result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring).

To ensure their cybersecurity programs comply with an approved cybersecurity framework, including NIST CSF, ISO 2700x, and CIS Top 20, and a risk-based approach, the City Services Auditor conducts readiness assessments to measure implementation.

Readiness assessments align with an approved cybersecurity framework and enable departments to determine their current cybersecurity capabilities, set individual goals for a target state, and establish a plan for improving and maintaining cyber security programs. Readiness assessments also assist the Department of Technology and the Controller in the efficient and effective planning of cybersecurity activities.

CYBERSECURITY REQUIREMENTS

Departments are required to develop and update cybersecurity requirements to mitigate risk profiles and comply with legal and regulatory cybersecurity requirements. The City Chief Information Security Officer will develop baseline cybersecurity requirements to address the citywide risk profile. All proposed requirements will be reviewed and approved by the Architecture Policy and Review Board (APRB). Upon adoption by the APRB, Departments should subsequently develop cybersecurity requirements that should be equivalent to or greater than the citywide security requirements to address department risks. APRB should establish meaningful timelines for adoption based on the complexity of the proposed requirements.

City-wide cyber-security requirements shall not supersede State or Federal requirements that may apply to certain specific city departments.

-

ROLES AND RESPONSIBILITIES

1. **Department Heads** shall:
    a. Promote a culture of cybersecurity awareness and compliance with the City's cybersecurity policy. Department heads must remind their employees and contractors about the City's Cybersecurity policies, standards, procedures, guidelines, and best practices.

   b. To the extent resources allow, budget and staff the cybersecurity function for systems procured, operated, or contracted by their departments to ensure that all systems and the data contained by them are protected in accordance with the category / classification of the data and systems.
   c. Designate a Departmental Information Security Officer (DISO) or a Chief Information Security Officer

2. **City Chief Information Security Officer (CCISO)** shall:
   a. Establish and maintain a security team and function with the ability to identify, protect, detect, respond, and recover from attacks against City information resources.
   b. Develop and maintain a centralized incident response program capable of addressing major compromises of City information resources.
   c. Review Emergency Support Function 18 Unified Cyber Command annex annually and ensure it is updated as needed.
   d. Support departments' cyber emergency exercises and conduct periodic Citywide cybersecurity emergency exercise with City leaders.
   e. Ensure that Department, Commission, and the Centralized Information Technology Cybersecurity Programs employ a risk-based assessment and treatment program, and regularly report the status of the City's residual risk profile to City leadership.
   f. Develop cybersecurity risk assessment methodology and provide training to DISOs on conducting cybersecurity risk assessments.
   g. Provide guidance on building the security organization at the department level.
   h. Ensure that Departments' cybersecurity risk assessment results are protected adequately and access is restricted to limited City cybersecurity personnel.
   i. At least annually, develop and update citywide cybersecurity requirements to mitigate the City's residual risk profile, and comply with legal and regulatory cybersecurity requirements. All cybersecurity requirements will be approved by the Architecture Policy & Review Board (APRB) before going into effect.
   j. Support departments' implementation of citywide cybersecurity requirements.
   k. Support department DISOs in their cybersecurity responsibilities, including through the centralized incident response program, cybersecurity defense capabilities, and a citywide cybersecurity toolset.
   l. Organize citywide cybersecurity forum meetings.

3. **Departmental Information Security Officers (DISOs)** shall:
   a. Ensure information resources are properly protected through risk treatment strategies that meet the acceptable risk threshold for the category / classification of the information resource.
   b. Develop the necessary security organizations based on the available resources and budget.
   c. Inform the City Chief Information Security Officer when there is an event which compromises the control, confidentiality, integrity, or availability of a system or data involving Personally Identifiable Information, Regulatory Protected Information (such as HIPAA or Social Security Numbers), and/or data that is not considered public as soon as practical.

d. Participate in the citywide cybersecurity round table meetings.
e. Conduct and update, at least annually, department cybersecurity risk assessments, and confidentially share results with the City Chief Information Security Officer.
f. Meet annually with department Disaster Preparedness Coordinator to review results of cyber risk assessment and update department COOP cyber appendix as needed. Departments with dedicated Emergency Management Functions shall review the results of their department's cyber-security risk assessments and update their incident response procedures as appropriate
g. Conduct, at least annually, department cybersecurity emergency exercise with department leadership, City partners, and critical third parties. Departments with dedicated Emergency Management Functions may elect to incorporate cyber-security as part of their department emergency exercises.
h. Develop and update, at least annually, department cybersecurity requirements to mitigate department risk profile and comply with legal and regulatory cybersecurity requirements, and confidentially share requirements with the City Chief Information Security Officer. Department requirements that should be equivalent to or greater than the citywide security requirements.
i. When appropriate, consult with the City Chief Information Security Officer when gathering the requirements for new information systems to ensure the security design is vetted before selection and deployment.

4. **Department of Emergency Management**
    a. Activate the city emergency operations center to coordinate response to emergency level cyber event as outlined in Emergency Support Function 18 Unified Cyber Command.
    b. Support Citywide cybersecurity emergency exercise for City leaders in coordination with the City Chief Information Security Officer.

5. **Department Disaster Preparedness Coordinators (DPC)**
    a. Train department leadership and cybersecurity incident response staff with Department and Emergency Operation Center roles and responsibilities
    b. Work with the DISO to adopt the reporting processes for Emergency Support Function 18 Unified Cyber Command.
    c. Participate, at least annually, in the department cybersecurity emergency exercise.

6. **COIT and Mayor's Budget Office** shall:
    a. To the extent possible, adequately support and fund City and Department cybersecurity operations in alignment with the risk assessment.

7. **Chief Data Officer** shall:
    a. Work with the City Chief Information Security Officer to develop and maintain an information classification system and support departments in their data classification efforts.

8. **City Services Auditor** shall:

a. Evaluate City cybersecurity efforts with regular readiness assessments and assist in the evaluation of cybersecurity audit controls.
b. Review, at least annually, department implementation plans for adoption of citywide and department-specific cybersecurity requirements.
c. Perform security testing for departments in alignment with the citywide cybersecurity requirements to validate that departments effectively implement the requirements.
d. Share results of this testing with the Department Head, and when requested, facilitate the discussion of potential risk reduction strategies between the department and the City CISO.

9. **City Employees, contractors, and vendors** shall:
    a. Comply with cybersecurity practices, requirements, and acceptable use agreement, and promptly report any incidents to the appropriate officials.

COMPLIANCE

To the extent resources allow:

1. Department heads are accountable for ensuring that systems procured, operated, or contracted by their respective department or commission meet the appropriate security protections required by the system's risk category /classification, in addition to any regulatory requirements.
2. Employees, consultants, and vendors shall ensure that information resources are appropriately and securely utilized, administered, and operated while authorized access is granted, according to the Acceptable Use Policy.
3. City Services Auditor shall evaluate City cybersecurity efforts and validate departments' implementation of the applicable security requirements.

EXCEPTIONS

No exceptions to this policy will be approved.

AUTHORIZATION

SEC. 22A.3. Of the City's Administrative Code states, "COIT shall review and approve the recommendations of the City CIO for ICT standards, policies and procedures to enable successful development, operation, maintenance, and support of the City's ICT."

REFERENCES

- NIST Cybersecurity Framework Website - http://www.nist.gov/cyberframework/
- Cyber Safe SF which contains documentation for the CCSF cybersecurity requirements and ESF-18 Unified Cyber Command - https://sfgov1.sharepoint.com/sites/TIS-National-Cybersecurity-Awareness

DEFINITIONS

For a list of definitions please refer to:
http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Citywide Data Classification Standard

PURPOSE AND SCOPE

This Data Classification Standard (Standard) is an implementing standard of the forthcoming Data Policy and Citywide Cybersecurity Policy.

The provisions of this Standard apply to the City and County of San Francisco (City) and its component departments, agencies, offices, commissions and other governmental units (departments). All employees and other data users (defined below) are responsible for adhering to this Standard.

This Standard does not alter public information access requirements. California Public Records Act or the San Francisco Sunshine Ordinance requests and other legal obligations may require disclosure or release of data from any classification.

REQUIREMENTS

Departments must:

1. Categorize and label or mark data per the classification levels in Table 2 below as part of the annual data inventory process set out in the Data Policy. Where a range of data classes are held within a single system, Departments should prioritize classifying the system (not individual datasets) according to the highest classification of data held within it. However, this should not hinder the security objective of "availability" as set out in Table 1 below.
2. Review classification of data on a regular basis, but no less than annually as part of the annual data inventory process set out in the Data Policy.
3. Review and modify the data classification as appropriate when the data is de-identified, combined or aggregated.

Departments should follow the guidelines below when using this Standard:

1. **Appendix A**, which provides a step-by-step procedure for classifying data according to this data classification scheme.
2. **Appendix B**, which provides examples of data in each classification level.

Once data is classified, Departments should refer to:

1. The Citywide Cybersecurity Policy and its associated standards for the risk assessment framework and methodology to select appropriate security controls for the classes of data they collect and maintain.
2. The Data Policy and its associated standards for data management and privacy principles that apply to the classes of data they collect and maintain.

COIT Policy Dates
Approved: October 27, 2017
Next Review Date: FY 2018-19

DATA CLASSIFICATION OBJECTIVES

Table 1 sets out objectives for data classification, as defined by the Federal Government's FISMA (Federal Information Security Management Act) information security framework and supporting FIPS (Federal Information Processing Standard).

Table 1. Data Classification Objectives

Security objective	FISMA Definition *[44 U.S.C., Sec. 3542]*	FIPS 199 Definition
Confidentiality	"Preserve authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information..."	A loss of **confidentiality** is the unauthorized disclosure of information.
Integrity	Avoid "improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity..."	A loss of **integrity** is the unauthorized modification or destruction of information.
Availability	"Ensure timely and reliable access to and use of information..."	A loss of **availability** is the disruption of access to or use of information or an information system.

DATA CLASSIFICATION

Table 2 contains descriptions of each data classification and its associated potential adverse impact.

Table 2. Data Classification

Data class	Description	Potential adverse impact
Level 1 Public	Data available for public access or release.	None - Low
Level 2 Internal Use	Data that is normal operating information, but is not proactively released to the public. Viewing and use is intended for employees; it could be made available Citywide or to specific employees in a department, division or business unit. Certain data may be made available to external parties upon their request.	Low
Level 3 Sensitive	Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions.	Low - Moderate
Level 4 Protected	Data that triggers requirement for notification to affected parties or public authorities in case of a security breach.	Moderate
Level 5 Restricted	This data poses direct threats to human life or catastrophic loss of major assets and critical infrastructure (e.g. triggering lengthy periods of outages to critical processes or services for residents).* **Before classifying data as Level 5 Restricted, you should speak with leadership in your department and the City's Chief Information Security Officer. Only in rare instances will data be classified at this level. For example, in the federal NIST guidance, homeland security, national defense and intelligence information is classified as "high" impact.*	High

ROLES AND RESPONSIBILITIES

Data Stewards must:

- As set out in Requirements above, determine the appropriate classification of the data generated by the department according to the Standard, in consultation with their department's Cybersecurity Officer or Liaison, Data Custodian, Privacy Officer, legal counsel, risk management and/or other staff as needed;
- Review and/or modify the classification of the data as set out in Requirements above.
- Ensure communication of the data classification when the data is released or provided to another entity; and
- Ensure that appropriate privacy and security controls are implemented with respect to the data classification.

Cybersecurity Officers or Liaisons must:

- Advise on acceptable levels of risk and the appropriate level of security controls for information systems in accordance with this Standard and the Citywide Cybersecurity Policy.

Privacy Officers must:

- Adequately support their department's Data Stewards to classify data and adhere to the Data Policy and its implementing standards.

Data Custodians must:

- Adequately support their department's Data Stewards and Cybersecurity Officer or Liaison in conducting their roles and responsibilities in this Standard.

City Chief Information Security Officer must:

- Adequately support departments in their efforts to classify data and adhere to the Citywide Cybersecurity Policy and its implementing standards.

City Chief Data Officer must:

- Adequately support departments in their efforts to classify data and adhere to the Data Policy and its implementing standards.

Data users must:

- Obtain permission to collect, access or use data from the Data Steward or their designee (this includes pre-set permissions based on job assignment);
- Comply with the handling and security requirements specified by their department's Cybersecurity Officer or Liaison or their designee; and
- Be familiar with federal, state and local confidentiality or privacy laws pertaining to the data they collect, access, use, or maintain in conducting their work.

AUTHORIZATION

SEC. 22D.2. of the City's Administrative Code states, "Each City department, board, commission, and agency ("Department") shall:

1. Make reasonable efforts to make publicly available all data sets under the Department's control, provided however, that such disclosure shall be consistent with the rules and technical standards drafted by the CDO and adopted by COIT and with applicable law, including laws related to privacy.
2. Review department data sets for potential inclusion on DataSF and ensure they comply with the rules and technical standards adopted by COIT.
3. Designate a Data Coordinator…."

REFERENCES

- Citywide Cybersecurity Policy
- Data Policy
- NIST (National Institute of Standards and Technology) 800-60 Vol. 2 Rev. 1
- San Francisco Administrative Code

DEFINITIONS

Table 3 defines terms used in this Standard. Please refer to the Data Policy for other definitions.

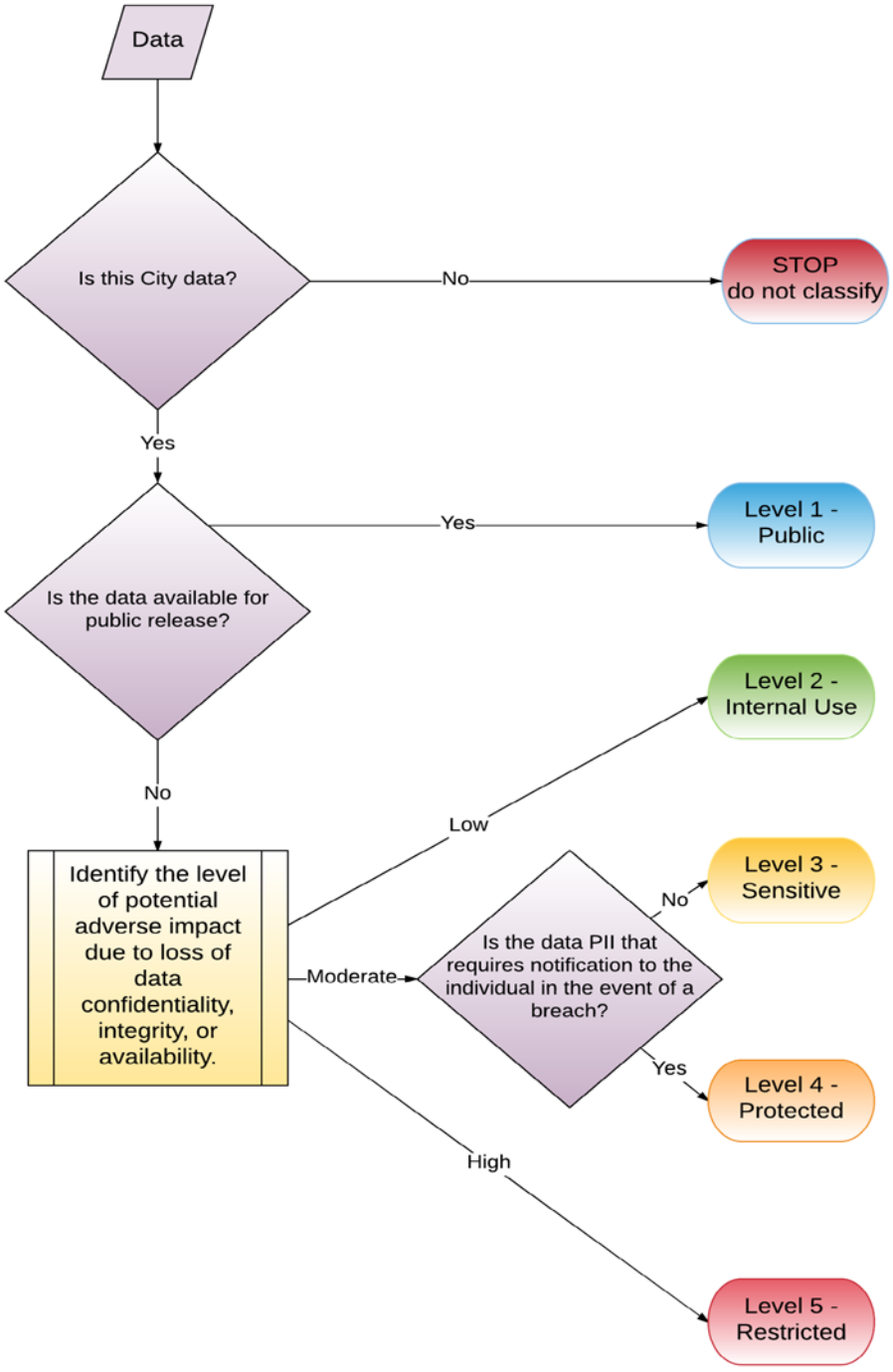
Table 3. Definitions

Term	Definition
Cybersecurity Officer or Liaison	The Cybersecurity Officer or Liaison appointed by each department as set out in the Citywide Cybersecurity Policy
Data	Information prepared, managed, used, or retained by a department or employee of the City or a data user relating to the activities or operations of the City, including personally identifiable information (PII) defined below. Data excludes any incidental employee or data user PII that is not related to (i) the activities or operations of the City or (ii) their status as an employee, volunteer, contractor, grantee, affiliate or agent of the City.
Data Coordinator	The City employee designated by a department as the main point of contact and coordination for data management and classification in their department.
Data Custodian	The person responsible for the technical environment (e.g. database or system). The Data Custodian and Steward may be the same person for small teams. The Data Custodian may be a contractor for some technical environments.
Data Steward	The person with day-to-day management responsibility of individual databases, datasets, or information systems. In general, a data steward has business knowledge of the data and can answer questions about the data itself.
Data user(s)	A City employee, contractor, or other individual affiliated with the City who is eligible and authorized to collect, access and/or use the data. A dataset may have more than one user group.

Personally identifiable information (PII)	Any data about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
Privacy Officer	The City employee designated by a department as the main point of contact and accountability for privacy. Not all departments will have a Privacy Officer.

APPENDIX A

Diagram 1. Data Classification Procedure



Step 1: Is this City data?

Data is:

- Information prepared, managed, used, or retained by a department or employee of the City or a data user, AND
- Relates to the activities or operations of the City, including:
    - Personally identifiable information (PII);
    - Data originating from external sources but managed, used or retained by the City; and
    - PII relating to a person's status as an employee, volunteer, contractor, grantee, affiliate or agent of the City.

Data excludes:

- Any incidental employee or data user PII that is **not** related to (i) the activities or operations of the City or (ii) their status as an employee, volunteer, contractor, grantee, affiliate or agent of the City.

Step 2: Is the data available for public release?

Caution: You must ensure this data is not regulated by any laws limiting its public release. If it is, proceed to Step 2. Data available for public release will be classified as **Level 1: Public.** That's it, you are done!

Step 3: Identify the level of potential adverse impact due to loss of confidentiality, integrity or availability

The following set of resources will help you identify the level of potential adverse impact due to loss of data confidentiality, integrity or availability. These resources cover 3 areas:

A. A template to document your decision-making
B. Understand the levels of potential adverse impacts (low, medium, high)
C. Choose the level(s) that apply to your data for each security objective (confidentiality, integrity, availability)

a) A template to document your decision-making

The form below can help you to structure and record your decision-making in this step.

Information System Name:			
Business/operations supported:			
Data Types:			
[Name of data type 1]	[Detail on type of data]		
[Name of data type 2]	[Detail on type of data]		
[Name of data type 3]	[Detail on type of data]		
Data Type	**Confident. Impact**	**Integrity Impact**	**Availability Impact**
[Data type 1]	[None, Low, Moderate, High]	[None, Low, Moderate, High]	[None, Low, Moderate, High]
[Data type 2]	[None, Low, Moderate, High]	[None, Low, Moderate, High]	[None, Low, Moderate, High]
[Data type 3]	[None, Low, Moderate, High]	[None, Low, Moderate, High]	[None, Low, Moderate, High]
Final Categorization	**[None, Low, Moderate, High]**	**[None, Low, Moderate, High]**	**[None, Low, Moderate, High]**
	Overall Impact: [None, Low, Moderate, High]		

b) Understand the levels of potential adverse impacts

FIPS 199 defines three levels of potential adverse impacts - low, moderate, and high - on organizations or individuals in the event of a loss of confidentiality, integrity, or availability.

FIPS 199 Potential Adverse Impact Levels

Potential Adverse Impact Level	**Definition**
Low	The potential impact is **low** if—The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

Moderate	The potential impact is **moderate** if—The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
High	The potential impact is **high** if—The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

FISMA also provides impact level definitions for each of the three security objectives: confidentiality, integrity, or availability.

FISMA Potential Adverse Impact Levels by Security Objective (Confidentiality, Integrity, Availability)

Security Objective	Potential Adverse Impact		
	Low	Moderate	High
Confiden-tiality	Unauthorized disclosure could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	Unauthorized disclosure could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	Unauthorized disclosure could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	Unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

c) Choose the potential adverse impact level(s) that apply to your data

Most of the time, you can use the levels already chosen in NIST (National Institute of Standards and Technology) 800-60 Vol. 2 Rev. 1 - see pp. 4-6 and pp.104-107. We strongly encourage you to refer to the detailed data classification tables. The tables cover most government information types and are separated into Management & Support (pp.4-6) and Mission-based (pp.104-107).

If you are still not sure, consider the following:

- **Question 1**: Will a loss of confidentiality, integrity, or availability lead to:
    - Loss of critical City operations?
    - Negative financial impact (e.g. money lost, lost opportunities, value of the data)?
    - Damage to the reputation of the City?
    - Violation of applicable laws, regulations, policies or standards?
    - Potential for regulatory or legal action (e.g. in relation to breaches or intellectual property)?
    - Potential harm to the individuals to whom the data pertains?
    - Requirement for corrective actions or repairs (e.g. notify to individuals about a breach)?
- **Question 2**: How will the data be used and what impact will the intended use have on the classification assigned to the data?
    - Departments with unique missions and business objectives should take those needs into consideration. In some cases, departments may be obligated to share as much of their data as possible with the public or other outside departments while others may be under the stricter constraints in ensuring that their data is protected against disclosure.
    - Is this metadata? Consider the potential sensitivity of metadata itself when determining whether or not to classify at the same level as the associated data.

Step 4: If applicable, consider whether notification requirements apply to PII

- **Question 1**: Does your department collect or maintain PII? PII is defined in Section II. Definitions of this Standard.
    - If no, ignore this final step.
    - If yes, proceed to Question 2.
- **Question 2**: Is the PII regulated by state or federal laws or regulations -or otherwise restricted by contract, grant, or other agreement - requiring notification to individuals in the event their PII is improperly disclosed due to a breach or privacy or security?
    - If no, the PII will be classified as **Level 3: Sensitive**.
    - If yes, the PII will be classified as **Level 4: Protected**.

APPENDIX B

The following are examples of types of data by classification level. Your data may differ from the examples below. Use the Data Classification Procedure in **Appendix A** above for additional help.

Data class	Examples
Level 1 Public	• Open data • Public websites • Press releases • Job announcements • Public reports • Bid/contract/RFP listings • Certain financial data and reports • Health or building inspection information • Notices about future construction projects
Level 2 Internal Use	• Employee phone directory • Draft reports, memos, and meeting minutes • Internal project documents • Intranet • Fuel consumption/fleet management data • Learning management data • Some financial data • Some audio and video recordings
Level 3 Sensitive	• Personnel records (including employee name + DSW number, performance appraisals) • Personally identifiable information (PII) not triggering statutory notification requirements • Certain public safety/criminal record data • Sensitive Security Information (SSI) • Physical security access logs • Investigative data (e.g. related to citations, legal proceedings) • Trade secrets/proprietary/commercially sensitive data • Internal risk management and mitigation data • Central property management information
Level 4 Protected	• Social security number • Driver's license number • California ID number • Payment Card Industry (PCI) data and other customer financial information • Protected health information (PHI)
Level 5 Restricted	• Certain network/infrastructure information

City and County of San Francisco
Carol Isen
Human Resources Director

Department of Human Resources
Connecting People with Purpose
www.sfdhr.org

Confidentiality Form for Human Resources Representatives
with Access to the City's Human Resources Systems

Employee Name: _____

Employee Job Class: _____Title: _____

Phone Number: _____ Email: _____

Department: _____ Division: _____

Supervisor Name: _____

Supervisor Job Class: _____Title: _____

Phone Number: _____ Email: _____

System(s) to which the employee will have access (complete each applicable section below):

_____

The City is committed to ensuring its internal and external clients trust the environment(s) in which their personal data is stored. This includes, but is not limited to, the City's human capital management and applicant tracking systems. City employees with access to confidential information (system users) are responsible for preserving this trust.

System users must adhere to the following policies, restrictions, and requirements at all times. If you are not clear about any of the rules and policies detailed here, please consult your supervisor, manager, departmental personnel officer, and/or the Department of Human Resources. Violation of any of these terms may lead to discipline, up to and including termination, and possible restriction on future employment with the City.

****

Requirements and Restrictions on All Users of any City Human Resources System

"Confidential information" includes, but is not limited to data, records, information, or materials regarding:

- Personal Information: This includes, but is not limited to, the individual's home or email address, social security number, medical records, health information, ADA/disability information, age, gender, ethnicity, marital status, conviction history, etc. Disclosure of this information would infringe upon an individual's right to privacy. Individual includes, but is not limited to, an applicant, candidate, employee, previous employee, or retiree.

- Examination or Applicant Pool-Related Information: This includes, but is not limited to, the names and numbers of applicants who have filed job application data, test design (e.g., numbers of test questions), assessor ratings, examination answer keys, examination-related statistical data, scoring criteria, failure results and candidate test performance. Such information is considered confidential if: 1) it has not been appropriately released to the public and is exempt from disclosure under public records laws; or 2) it would provide any candidate with an actual or perceived unfair advantage over others.

In the interest of ensuring the secure and proper use of confidential information, and out of respect for the privacy of others, the following requirements and restrictions apply to all users who have access to any of the City's human resources systems and/or the confidential information they contain:

1. The disclosure or dissemination of, or allowing access to, confidential information or materials (whether intentional or otherwise) without the express approval of the Human Resources Director or authorized designee is strictly prohibited. Disclosure or dissemination of confidential information, or allowing disclosure to other parties or colleagues, is authorized only when it is legally required to do so and/or when it is essential to the operation of the City, and strictly on a need-to-know basis.
2. Every effort is made to limit access to confidential information to those individuals who have a legitimate business reason to access it. Even if a user gains access to confidential information, it is understood that information may only be used in the conduct of official City business and individual duties. Access privileges to all human resources information systems are issued to individuals with the understanding that they may use the information obtained by virtue of such access only in the conduct of their official duties.
3. Confidential information must be properly safeguarded and kept confidential at all times. Confidential information must never be left unattended or unsecured.
4. Users must maintain the confidentiality of passwords to the human resources system. Sharing passwords is strictly prohibited.
5. Users must develop, maintain, and view the information/data in a strictly confidential manner, and only as authorized. The information developed and/or viewed may not be shared in any manner with others who are not authorized to access it.
6. Access to, or use of confidential information/data contained in a human resources system for any unauthorized purpose is strictly prohibited.
7. Users are required to consult with their supervisors if they are unclear about whether information is considered confidential, or whether any particular individual is authorized to receive confidential information.
8. Inappropriate use of privileges to access and use data may result in loss of access to the system and possible disciplinary action, up to and including termination.

By signing below, I acknowledge that I have received and read this confidentiality form, and that I will adhere to all the above policies, restrictions and requirements at all times regarding any City human resources system to which I have access.

Employee Signature: _____ Date: _____

Supervisor Signature: _____ Date: _____

****

Additional Restrictions and Requirements for JobAps Users

This section must be completed by individuals with access to JobAps

Actual or perceived breaches in the security of examinations and/or examination materials, and actual or perceived favoritism in examinations, undermine public trust and candidate confidence in our employment and selection processes. Users with access to JobAps are required to adhere to the following additional requirements and restrictions:

1. An employee may be an applicant for an announcement to which the employee has been given access in JobAps. Similarly, an employee may have a close friend or family member (spouse, domestic partner, child, legal ward, grandchild, foster child, parent, legal guardian, grandparent, brother, sister, cousin, father-in-law, mother-in-law, sister-in-law, father-in-law, and/or any individual living with the employee with whom the employee has some familial relationship) who is an applicant for an announcement to which the employee has access in JobAps. In an effort to avoid possible perceptions of impropriety or conflicts of interest, employees are required to notify their supervisor(s) or DHR's Selection and Hiring Resources Director when these situations occur, so that adjustments can be made, if appropriate, to the employee's job assignment and/or JobAps access.
2. Employees who know about discussions regarding confidential JobAps information are prohibited from discussing, disclosing or disseminating that information to unauthorized individuals without the express approval of the Human Resources Director or authorized designee.
3. Employees are prohibited from giving confidential information contained in JobAps to any person who would use it to improve or injure anyone's prospects or chances of being appointed, employed, or promoted.
4. Employees are prohibited from—either by themselves or by aiding another—falsely marking an application, falsely marking or grading an examination, or falsely estimating or reporting upon the examination or proper standing of any person examined.
5. Employees are prohibited from disclosing information regarding candidate test performance prior to its appropriate release to the public.
6. System users are also required to report any violations by candidates or City employees of any of the above policies.

By signing below, I acknowledge that I have received and read the above terms regarding my access to JobAps, and I agree to adhere to all of the above policies, restrictions, and requirements at all times.

Employee Signature: _____ Date: _____

Supervisor's Signature: _____ Date: _____

SAN FRANCISCO
HEALTH SERVICE SYSTEM

Confidentiality of Health Information and Non-Disclosure Agreement

I have read and understand the San Francisco Health Service System (SFHSS) policies regarding the privacy of individually identifiable health information (or protected health information ("PHI")), pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the State of California Civil Code Section 56-56.16 (Confidentiality of Medical Information Act).

In addition, I acknowledge that I have received training concerning the use, disclosure, storage and destruction of PHI as required by HIPAA and the State of California.

I further understand that, through my employment or affiliation with the San Francisco Health Service System, I will be exposed to privileged, intimate and personal information in addition to PHI (such information and PHI shall collectively be referred to as "PHI" herein).

I hereby agree that I will not at any time—either during or after my employment/affiliation with SFHSS—use, access or disclose PHI in any manner to any person or entity, internally or externally, except as is required and permitted in the course of my duties and responsibilities and as permitted under their privacy policies and procedures as adopted and amended from time to time or as permitted under HIPAA and the State of California. I understand that this prohibition includes, but is not limited to, disclosing any information about the identity of the people with whom I work or any information about them, including their medical and other personal information, to family, friends, other patients, other clients, or co-workers, unless such person is lawfully authorized to receive such information.

I agree that I will immediately report any knowledge of an impermissible use or disclosure of PHI to the San Francisco Health Service System Privacy Officer.

I understand that my personal access code, user ID, and password can be used to access PHI and must be kept confidential at all times. I understand that I will not remove from SFHSS any devices or media that contain PHI unless instructed or authorized to do so. I agree to return all means of access to PHI upon termination of my employment/affiliation with SFHSS.

I understand that unauthorized use or disclosure of PHI will result in disciplinary action, up to and including the termination of employment and could result in the imposition of civil and criminal penalties under applicable laws.

I understand that my obligations will survive the termination of my employment/affiliation with SFHSS, regardless of the reason for such termination. I understand that my obligations extend to any PHI that I may acquire during the course of my employment/affiliation whether in oral, written or electronic form and regardless of the manner in which access was obtained.

I understand that as an employee or affiliate of the City and County of San Francisco's HSS, I have an obligation to complete Confidentiality of Health Information/HIPAA Training on an annual basis, and in signing this agreement, I confirm that I have completed confidentiality training.

Signature: _____ Date: _____

Printed Name: _____ DSW Number: _____

Form Reviewed: July 18, 2018

SF People & Pay
Security & Access Request Form – Health Service System

Section I: Request Type

☐ New User ☐ Modify Existing User ☐ Delete Existing User

Section II: Employee Information

User Name:		**Employee ID:**	
Department / Division:		**Dept. Start Date:**	
Working Job Title:		**Job Code:**	

Section III: Job Responsibilities

Job Responsibilities determine the SF People & Pay pages the employee will be granted access. Use only the below options to indicate Job Responsibilities to be added or removed for the employee. If you are submitting a Modify Existing User request and need to know what access the user currently has, contact sfemployeeportalsupport@sfgov.org.

***A** = Add Job Responsibility for employee*

***R** = Remove Job Responsibility for employee*

A / R	Job Responsibility	System Access & Tasks
	View Only	View job data, benefits data, benefits comments and financial information.
	Benefits Analyst	Process new hires for benefits, enroll employees, verify benefit plans, process terminations, make family status changes, enroll members in billing, manage job data for benefits and send deduction requests.
	Senior Benefits Analyst	Make corrections. Run benefits reports and processes.
	Benefits Manager	View configuration tables. Make corrections. Run benefits reports and processes.
	Benefits Finance	Process over the counter payments, perform deduction calculations and reconciliation, perform delinquency reconciliation, access financial reports

Section IV: Department Approval

I certify that I am a manager at the Health Services System and approve this access.

Print Name: _____

Signature: _____ **Date:** _____

NOTE: Employees must successfully complete the appropriate training provided by HSS.

User Security Approval Processing:

- Employee & Supervisor signs the SF People & Pay Security & Access Request and Confidentiality Agreement forms
- System Access Approver submits SAR and Confidentiality Agreement to sfemployeeportalsupport@sfgov.org.
- System access is granted. All training for HSS-specific functions are provided internally by the Department.

SAN FRANCISCO
HEALTH SERVICE SYSTEM

SFHSS PRIVACY AND INFORMATION PROTECTION POLICY AGREEMENT

The San Francisco Health Service System (SFHSS) is a Covered Entity as defined in the Health Insurance Portability and Accountability Act of 1996. Under those provisions as well as the California Confidentiality of Medical Information act (CMIA), SFHSS and its Business Associates must comply with privacy and protection of protected health information (PHI). PHI includes personally identifiable information combined with medical information. Examples of PHI include, but are not limited to:

- Names
- Addresses
- Dates (except year) Birth, Death, etc.
- Phone/Fax Numbers
- SSN
- Health Plan Beneficiary Numbers
- Email
- Account Numbers
- Dates of Services / Admission
- Claim Numbers
- Prescriptions
- Notes/Clinical History
- Plan Enrollment
- Premiums
- Procedures
- Diagnosis

Additionally, employees and contractors of SFHSS also may have access to a variety of confidential or sensitive information, including personally identifiable information, examples which include, but are not limited to:

- Name
- Address
- Phone
- Email
- Marital Status
- SSN
- Compensation
- Payroll Deductions
- Race / Ethnicity
- Gender
- Dependent information
- Social Security Numbers
- Job Data (Hire dates, Leaves, Terminations, Disability, etc.)

SFHSS manages and operates Enterprise-Level Systems containing PHI/PII which include:

- SalesForce
- Hyland Perceptive Content (ECM)

PHI and PII is also stored on network drives to which you may have access.

The Controller's office manages and operates Enterprise-Level Systems accessed by SFHSS containing PHI/PII which include:

- PeopleSoft Human Capital Management (HCM) – The system of record for human resource, benefits, and payroll functions Citywide.
- PeopleSoft Financials & Supply Chain Management (FSCM) – The system of record for financials, purchasing and supply chain management Citywide.

It is the obligation of City employees and contractors to only access such Confidential Information if required by their assigned duties and to protect all Confidential Information that can be accessed through these systems.

By signing this document, I acknowledge that I am required to maintain the confidentiality of personal or confidential or sensitive/protected information.

1. Specifically certify that I will only access Confidential Information when I have a legitimate business reason and in the course of carrying out my assigned duties. I will not seek, delete or alter information for which I do not have a legitimate business reason to know, use, add or amend.
2. Will take every reasonable precaution to prevent unnecessary or unauthorized access to any passwords, user identifications, or other information that may be used to access information systems, whether those systems belong to DT or others.
3. Will keep my login password private from other users and protect the login password from discovery or use by others.
4. Will not allow any unauthorized individual to use or view information through my login.
5. Will treat all information encountered in the performance of my duties as confidential unless and until advised otherwise by my supervisor.
6. Will seek guidance from my supervisor or the SFHSS Privacy Officer whenever I am unsure of the correct decision regarding the appropriate use and confidentiality of information and will do so before taking any action that might compromise that use or confidentiality.
7. Will not share, record, transmit, alter, copy, or delete confidential information in the information systems except as required in performance of my job duties, including printing or copying such information to personal or contractor equipment or destinations unless having prior approval from SFHSS or authorized designee.
8. Will protect Confidential Information from all disclosure or dissemination by properly safeguarding the information and never leaving the Confidential Information unattended or unsecured.
9. Will take reasonable action to ensure the accuracy of data I enter into City and SFHSS systems.
10. Will immediately notify my supervisor if I believe Confidential Information has been improperly disclosed.

The employee or City contractor understands that inappropriate access or use of Confidential Information or inappropriate use or disclosure of login passwords.

A violation of these requirements is considered a serious offense and can lead to loss of access to Systems and possible disciplinary actions, up to and including dismissal, criminal and civil penalties.

By signing this document, I acknowledge that I am required to maintain the confidentiality of such information.

_____ _____ _____

Name of Contractor/City Employee Signature Date

I have read and understand the attached City policies (please initial):

Data Classification Standard _____ Citywide Cybersecurity Policy _____