Citywide Data Classification Standard - DRAFT

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: TBD
Next Review Date: TBD

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. 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."

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.

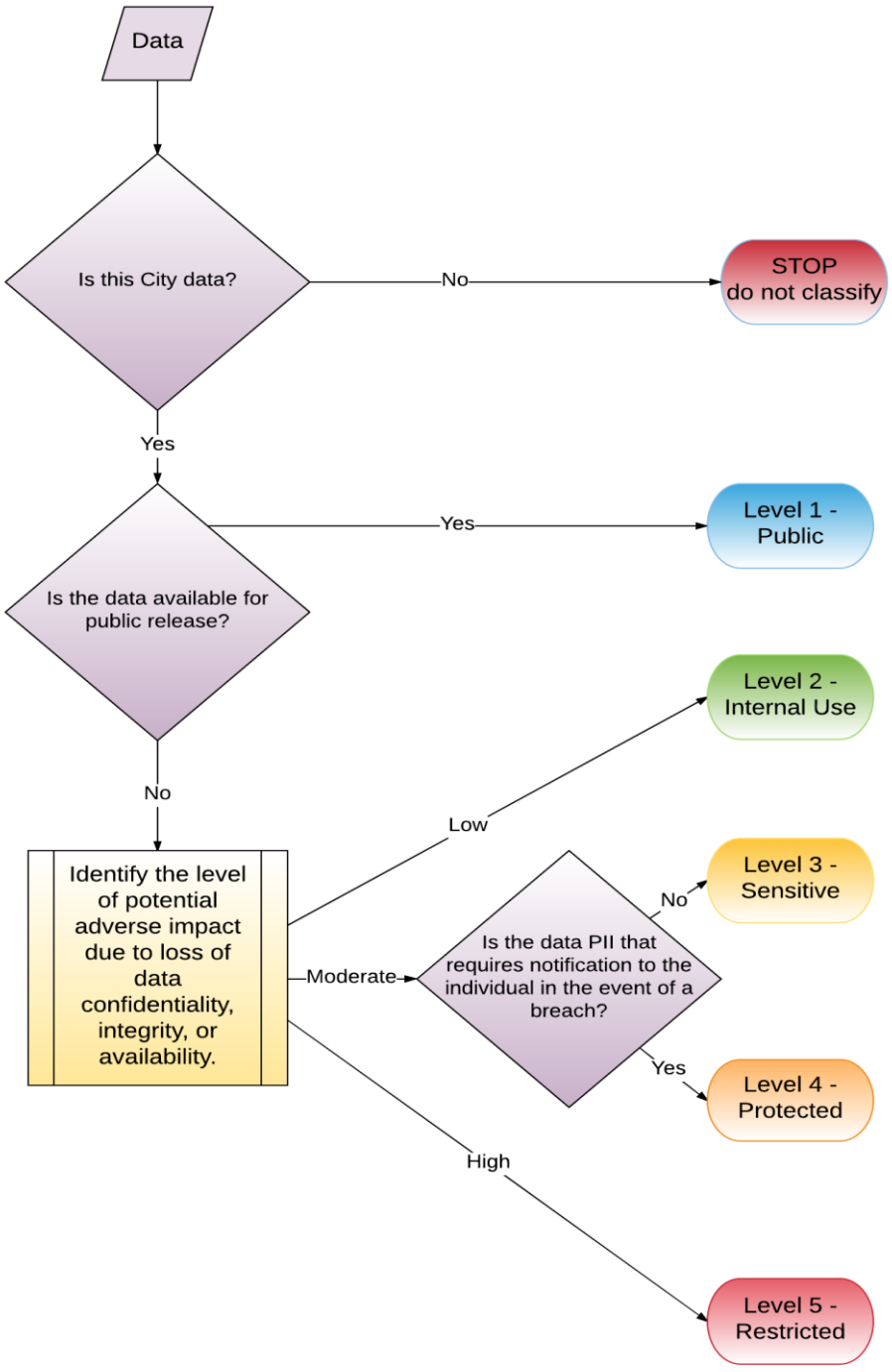
Table 3. Definitions

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