1. POLICY INTENT

This document establishes the San Francisco Department of Public Health (SFDPH) policy for the classification of information by its degree of sensitivity. The classification assigned to an item of information controls: who has access to it, who may make changes to it, who may transmit it to what places and how it is stored and disposed of. The policy intends to allow the most effective use of SFDPH security resources to protect information from security threats, improve control of sensitive information, and provide accountability for information use. This policy is intended to comply with those sections of the Code of Federal Regulations that govern HIPAA requirements for Information Security. The section that relates to the Classification of Information is CFR 164.308(a)(7).

Definition: “INFORMATION” is data that is organized stored, processed or transmitted in electronic, optical or digital form. For the purposes of this policy, ‘Information’ also includes ‘RAW DATA’, which is unorganized facts – demographics, statistics, diagnostics, treatments etc., in the form in which they were originally gathered. ‘Information’ specifically does not include matter that is printed, written or spoken. Although these types of information are also subject to classification, they are regulated by their own policies.

Inclusion by Reference: JCAHO, California State Law and other relevant sets of mandatory standards for classifying, labeling, storage, protection, disposal etc. of privileged/sensitive/patient information are included as part of this policy by reference.

2. POLICY STATEMENTS

All information must be classified by its criticality to the organization, its vulnerability to being compromised and its sensitivity to causing legal complications if it has been revealed to unauthorized persons. Additionally, information will be classified on the basis of the particular jobs (Roles) that have a ‘Need-to-Know’ that information.

2.1. Four-Level Classification: Not all information is critical to business operations or patient treatment, nor is it possible to equally protect all information held and used by a business. All
information owned by or entrusted to SFDPH is assigned to one of four sensitivity classifications. If not specifically designated, the default classification is **Internal Use Only**.

- **Legally Defined Sensitive Information**: Information that, by law, requires more stringent control than routine professional ethical guidelines and business operational information cover. Protected Health Information (PHI) - is the primary type of Sensitive Restricted Information that SFDPH deals with. Subsets of Protected Health Information may have additional legislative or administrative restrictions and associated penalties for violations - Examples include information related to Mental Health, Substance Abuse treatment, Sexually Transmitted diseases, and health service involving minors. Access to this information must be limited to as few persons as possible and to only those with a legitimate and specific ‘Need-to-Know’. Such information must be tightly controlled from creation through destruction. Access to or release of this health care information requires, except as defined by law, specific written authorization to be released, from the subject of the data their legal guardian or by specific, legally executed court order such as a subpoena. *(California Welfare and Institutions Code §5330; California Welfare and Institutions Code §14100.2. (h); Title 9, California Administrative Code, Section 942; Code of Federal Regulations Title 45.)*

- **Confidential Data**: Access to this information must be tightly restricted, based on professional good practices and the concept of need-to-know. Disclosure requires, except as defined by law, formal approval by the subject of the information, their legal guardian or by legally executed subpoena. Examples include, but are not limited to: HIPAA “Protected Health Information” (PHI), confidential patient information as defined by Health-related professional codes of ethics (see citation at end of paragraph), and personal information about employees and employment-related information subject to laws, regulations or collective bargaining agreements. *(California Welfare and Institutions Code §5330; California Welfare and Institutions Code §14100.2. (h); Title 9, California Administrative Code, Section 942; Code of Federal Regulations Title 45.)*

- **Internal Use Only**: This information is provided freely to all internal workforce members via the organization's intranet and written communications. It may be disclosed to third parties only if a confidentiality agreement has been signed and disclosure is not expected to cause serious harm to SFDPH, examples include the organizational telephone book and staff’s automated calendars.

- **Public**: This information has been explicitly approved by Management or the Public Information Office as suitable for public dissemination, or is explicitly covered by the ‘Sunshine Laws’ of the City and County of San Francisco and the State of California.
relevant state and federal laws and regulations. Examples include Commission meeting minutes and press releases.

2.2. ‘RESTRICTED INFORMATION’: Is a blanket term for information encompassing the first two bullet points of section 2.1 above, plus the following additional items:

2.2.1. System Administration and System Maintenance passwords and access codes.

2.2.2. The computer operating systems, files and applications required to provide security to Confidential Information.

2.2.3. Computer operating systems, files and applications without which the Department would be unable to operate and provide its services to the people of San Francisco.

2.3. Role-Based Classification: Each job role ‘Needs to Know’ specific information, in order to accomplish its duties. Conversely, no role ‘Needs to Know’ everything, for example System Engineers need access to a computer’s operating system, but they do not need access to the patient data stored on the computer. For this reason, Restricted Information is further subdivided within the larger overall classification scheme to permit control of information based on each job role’s Need-to-Know (refer to the Information Access Control Policy and the Access Control Administration Policy).

3. STANDARDS and GUIDELINES

3.1. By default - any information which involves an individual patient or employee is to be treated as confidential, regardless of whether it has been formally classified and/or labeled. Information about the diagnosis, treatment and prognosis of a patient’s health is the most sensitive information that a Health Care organization handles. Because of this, any document, system or medium of transmission and storage of this information is to be protected regardless of whether it has been labeled as confidential or not.

NOTE: “Protected Health Information (PHI)”: Is the term used within the Federal HIPAA Privacy and Security regulations to designate ANY health information that can be identified as pertaining to a particular individual. Refer to section 6.1 of this document for the details of the regulation’s definition of PHI.

3.2. Restricted information is subject to formal structured controls, including but not limited to:
3.2.1. Required, standardized labeling of media by classification (see section 2.1) and need-to-know category of content.

3.2.2. Elevated security requirements for access, storage, use, transmission and disposal.

3.2.3. Required Audit Trail procedures, including, but not limited to:

   3.2.3.1. Required signing in-and out of storage and documentation of transportation and receipt of media classified as Restricted.

   3.2.3.2. Logging, tracking and reporting of all access and use of Restricted Data, including specific reporting separate from general network and system access and use.

   3.2.3.3. Required documentation of the disposal of media.

   See Section 6.2 for the detailed standards for implementing the above. (To be developed.)

4. RESPONSIBILITIES

4.1. It is the Responsibility of SFDPH Executive Management to:

   4.1.1. Set and enforce Enterprise-wide standards for the classification of information.

   4.1.2. Set and enforce Enterprise-wide standards and procedures for the labeling, handling, transportation and disposal of information, devices and media based on the classification of their contents.

   4.1.3. Ensure that Third Parties are contractually obligated to follow SFDPH policies when using information, devices and media based on the classification of their contents.

4.2. It is the Responsibility of the SFDPH CIO/CISO to:

   4.2.1. Implement SFDPH-wide policy for data classification and ultimately for the safety and security of the SFDPH Enterprise Network. The SFDPH CIO or designee must approve all exceptions to this policy.

   4.2.2. Advocate, represent and support DPH-IT security needs, concerns and projects to ‘Chief Officer’ and ‘Division Director’ level Senior management.
4.2.3. Development, deployment and maintenance of policies for the application of Data Classifications to SFDPH Data.

4.2.4. Directing the development and promulgation of training and orientation materials to enable and encourage employee awareness of the security problems and issues involved in the classification and handling of SFDPH information.

4.2.5. Directing the monitoring, and analysis of the state of compliance and risk-management of existing Information Classification programs and procedures.

4.3. **SFDPH Information Technology (DPH-IT)** is responsible for establishing standards and procedures for the secure *electronic* handling, transmission, storage and disposal of Information that has been classified as Restricted.

4.4. **Local-Unit Management** is responsible for establishing *local* operational standards and procedures for the secure use, handling, transmission, storage and disposal of information that has been classified as Restricted.

4.5. **Individual information users** are responsible for protection of the information that has been entrusted to their care. All workforce members who come into contact with "sensitive" information are expected to familiarize themselves with this Information classification policy and to consistently use it in their SFDPH business activities. Although this policy provides overall guidance, to achieve consistent information protection, workforce members will be expected to apply and extend these concepts to fit the needs of day-to-day operations.

5. **PENALTIES FOR VIOLATIONS:**

5.1. **General Workforce Violations:** Violation of published Information Security Policy, standards, guidelines, rules or procedures are subject to the same progressive discipline processes and sanctions as any other violation of the terms and conditions of employment at SFDPH.

5.2. **Individual Non-Employee and Third Party Workforce Violations:** Violation of published Information Security Policy, standards, guidelines, rules or procedures by persons employed through a third party or otherwise not subject to the progressive discipline processes and sanctions of the terms and conditions of employment at SFDPH are subject to the sanctions provided under the terms and conditions of the agreement(s) whereby their services are provided.
5.3. **Trusted Workforce member Violations:** Managers, System Engineers, System Administrators and other classifications who are given greater than routine access to and control of critical information systems and data may be subject to stricter standards of security behavior and more abrupt and stringent penalties in the case of violations.

5.4. **Contractor and Third Party Entity Violations:** In addition to the individual sanctions noted in 2.1 and 2.2 above, third party organizations, business entities and others who are contractually required to comply with SFDPH Security Policies and standards may be subject to specified monetary fines or penalties or termination of the agreement as required for by the written contract and criminal penalties provided for in the applicable laws and regulations.

6. **ATTACHMENTS**

6.1. **Procedures to be created:**

   6.1.1. Identification, Classification and Labeling of Protected Health Information.

   6.1.2. Identification, Classification and Labeling of other than - Protected Health Information that may require safeguards.

   6.1.3. Access, storage, use, transmission and disposal of classified information, including:

   - Required signing in-and out of storage and documentation of transportation and receipt of media classified as Restricted.

   - Logging, tracking and reporting of all access and use of Restricted Information, including specific reporting separate from general network and system access and use.

   - Documentation of the disposal of media containing or previously containing Restricted Information.

6.2. **Definition of Protected Health Information** - CFR section 160.103 gives the following definition: “Protected Health Information means individually identifiable health information:

   (1) Except as provided in paragraph (2, below) of this definition, information that is:

   (i) Transmitted by electronic media;
(ii) Maintained in electronic media; or
(iii) Transmitted or maintained in any other form or medium.

(2) Protected Health Information excludes individually identifiable health information in:

(i) Educational records covered by the Family Education and Privacy Act, as amended, 20 U.S.C. 1232g;
(ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
(iii) Employment records held by a covered entity in its role as employer.”

6.3. **Specifics of Standard labeling, Security Measures, Audit Trail etc.** *To be added when developed.*