California DEPARTMENT OF TECHNOLOGY	3113

DATA CLASSIFICATION STANDARD			
OWNER:	Security Management Branch	**ISSUE DATE:**	6/6/2007
DISTRIBUTION:	All Employees	**REVISED DATE:**	12/31/2015

This document was last reviewed/updated in December, 2015.

SECTION 1 - INTRODUCTION

Data classification standards and methods are adopted to protect the confidentiality, integrity, and availability of data. The California Department of Technology (CDT) will adopt and abide by the following data classification standard requirements owned by the Department of General Services (DGS) as indicated in the State Administrative Manual (SAM) section 5305.5 and the Statewide Information Management Manual (SIMM) section 5305-A.

IMPORTANT: System data in the hosted environment must be classified by the customer and disclosed to the Office of Technology Services (OTech) staff; specifically the Customer Representative and/or Account Manager. The owner of the file or database is also responsible for informing OTech staff of the classifications and sub-classifications that is contained therein. Hosted systems containing unclassified data will be classified with the most restrictive security measures by default.

SECTION 2 – STANDARD REQUIREMENTS

Part I - Data Classifications

SIMM section 5305-A specifically states the following:

“Subject to executive management review, the agency unit that is the designated owner of a record (paper or electronic, including automated files, or databases) is responsible for making the determination as to whether that record, file, or database should be classified as public, or confidential, and whether it contains personal, and/or sensitive data. The owner of the record, file, or data is responsible for defining special security precautions that must be followed to ensure the integrity, security, and appropriate level of confidentiality of the information.

The state's records, automated files, and databases are essential public resources that must be given appropriate protection from unauthorized use, access, disclosure, modification, loss, or deletion. Each agency must classify each record, file, and database using the following classification structure:

1. **Public Information** - information maintained by state agencies that is not exempt from disclosure under the provisions of the California Public Records Act (Government Code sections 6250-6265) or other applicable state or federal laws.

2. **Confidential Information** - information maintained by state agencies that is exempt from disclosure under the provisions of the California Public Records Act (Government Code sections 6250-6265) or other applicable state or federal laws.

Sensitive Information and Personal Information, as defined below, may occur in Public Information and/or Confidential Information. Records, files, and databases containing sensitive and/or personal information require special precautions to prevent inappropriate disclosure. When confidential, sensitive or personal information is contained in public records, procedures must be used to protect it from inappropriate disclosure. Such procedures include the removal, redaction or otherwise masking of the confidential, sensitive or personal portions of the information before a public record is released or disclosed.

While the need for the agency to protect data from inappropriate disclosure is important, so is the need for the agency to take necessary action to preserve the integrity of the data. Agencies must develop and implement procedures for access, handling, and maintenance of personal and sensitive information.

1. **Sensitive Information** - information maintained by state agencies that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive information may be either public or confidential. It is information that requires a higher than normal assurance of accuracy and completeness. Thus the key factor for sensitive information is that of integrity. Typically, sensitive information includes records of agency financial transactions and regulatory actions.

2. **Personal Information** - information that identifies or describes an individual as defined in, but not limited by, the statutes listed below. This information must be protected from inappropriate access, use, or disclosure and must be made accessible to data subjects upon request.

    a. **Notice-triggering personal information** - specific items or personal information (name plus Social Security Number, driver's license/California identification card number, or financial account number) that may trigger a requirement to notify individuals if it is acquired by an unauthorized person. See Civil Code sections 1798.29 and 1798.3.

    b. **Protected Health Information** - individually identifiable information created, received, or maintained by such organizations as health care payers, health care providers, health plans, and contractors to these entities, in electronic or physical form. State laws require special precautions to protect from unauthorized use, access or disclosure. See Confidentiality of Medical Information Act, Civil Code section 56 et seq. and the Patients' Access to Health Records Act, Health and Safety Code sections 123100-123149.5.

    c. **Electronic Health Information** - individually identifiable health information transmitted by electronic media or maintained in electronic media. Federal regulations require state entities that are health plans, health care clearinghouses, or health care providers that conduct electronic transactions to ensure the privacy and security of electronic protected health information from unauthorized use, access, or disclosure. See Health Insurance Portability and Accountability Act, 45 C.F.R. parts 160 and 164.

    d. **Personal Information for Research Purposes** - personal information requested by researchers specifically for research purposes. Releases may only be made to the University of California or other non-profit educational institutions and in accordance with the provisions set forth in the law, including the prior review and approval by the Committee for the Protection of Human Subjects (CPHS) of the California Health and

Human Services Agency before such information is released. See Civil Code section 1798.24(t)."

Part II – Information Categorization

Listed below are additional categories that align with the above data classifications.

Information Category	Reference Document(s)
Notice triggering Personal Identity Information (PII)	Civil Code sections 1798.29 and 1798.3
Protected Health Information (PHI)	Confidentiality of Medical Information Act, Civil Code section 56 et seq. and the Patients' Access to Health Records Act, Health and Safety Code sections 123100-123149.5
Electronic Patient Health Information (EPHI)	Health Insurance Portability and Accountability Act, 45 C.F.R. parts 160 and 164
Payment Card Information (PCI)*	Payment Card Industry (PCI) Security Standards Council in their Data Security Standard (PCIDSS)
Federal Tax Information (FTI)	Internal Revenue Service (IRS) Code, Section 6103 and is covered by the IRS Publication 1075, "Tax Information Security Guidelines for Federal, State and Local Agencies and Entities"

***Payment Card Information** – financial information as defined by the Payment Card Industry (PCI) Security Standards Council in their Data Security Standard (PCIDSS). The most common example of PCI data requiring protection is the Primary Account Number (PAN), but additional items that must also be protected if stored with the PAN include Cardholder Name, Service Code, and Expiration Date. Customer (internal and external) information technology (IT) systems and environments must be technically architected in a PCI compliant manner.*

SECTION 3 – APPLICABILITY AND EXCLUSIONS

A. This Standard applies to CDT IT resources and to anyone accessing these resources. Direct any questions regarding the applicability of this Standard to the Security Management Branch for clarification.

B. Exceptions to this Standard must be documented and will be considered on a case-by-case basis. Requests for an exception to this Standard must be submitted via the Security Policy/Standard Exception Request Form, TECH 358.

SECTION 4 – AUDITING AND REPORTING

A. Auditing may be performed on a periodic or random basis by the Security Management Branch or its designees. In the event an audit determines this Standard is not being applied, notification will be sent to the appropriate person for remediation.

B. Any known violations of this Standard must be reported to the CDT Chief Information Security Officer and the reporting employee's immediate supervisor.

SECTION 5 – AUTHORITY/REFERENCES

State Administrative Manual (SAM) section 5305.5

Statewide Information Management Manual (SIMM) section 5305-A
Government Code sections 6250-6265
Civil Code section 56
Civil Code section 1798.24(t)
Civil Code sections 1798.29 and 1798.3
Health and Safety Code sections 123100-123149.5
Health Insurance Portability and Accountability Act, 45 C.F.R. parts 160 and 164
Committee for the Protection of Human Subjects (CPHS)
California Health and Human Services Agency
Payment Card Industry Data Security Standard (PCIDSS)
United States of America Code – Title 26, Section 6103
Internal Revenue Service Publication 1075
Security Policy/Standard Exception Request Form, TECH 358

Please contact your OTech Customer Representative for the below document:
3100 - Asset Protection Policy