UNIVERSITY
OF
CALIFORNIA

UCOP
ITS
Systemwide CISO Office
Systemwide IT Policy

UC Protection Level Classification Guide

Revision History

Date:	By:	Contact Information:	Description:
08/16/17	Robert Smith	robert.smith@ucop.edu	Approved by the CISOs for consideration by ITLC and shared governance. Interim until approved by ITLC
5/29/18	Robert Smith	robert.smith@ucop.edu	Administrative update, added page of pages in the footer.
7/xx/18	Robert Smith	robert.smith@ucop.edu	Added GDPR, Security Documents

Classification Guide: Protection Levels for Institutional Information and IT Resources

UC's Institutional Information and IT Resource Classification Standard specifies that all UC Institutional Information and IT Resources must be assigned one of four Protection Levels based on confidentiality and integrity requirements, with P4 requiring the highest level of protection and P1 requiring a minimal level of protection. The process outlined in the Institutional Information and IT Resource Classification Standard provides guidance on determining Protection Levels.

Proprietors, with the support of their Security Subject Matter Experts (SMEs) and Unit Information Security Leads (UISLs), are responsible for determining the Protection Level for Institutional Information and IT Resources under their area of responsibility.

> **Note**: Be careful when classifying information. Over-classification may result in additional cost and compliance requirements. Under-classification may result in inadequate protections that could lead to data breaches.

Proprietors can refer to the charts below to appropriately classify Protection Levels. If the Institutional Information or IT Resource in question is not included in this chart, Proprietors should consult their Chief Information Security Officer (CISO), Privacy Officer or Compliance Officer for guidance.

There are definitions of acronyms at the end of this guide.

PROTECTION LEVEL 4

INSTITUTIONAL INFORMATION TYPE	JUSTIFICATION
Building access systems	Life and safety
Certain types of Federal data (Pre-CUI) – like HIPAA data.	FISMA
Code signing certificates or keys.	Operational integrity
Controlled Unclassified Information (CUI).	Government contract
Covered Technical Information (CTI) – this includes CTI and Covered Defense Information (CDI) DFARS 252.204-7012.	Government contract
Credit card cardholder information.	PCI
Disability information or other medical information collected from students to provide services.	Regulation
Financial aid information, student loans.	GLBA
Financial, accounting, payroll information.	Integrity
Human subject research data with individual identifiers, particularly identifiers listed in CA law.	Privacy, regulatory
Individually identifiable genetic information (human subject identifiable).	Privacy, regulatory
Information with contractual requirements for P4-level protection.	Contract

INSTITUTIONAL INFORMATION TYPE	JUSTIFICATION
Passwords, PINs and passphrases or other authentication secrets that can be used to access P2 to P4 information or to manage IT Resources.	Operational integrity
Personal Information (California Code) and/or Personally Identifiable Information (PII) when contained in large sets and when containing a comprehensive set of information about a person. Example 1: Information about a person's work-related accident that contains medical records. Example 2: GDPR special categories (Article 9 'sensitive') of identifiers.	PII, regulatory
Private encryption keys.	Operational integrity
Protected Health Information (PHI) / patient records.	HIPAA
Research information classified as Protection Level 4 (P4) by an IRB or otherwise required to be stored or processed in a high-security environment.	Academic integrity
Sensitive Identifiable Human Subject Research data.	Privacy
Social Security Numbers – subset of PII.	PII, GLBA, regulatory

PROTECTION LEVEL 3

INSTITUTIONAL INFORMATION TYPE	JUSTIFICATION
Animal research protocols.	Academic integrity
Attorney-Client Privileged Information.	Legal protection
Building entry records from automated key card systems.	Protective information
Certain types of federal data (Pre-CUI).	FISMA
Exams (questions and answers).	Academic integrity
Export Controlled Research (ITAR, EAR).	Regulation
IT security information, exception requests and system security plans.	Protective information
Personally Identifiable Information (PII) and Personal Data as defined in GDPR contained in large sets (Article 4).	Civil code, regulation
Research information classified as Protection Level 3 (P3) by an Institutional Review Board (IRB).	Academic integrity
Security camera recordings, body worn video system recordings, and cameras recording cash handling or payment card handling areas.	Protective information, contract
Student education records.	FERPA

INSTITUTIONAL INFORMATION TYPE	JUSTIFICATION
Student special services records. These records may contain information needed to provide services or plan accommodations, but for which the student has an expectation of privacy.	FERPA, privacy
UC personnel records.	Privacy
Video recordings.	Privacy, information integrity

PROTECTION LEVEL 2

INSTITUTIONAL INFORMATION TYPE	JUSTIFICATION
Building plans and information about the university physical plant.	Operational integrity, protective information
Calendar information that does not contain P3 or P4 information.	Operational integrity
De-identified patient information (with negligible re-identification risk).	Academic integrity
Meeting notes that do not contain P3 or P4 information.	Operational integrity
Patent applications and work papers, drafts of research papers.	Academic integrity, operational integrity
Research using publicly available data.	Operational integrity
Routine business records and email that does not contain P3 or P4 information.	Operational integrity
UC directory (faculty, staff and students who have not requested a FERPA block).	Operational integrity
Unpublished research work and intellectual property not classified as P3 or P4.	Academic integrity

PROTECTION LEVEL 1

INSTITUTIONAL INFORMATION TYPE	JUSTIFICATION
Course catalogs.	Intended for public use
Hours of operation.	Intended for public use
Parking regulations.	Intended for public use
Press releases.	Intended for public use
Public event calendars.	Intended for public use
Public-facing websites with Institutional Information intended for unrestricted access.	Intended for public use
Published research.	Intended for public

INSTITUTIONAL INFORMATION TYPE	JUSTIFICATION
	use

Special Cases

Records that are assigned a legal “Notice of Duty to Preserve” may not necessarily qualify as attorney-client privileged information. Unit Information Security Leads and Proprietors must consult with Location Counsel to determine if a higher Protection Level is required when specific records are subject to a Duty to Preserve. At no time may the Protection Level be lowered.

KEY TERMINOLOGY:

Attorney-Client Privileged Information: Confidential communications between a client and an attorney for the purpose of securing legal advice. For the privilege of confidentiality to exist, the communication must be to, from or with an attorney.

Controlled Unclassified Information (CUI): Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations and government-wide policies, but that is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

> **Note**: IS-3 and supporting standards lay the foundation for protecting CUI. See NIST Special Publication 800-171 for requirements.

EAR/ITAR: Export Controlled Research includes information that is regulated for reasons of national security, foreign policy, anti-terrorism or non-proliferation. The International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR) govern this data type. Current law requires that this data be stored in the U.S and that only authorized U.S. persons be allowed access to it. Examples:

- Chemical and biological agents.
- Scientific satellite information.
- Certain software or technical data.
- Military electronics.
- Certain nuclear physics information.
- Documents detailing work on new formulas for explosives.

Family Educational Rights and Privacy Act (FERPA): Records that contain information directly related to a student and that are maintained by UC or by a person acting for the university. The Family Educational Rights and Privacy Act (FERPA) governs release of, and access to, student education records.

Federal data (Pre CUI): The Federal Information Security Management Act (FISMA) requires federal agencies and those providing services on their behalf to develop, document and implement security programs for information technology systems and to store the data on U.S. soil. Under some federal contracts or grants, information collected by the university or information systems used by the university to process or store research data needs to comply with FISMA.

FISMA: The Federal Information Security Management Act (FISMA) requires federal agencies and those providing services on their behalf to develop, document and implement security programs for information technology systems and store the data on U.S. soil. Under some federal contracts or grants, information collected by the university or information systems used by the university to process or store research data needs to comply with FISMA. Examples:

- National Institutes of Health.
- NASA.
- Department of Veterans Affairs.

GLBA: Student loan application information. Personal financial information held by financial institutions and higher education organizations as related to student loan and financial aid applications. The Gramm Leach Bliley Act (GLBA) provisions govern this data type.

Personally Identifiable Information (PII): A category of sensitive information that's associated with an individual person and can be used to uniquely identify, contact or locate that person. PII should be accessed on a strict need-to-know basis and handled carefully. Examples include:

- Social Security Number.
- Driver's license number.
- Passport number.
- National ID number.
- Visa identification number.

California S.B. 1386 amended civil codes 1798.29, 1798.82 and 1798.84, the California law regulating the privacy of personal information. Therefore, while Federal law and NIST uses PII, California law uses PI. UC generally opted to follow California law.

Payment Card Industry (PCI): Information related to credit, debit or other payment cards. This data type is governed by the PCI Data Security Standards.

Protected Health Information (HIPAA): Protected Health Information (PHI) is defined by the Health Insurance Portability and Accountability Act (HIPAA). PHI is individually identifiable health information that relates to the:

- Past, present or future physical or mental health or condition of an individual.
- Provision of health care to the individual by a covered entity (for example, hospital or doctor).
- Past, present or future payment for the provision of health care to the individual.

Researchers should be aware that health and medical information about research subjects may also be regulated by HIPAA.

Sensitive Identifiable Human Subject Research: Sensitive identifiable human subject research data is regulated by the Federal Policy for the Protection of Human Subjects (also called the "Common Rule"). Among other requirements, the Common Rule mandates that researchers protect the privacy of subjects and maintain confidentiality of human subject data.