UNIVERSITY
OF
CALIFORNIA

UCOP
ITS
Systemwide CISO Office
Systemwide IT Policy

UC Protection Level Classification Guide

Revision History

Date:	By:	Contact Information:	Description:
8/16/17	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.
7/19/18	Robert Smith	robert.smith@ucop.edu	Added GDPR, Security Documents
8/6/19	Robert Smith	robert.smith@ucop.edu	Addressed comments by users. Added EAR, ITAR and 10 CFR Part 810 to the P4 table. Moved Exams and Answer Keys from the P3 table to the P2 table.
10/3/19	Robert Smith	robert.smith@ucop.edu	Approved by ITLC.
6/23/20	Robert Smith	robert.smith@ucop.edu	Updated EAR description to clarify the distinction between P4 and P3.
7/18/22	Robert Smith	robert.smith@ucop.edu	Administrative update, including corrections, formatting and technical updates.

UC Protection Level Classification Guide - Protection Levels for Institutional Information and IT Resources

This guide identifies types of Institutional Information that have been pre-classified to save Institutional Information Proprietors time.

The reason for this guide is to meet the requirement of UC's Institutional Information and IT Resource Classification Standard. That 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 Protection Level 4 (P4) requiring the highest level of protection and Protection Level 1 (P1) requiring the lowest level of protection. The process outlined in the Institutional Information and IT Resource Classification Standard provides guidance on determining Protection Levels.

Institutional Information Proprietors, with the support of their 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, while under-classification may result in inadequate protections that could lead to data breaches.

Using the Protection Level Tables

Several types of Institutional Information have been assigned Protection Levels to apply applicable security controls afforded by statute, regulation, contract or other rationale. These classifications are listed in the tables below.

Institutional Information Proprietors can refer to the tables below for common types of Institutional Information that have been pre-classified.

If the Institutional Information in question is not included in the tables below, Institutional Information Proprietors must consult the UC Institutional Information and IT Resource Classification Standard.

There are definitions of acronyms and associated information at the end of this guide.

PROTECTION LEVEL 4

P4 - INSTITUTIONAL INFORMATION TYPE	JUSTIFICATION
Building access systems.	Life and safety
Code-signing certificates or keys.	Operational integrity
Covered Defense Information (CDI) - this includes Controlled Technical Information (CTI), commonly found in DFARS 252.204-7012.	Government contract
Controlled Unclassified Information (CUI).	Government contract
Credit card cardholder information.	Payment Card Industry (PCI)

P4 - INSTITUTIONAL INFORMATION TYPE	JUSTIFICATION
Disability information or other medical information collected from students to provide services.	Privacy, regulation, statute
Export Administration Regulations (EAR), International Traffic in Arms Regulations (ITAR) and 10 CFR Part 810 – Department of Energy - transfer of unclassified nuclear technology. **Note:** EAR can be P4 or P3. Contact the Export Control Office for a determination.	Regulation
Customer Information about student loans, federally funded student financial aid and other financial services listed in UC's Gramm Leach Bliley Act (GLBA) Compliance Plan.	Privacy, GLBA
Financial, accounting and payroll information (official accounting records of the university).	Integrity
Human subject research data with individual identifiers, particularly identifiers listed in law.	Privacy, regulation
Individually identifiable genetic information (human subject identifiable).	Privacy, regulation
Information with contractual requirements for P4-level protection.	Contract
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
Personally Identifiable Information (PII) and/or Personal Information (PI) 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: European Union General Data Protection Regulation (GDPR) special categories (Article 9 'sensitive') of identifiers.	Privacy, regulation, statute
Private encryption keys.	Operational integrity
Protected Health Information (PHI), Health Information, medical records and patient records.	Health Insurance Portability and Accountability Act (HIPAA), California Confidentiality of Medical Information Act (CMIA), California Information Practices Act (IPA) and other state and federal health recommendations
Research information classified as P4 by an Institutional Review Board (IRB) or otherwise required to be stored or processed in a high-security environment.	Academic integrity

P4 - INSTITUTIONAL INFORMATION TYPE	JUSTIFICATION
Sensitive Identifiable Human Subject Research data or research covered by a Certificate of Confidentiality (CoC) or the Common Rule.	Privacy, regulation
Social Security Numbers – subset of PII.	Regulation, statute

PROTECTION LEVEL 3

P3 - INSTITUTIONAL INFORMATION TYPE	JUSTIFICATION
Animal research protocols.	Academic integrity, safety
Attorney-client privileged information.	Legal protection, statute
Building entry records from automated key card systems.	Protective information
Certain types of federal data.	Federal Information Security Management Act (FISMA)
Export-Controlled Research (EAR and ITAR). **Note:** EAR can be P3 or P4. Contact the Export Control Office for a determination.	Regulation
IT security information, exception requests and system security plans.	Protective information
Personally Identifiable Information (PII) and/or Personal Data as defined in GDPR [Article 4(1)] when either is contained in large sets.	Regulation, statute
Research information classified as P3 by an 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.	Family Educational Rights and Privacy Act (FERPA)
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.	Privacy, FERPA
UC personnel records.	Privacy

PROTECTION LEVEL 2

P2 - 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
Exams (questions and answers).	Academic integrity
Meeting notes that do not contain P3 or P4 information.	Operational integrity

P2 - INSTITUTIONAL INFORMATION TYPE	JUSTIFICATION
Patent applications and related work papers that are not subject to a secrecy order issued by the federal government or other contractual restriction.	Academic integrity, operational integrity
Research using publicly available data.	Operational integrity
Routine business records and emails that do 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, drafts of research papers and intellectual property not classified as P3 or P4.	Academic integrity

PROTECTION LEVEL 1

P1 - 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 use

Special Cases

Records that are assigned a legal “Notice of Duty to Preserve” may not necessarily qualify as attorney-client privileged information. UISLs and Institutional Information Proprietors must consult with Location Counsel to determine if a higher Protection Level is required when specific records are subject to a Notice of Duty to Preserve.

Key Terminology and Acronyms

Attorney-Client Privileged (ACP) 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.

Certificate of Confidentiality (CoC): Certificates of Confidentiality (Certificate or CoC) protect the privacy of research participants by prohibiting disclosure of identifiable, sensitive research information to anyone not connected to the research except when the participant consents or in a few other specific situations. Investigators and institutions have responsibilities associated with the CoC, including: 1) informing participants about the CoC 2) not releasing participants identifiable, sensitive information except under limited circumstances 3) upholding the CoC protections and 4) informing investigators and institutions receiving a copy of protected information about the CoC protections.

Common Rule: The Federal Policy for the Protection of Human Subjects (also called the "Common Rule") regulates sensitive identifiable human subject research data. Among other requirements, the Common Rule mandates that researchers protect the privacy of subjects and maintain confidentiality of human subject data.

Covered Defense Information (CDI): 32 CFR Part 236 means unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html) that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies, and is:

> (1) Marked or otherwise identified in an agreement and provided to the contractor by or on behalf of the DoD in support of the performance of the agreement; or
>
> (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the agreement.

The term does not include information that is lawfully publicly available without restrictions. This same term is used in DFARS 252.204-7012.

Controlled Unclassified Information (CUI): Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, contracts (Federal Acquisition Regulations – FAR clauses) 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. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

---

Export Administration Regulations (EAR) and **International Traffic in Arms Regulations (ITAR):** Export-Controlled Research includes information that is regulated for reasons of national security, foreign policy, anti-terrorism or non-proliferation. EAR and ITAR 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 include:

- 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 related to a student and that are maintained by UC or by a person acting for the university. FERPA governs release of, and access to, student education records.

Federal Information Security Management Act (FISMA): 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. While such information may not yet be classified, it still requires some level of protection from unauthorized access and release.

General Data Protection Regulation (GDPR): Europe's data privacy and security law includes requirements for organizations around the world. It was drafted and passed by the European Union (EU) and imposes obligations onto organizations anywhere if they target or collect data related to people in the EU.

Gramm Leach Bliley Act (GLBA): "Customer Information" as defined in the GLBA Safeguarding Rule, 16 CFR 314.2 (incorporating other definitions from the GLBA Privacy Rule, 16 CFR 313.3). See also the UC GLBA Compliance Plan.

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

Personally Identifiable Information (PII): A generic term used to describe a category of sensitive information that is associated with an individual person and that 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:

- Any unique identification number on a government issued document commonly used to verify the identity of a specific individual. For example:
  - Social Security Number.
  - Driver's license number.
  - Passport number.
  - National ID number.
  - Visa identification number.
- Genetic data.
- Biometric information.
- Medical information or health insurance information.
- Other data elements identified in California civil code and other regulations.

Note regarding terminology: California civil codes 1798.29, 1798.82 and 1798.84 are key California laws regulating the privacy of personal information (PI). Federal law and NIST use PII, while California law uses PI. UC opted to follow the PII convention.

Protected Health Information (PHI)/Health Information/Medical Information: Individually identifiable health information governed by the Health Insurance Portability and Accountability Act (HIPAA) and California Confidentiality of Medical Information Act (CMIA). This includes individually identifiable health information held by UC or UC providers that may relate to the:

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

Researchers should be aware that health and medical information about research subjects may also be regulated by HIPAA, California Information Practices Act (IPA) or CMIA.