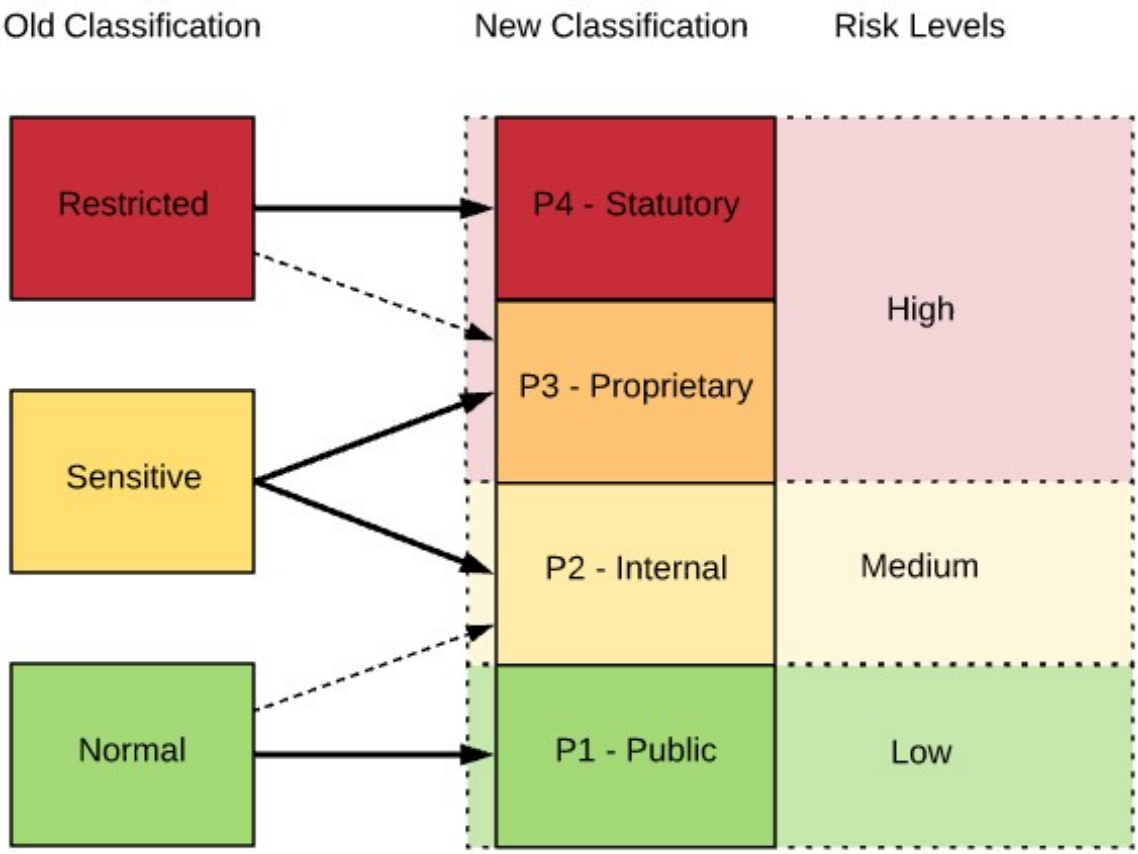
Information Security and Privacy

Data Classification

UCI is changing the way the campus classifies data in order to standardize on the new data classification scheme required by the new systemwide IT policy, IS-3. The old classification scheme used three data classifications, *Normal*, *Sensitive*, and *Restricted* which corresponded to three categories of risk, *low*, *medium* and *high*.

The new classification scheme uses four Protection Levels (defined below):

- *P1 (Public)*
- *P2 (Internal)*
- *P3 (Proprietary)*
- *P4 (Statutory)*



All information has some level of risk and a minimum level of protection requirements. There are categories of information which have higher levels of risk either because of the sensitive nature of the information (e.g. medical treatment information) or because of the value of the information (e.g. a name and social security number).

Information must be properly protected based on the value of the data and the likelihood that the data may be targeted for theft. It is important to classify information accurately as over-classification may result in additional complexity, cost and compliance requirements. Under-classification may result in inadequate protections that could lead to data compromise.

More information on the new UC Data Classification Standard can be found at: https://security.ucop.edu/files/documents/policies/institutional-information-and-it-resource-classification-standard.pdf

P1 Information (Public)

Public information or information intended to be readily obtainable by the public, but whose integrity is important and for which unauthorized modification is the primary protection concern. IT Resources for which the application of minimum security requirements is sufficient.

Examples:

- Public-facing websites
- Course catalogs
- Published research
- Press releases
- Parking information

P2 Information (Internal)

Institutional Information and related IT Resources that may not be specifically protected by statute, regulations or other contractual obligations or mandates, but are generally not intended for public use or access. In addition, information of which unauthorized use, access, disclosure, acquisition, modification or loss could result in minor damage or small financial loss, or cause minor impact on the privacy of an individual or group.

Examples:

- Routine business records

- Building plans
- Draft research papers
- Unpublished research
- De-identified research data
- UCI directory information (faculty, staff and students who have not requested a FERPA block).

P3 Information (Proprietary)

Institutional Information and related IT Resources whose unauthorized disclosure or modification could result in small to moderate fines, penalties or civil actions. Institutional Information of which unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in moderate damage to UC, its students, patients, research subjects, employees, community and/or reputation; could have a moderate impact on the privacy of a group; could result in moderate financial loss; or could require legal action. This classification level also includes lower risk items that, when combined, represent increased risk.

Examples:

- Student records
- UC Personnel records
- IT security information
- Security camera recordings
- Export-controlled research
- Personally Identifiable Information (PII)

P4 Information (Statutory)

Institutional Information and related IT Resources whose unauthorized disclosure or modification could result in significant fines, penalties, regulatory action, or civil or criminal violations. Statutory, regulatory and contract obligations are major drivers for this risk level. Other drivers include, but are not limited to, the risk of significant harm or impairment to UC students, patients, research subjects, employees, guests/program participants, UC reputation, the overall operation of the Location or essential services.

Examples:

- Credit card information
- Payroll information
- Financial aid information
- Protected health information (PHI)

- Social security numbers
- Sensitive identifiable human subject research data
- Personally Identifiable Information (PII) in large data sets

Personal Identity Information (PII)

Electronic information that includes:

1) an individual's first name or initial, and last name, in combination with any one or more of the following:

- Social Security number (SSN)
- Drivers license number or State-issued Identification Card number (including Passport)
- Financial account number, credit card number*, or debit card number in combination with any required security code, access code, or password
- Personal medical information **
- Health insurance information
- Information or data collected through the use/operation of an automated license plate recognition system

or 2) User name or email address with password or security question and answer that would permit access to an online account

* Credit card information is also regulated by the Payment Card Industry (PCI) Data Security Standard.

** Personal medical information is also regulated by HIPAA

Information Security &
Privacy
University of California,
Irvine
Irvine, CA 92697