UNIVERSITY
OF
CALIFORNIA

UCOP
ITS
Systemwide CISO Office
Systemwide IT Policy

UC Institutional Information and IT Resource Classification Standard

Revision History

Date:	By:	Contact Information:	Description:
08/19/17	Robert Smith	robert.smith@ucop.edu	Initial version, interim draft, pending ITLC approval
05/29/18	Robert Smith	robert.smith@ucop.edu	Administrative updates, fixed sentence structure to improve clarity, formatting and typos
7/15/18	Robert Smith	robert.smith@ucop.edu	Fixed broken web links. Clarified guide reference on page 8.

TABLE OF CONTENTS

Background and purpose 3
Scope 3
An overview of classification levels 3
Protection Levels 4
Availability Levels 6
Roles and responsibilities 6
Classifying Institutional Information and IT Resources 7
The classification process 7
Classifying Institutional Information 8
Classifying IT Resources 11
Special note on compliance and risk management 12
Questions on classification? 13
Standards 13
ISO 27002:2013 - Section Cross Reference 13
NIST CSF 1.1 – Section Cross Reference 13
UC Policy 14

Background and purpose

At UC, protecting our Institutional Information and IT Resources is critical to our mission of teaching, research and public service.

This Standard defines requirements for the appropriate classification of Institutional Information and IT Resources to ensure their confidentiality, integrity and availability. See the special note on compliance.

UC's Electronic Information Security Policy (IS-3) follows a risk-based approach to prescribe additional controls based on the need to achieve a specific Protection Level or Availability Level. UC's investment in security controls is commensurate with the level of need for protection or availability of the Institutional Information.

Scope

This Standard applies to all of the following:

- All UC campuses and medical centers, the UC Office of the President, UC Agriculture and Natural Resources, UC-managed national laboratories and all other UC locations (Locations).
- All Workforce Members, Suppliers, Service Providers and other authorized users of Institutional Information and IT Resources.
- All use of Institutional Information, independent of the location (physical or cloud) or ownership of any device or account that is used to store, access, process, transmit or control Institutional Information.
- All devices, independent of their location or ownership, when connected to a UC network or cloud service used to store or process Institutional Information.
- Research projects performed at any Location, and UC-sponsored work performed by any Location.

An overview of classification levels

All forms of UC electronic Institutional Information and IT Resources must be labeled with Protection Levels and Availability Levels in the associated inventory/tracking tools based on the Location/Unit Risk Assessment. The retention period for Institutional Information must also be documented.

Examples of Institutional Information include documents, records, video recordings, databases, log files and all other data in electronic form. Examples of IT Resources include personal and mobile computing devices, mobile phones, printers and other devices (both personally owned and UC-owned) that connect to any UC network.

Protection Levels

UC Institutional Information and IT Resources are classified into one of four Protection Levels based on the level of concern related to confidentiality and integrity. P4 requires the most security controls and P1 requires a minimal set of controls.

Protection Level	Potential Business Impact	Examples (not an exhaustive list)
P4 – High	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 related to a breach or compromise, the overall operation of the Location or essential services. (Statutory.)	- Protected Health Information (patient records). - Credit card data. - Controlled Unclassified Information (CUI). - Financial aid information. - Certain types of Personally Identifiable Information (PII) – Large collections or special sensitivity to privacy. - Human subject research data with individual identifiers. - Medical devices supporting care. - Industrial Control Systems affecting life and safety.
P3 – Moderate	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,	- Student records (FERPA). - Certain types of Personally Identifiable Information (PII) – not classified as P4. - Certain special services records. - Security camera recordings. - Building entry records from automated card key system. - Research results and supporting data from a 10-year study (not containing

Protection Level	Potential Business Impact	Examples (not an exhaustive list)
	employees, community and/or reputation related to a breach or compromise; 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. (Proprietary.)	P4 information). - Medical devices supporting diagnostics not containing P4 information). - Industrial Control Systems affecting operations.
P2 – Low	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. (Internal.)	- Routine e-mail not containing P3 or P4 information. - Calendar information not containing P3 or P4 information. - Meeting notes not containing P3 or P4 information. - Research using publicly available data.
P1 – Minimal	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. (Public.)	- Public-facing informational websites. - Public event calendars. - Hours of operation. - Parking regulations. - Press releases.

Availability Levels

All UC Institutional Information and IT Resources are also classified into one of four Availability Levels based on the level of business impact their loss of availability or service would have on UC. Compromises to A4 information or resources would cause the highest level of impact; compromises to A1 would cause a minimal level of service impact. A4 requires the most security controls, while A1 requires fewer security controls.

Availability Level	Potential Business Impact	Examples (not an exhaustive list)
A4 – High	Loss of availability would result in major impairment to the overall operation of the Location and/or essential services, and/or cause significant financial losses. IT Resources that are required by statutory, regulatory and legal obligations are major drivers for this risk level.	- Medical records system. - Directory services – SSO. - Border network devices. - E-mail. - Building access system. - Medical devices supporting care. - Industrial Control Systems affecting life and safety.
A3 – Moderate	Loss of availability would result in moderate financial losses and/or reduced customer service.	- Electronic sign board system. - Public website. - Time reporting system. - Building management system. - Clinical trial management system. - Medical devices supporting diagnostics. - Industrial Control Systems affecting operations.
A2 – Low	Loss of availability may cause minor losses or inefficiencies.	- Department website. - Front desk sign-in system.
A1 – Minimal	Loss of availability poses minimal impact or financial loss.	- Music streaming system.

Roles and responsibilities

Initiators identify the need to classify the Protection and/or Availability Levels of Institutional Information or IT Resources. A wide range of Workforce Member roles can

become Initiators when they acquire an application or system, or when they create or collect Institutional Information.

Proprietors must comply with this Standard and are responsible for determining the Protection Levels for Institutional Information and IT Resources under their area of responsibility. They are also responsible for determining the Availability Level of Institutional Information and IT Resources. A wide range of Workforce Member roles can also become Proprietors when they acquire or use an application or system, or when they create or collect Institutional Information. In academic settings, this includes faculty, researchers and principal investigators (PI).

Security Subject Matter Experts (SMEs) are responsible for supporting Proprietors in understanding cyber risk, determining the correct application of security controls, vetting security controls for appropriateness and making determinations on Protection and Availability Levels.

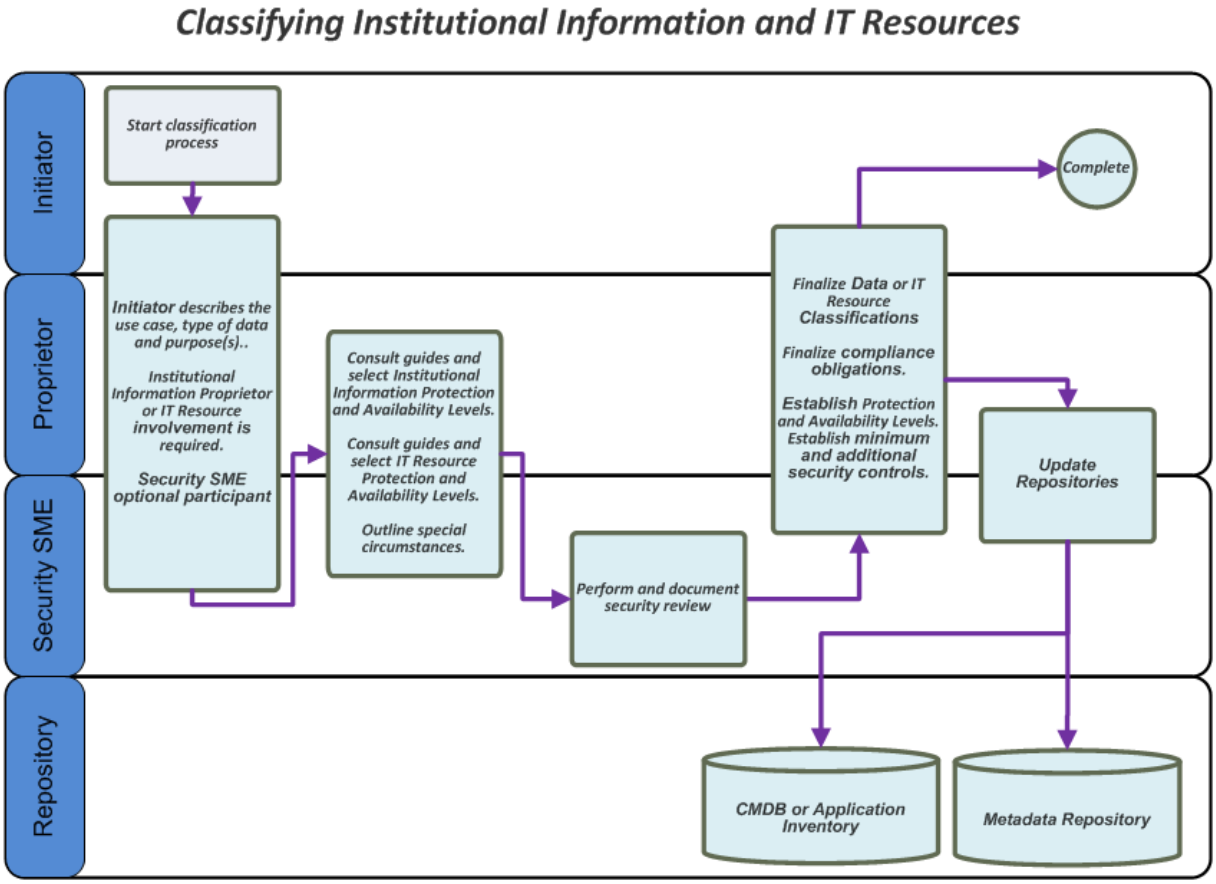
Unit Information Security Leads (UISLs) are responsible for supporting Proprietors in the determination of the Protection and Availability Level of Institutional Information and IT Resources under their area of responsibility.

If a Unit procures and/or installs a system that creates, processes, stores or transmits Institutional Information, it has created an IT Resource and must assign a named Workforce Member (or role) to act as the Proprietor. UISLs are responsible for ensuring this assignment.

Classifying Institutional Information and IT Resources

The classification process

The following diagram provides an overview of the roles and processes for the classification of Institutional Information and IT Resources:



Classifying Institutional Information

Step 1: Evaluate Institutional Information.

Proprietors must consider the following factors during the evaluation:

1. Regulatory framework. Proprietors must ensure that their use of and protection plans for Institutional Information comply with applicable laws, regulations, policies and standards. The Classification Guides outline the Protection Level and Availability Level classifications for many types of Institutional Information. For Institutional Information types not included in the guides, Proprietors must consult their Privacy Officer, Compliance Officer or CISO for guidance. Proprietors may also consult Location legal resources, the Office of the President Office of General Counsel or other Subject Matter Experts. See the special note on compliance.

2. Business impact of a loss of confidentiality, integrity or availability. Business impact can include any of the following: negative financial impact, damage to reputation related to a breach or compromise, potential for regulatory or legal action, loss of critical

campus operations, required corrective actions and/or violation of UC or campus mission, policy or principles.

The Protection Level must be commensurate with the level of need for confidentiality, integrity and availability of the Institutional Information.

> **Example**: Research data and results may be intended to be public-facing and thus could be classified at P1 or P2. However, if the research requires a high level of accuracy and integrity, it may need to be classified as P3 or P4 to protect against alteration.
> Ransomware could encrypt the data or wiper-malware could erase the data, preventing its recovery. Research Institutional Information often requires a high Protection Level to ensure that years of work are adequately protected from damage or loss.

3. Risk of harm to individuals. Proprietors must consider any potential harm or negative impact that the compromise of their data could have on the parties whose information is contained in the data. De-identified data must also be reviewed to ensure legal, regulatory and protocol requirements are met and to establish the risk of harm if the data is re-identified.

> **Example**: The use case for many industrial control systems (ICS) and medical devices involves physical health and safety. Proprietors must set the Protection Level appropriately to protect the critical function(s) that these systems may perform.

4. Required Availability Level. The use case for Institutional Information generally sets the Availability Level. Proprietors must consult the Availability Guide or perform their own analysis to make this determination. Unlike Protection Level, Proprietors may choose to select a lower Availability Level than what is specified in the guide.

> **Example**: The use case for many industrial control systems (ICS) and medical devices involves physical health and safety. Proprietors must set the Availability Level appropriately to protect the critical function(s) that these systems may perform.

5. Access needs. The decision to grant access to Institutional Information must be based on the use case as well as applicable Location policies. Proprietors must consider obligations under federal and state laws and consult their Privacy and Compliance Officers if they have any questions.

Institutional Information cannot be re-shared. The Proprietor must approve all requests for access.

> **Example**: David asks Susan for a set of Institutional Information. After considering the business need, Susan grants David access to the Institutional Information. Later, Jennifer asks David for access to the same Institutional Information. David cannot grant access to Jennifer. She must request access from Susan, the Proprietor.

If Institutional Information with higher Protection and/or Availability Levels also contains some lower-level information, the Institutional Information must be secured to meet the requirements of the highest Protection Level.

6. Data and system architecture. The type of data and where and how it is stored, processed and accessed can change the Protection Level of some parts of its associated system.

Combinations of data, particularly those that can identify an individual or group, may require higher Protection Levels according to laws, regulations or UC's privacy principles. The Institutional Information Classification Guide provides examples.

> **Example**: If all administrative functions (for power users or super-users) are separated from a general user application, it may be possible to lower the Protection Level on the user application. However, if administrative functionality is combined and intermixed with user functionality, the entire system must be set to the highest Protection Level.

7. Use case change. The Protection Level and Availability Level must be reviewed and reclassified (adjusted) if necessary when a new feature, use case or data element is introduced.

> **Example**: A purchased campus safety application adds a geo-location feature. Users can now opt in to have their location tracked so they can be found quickly in the event of an emergency. The new feature adds data that introduces an important privacy concern and warrants a Protection Level of P3 or P4.

Step 2: Select classification level.

1. Once Proprietors have considered the above factors, they must select the classification level using the classification guides and any analysis performed. If their specific data is not included in the guide, Proprietors must consult their Privacy Officer, Compliance Officer or CISO. Proprietors may also consult the Location legal resources, Office of the President Office of General Counsel or other subject matter experts. The classification guides can be found here: https://security.ucop.edu/policies/institutional-information-and-it-resource-classification.html.

> **Note**: UC's Institutional Information is considered an institutional asset and is ultimately owned by the UC Regents. Proprietors must avoid using language about ownership when documenting decisions about classification levels.

2. Proprietors may use the published Protection Level in the guide or raise it based on the specific use case, but they cannot lower it without going through the exception process described in IS-3, III.2.2, "Exception Process." However, Proprietors may raise or lower the Availability Level based on use case.

3. Proprietors must document the classification in the appropriate repository or system of record.

> **Tip**: Secured instances of inventory/asset management systems, SharePoint with versioning enabled, software version control systems, ticketing or work tracking systems and document management systems generally serve as reliable systems of record.

> **Note**: Some Locations or Units may have a metadata repository (metadata describes the data), which can also serve as a system of record.

4. The UISL receiving the Institutional Information must also record its classification in the appropriate repository or system of record for the Unit if the system of record is not shared with the Proprietor.

Step 3: Set review and retention schedules.

1. Proprietors must consult UC's Records Management Policy and record the retention schedule for the Institutional Information stored on the IT Resource. Records Managers at each Location can provide advice.

2. Proprietors must work with their Security SME to identify compensating controls and any other special issues, develop an implementation plan and document the disposition.

3. Proprietors must reclassify Institutional Information if the data, system or use case changes.

Classifying IT Resources

Step 1: Evaluate the IT Resource.

Proprietors must consider the following factors during the evaluation:

1. Institutional Information stored and processed. Proprietors must classify IT Resources based on the Institutional Information they create, store, process and transmit. See the special note on compliance.

2. Required Availability Level. The use case for the IT Resource generally determines the Availability Level. Proprietors can consult the Availability Guide or perform their own analysis to make this determination. Unlike Protection Level, Proprietors may select a lower Availability Level than what is specified in the guide.

3. Access to other systems: If the system is used to access another system, the highest Protection Level must be applied.

Step 2: Select classification level.

1. Once Proprietors have considered the above factors, they must select their classification level from the IT Resource guide and/or confirm their selection with the UISL or CISO.

2. Proprietors must document the Protection and Availability Levels in the appropriate repository or system of record.

> **Tip**: SharePoint with versioning enabled, software version control systems, ticketing or work tracking systems and document management systems generally serve as reliable systems of record.

Step 3: Set review and retention schedules.

1. Proprietors must consult UC's Records Management Policy and state retention requirements.

2. Proprietors must work with their Security SME to identify any other special issues and document disposition.

3. Proprietors must reclassify IT Resources if the data, system or use case changes.

4. Proprietors or UISLs must document the IT Resource Protection Level and Availability Level in the Location's inventory management system.

Special note on compliance and risk management

The University of California is a vast enterprise operating across a wide array of specialty areas. Units are always responsible for understanding their operating domain and correctly applying best practices and domain knowledge to information security. For example, certain chemicals, when possessed in certain quantities, require special protections for the systems that support them. Another example: Certain UC Locations handle hazardous

biological, radioactive or insect species that require special protections, including the systems that support the research and operations of those areas. This Standard and the supporting guides do not substitute for a thorough understanding and application of the laws and regulations governing operation.

Questions on classification?

Contact your Location CISO, Privacy Officer or Compliance Officer.

Standards

ISO 27002:2013 - Section Cross Reference

The requirements of this Standard are defined referencing the following sources.

Section	ISO 27002:2013 Topic
8.1.1	To identify organizational assets and define appropriate protection responsibilities.
8.1.2	Proper management of an asset over the whole asset lifecycle.
8.2.1	Classification of information.
11.1.4	Physical protection against natural disasters, malicious attack or accidents should be designed and applied.
17.1.1	The organization should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.
17.1.2	The organization should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

NIST CSF 1.1 – Section Cross Reference

Section	CSF Topic
ID.AM-1	Physical devices and systems within the organization are inventoried.
ID.AM-5	Resources (e.g., hardware, devices, data, time, software) are prioritized based on their classification, criticality and business value.

ID.BE-4	Dependencies and critical functions for delivery of critical services are established.
ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations).

UC Policy

This Standard is driven by BFB-IS-3 Electronic Information Security.