BFB-IS-3: Electronic Information Security

Responsible Officer:	Chief Information Officer & VP - Information Technology Services
Responsible Office:	IT - Information Technology Services
Issuance Date:	TBD, 2017
Effective Date:	TBD, 2017
Last Review Date:	TBD, 2017
Scope:	This policy 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. This policy does **not** apply to UC students. ● 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.

Contact: Robert Smith
Title: Systemwide IT Policy Director
Email: robert.smith@ucop.edu
Phone: (510) 587-6244

I. POLICY SUMMARY

At the University of California (UC), our knowledge and its discovery, advancement, transmission and organization are at the heart of our mission to provide world-class teaching, research and public service. Protecting the confidentiality, integrity and availability of this knowledge (Institutional Information), as well as our information technology resources (IT Resources), is critical to support our mission.

UC's Electronic Information Security Policy provides a security framework that protects Institutional Information and IT Resources from accidental or intentional unauthorized access, loss or damage, while preserving UC's collaborative academic culture.

This policy is designed to meet the following objectives:

1. Establish policy principles and goals.
Section III, subsections 1-5 provide an overview of this policy's purpose and goals; provide management direction and support for information security; specify principles to guide implementation, application and review of this policy; and describe elements expected in an Information Security Management Program.

2. Define policy requirements that govern information security at UC.
Section III, subsections 6-18 cover specific requirements for information security.

3. Outline information security requirements for Workforce Members and other users of Institutional Information and IT Resources.
Section III, subsection 7 and Section IV specify roles and responsibilities as related to information security.

II. DEFINITIONS

A comprehensive glossary of terms can be found at https://security.ucop[dot]edu/resources/IT-Policy-Glossary/index.html. **[LINK TBD, separate file for this review.**]

For ease of reference, following are definitions for several of the most commonly used terms in this policy:

Institutional Information: A term that broadly describes all data and information created, received and collected by UC.

IT Resources: A term that broadly describes information technology (IT) infrastructure and/or resources with computing and networking capabilities. These include, but are not limited to: personal and mobile computing systems and devices, mobile phones, printers, network devices, industrial control systems (SCADA, etc.), access control systems, digital video monitoring systems, data storage systems, data processing systems, backup systems, electronic and physical media, biometric and access tokens

and other devices that connect to any UC network. This includes both UC-owned and personally owned devices.

Location: A discrete organization or entity governed by the Regents of the University of California. Locations include, but are not limited to: campuses, laboratories and medical centers, health systems, as well as satellite offices, affiliates or other offices in the United States controlled by the Regents of the University of California.

Unit Head: A generic term for Dean, Vice Chancellor or similarly senior role who has the authority to allocate budget and is responsible for Unit performance.

At a particular location or in a specific situation the following senior roles may also be Unit Heads: department chairs, assistant/associate vice chancellor (AVC), principal investigators, directors or senior managers.

Unit Information Security Lead: A term for the Workforce Member(s) assigned responsibility for tactical execution of information security activities including, but not limited to: implementing security controls; reviewing and updating Risk Assessments and Risk Treatment Plans; devising procedures for the proper handling, storing and disposing of electronic media within the Unit; and reviewing access rights.

Workforce Manager: Person who supervises/manages other personnel or approves work or research on behalf of the University.

Workforce Member: Employee, faculty, staff, volunteer, contractor, researcher, student worker, student supporting/performing research, medical center staff/personnel, clinician, student intern, student volunteer, or person working for UC in any capacity or through any other augmentation to UC staffing.

III. POLICY TEXT

Section 1: General Overview

***Objective**: Provide an overview of this policy's purpose and goals, identify applicable sanctions, and establish responsibility for breach costs.*

In carrying out our mission of teaching, research, patient care and public service, UC's faculty, other academic personnel, staff, and other affiliates create, receive, transmit and collect many different types of Institutional Information. To carry out its mission, UC also maintains significant investments in IT Resources, which include information technology (IT) infrastructure, computing systems, network systems and industrial control systems.

An Information Security Management Program (ISMP) is a fundamental requirement for protecting the confidentiality, integrity and availability of UC's Institutional Information and IT Resources.

This policy establishes a minimum set of information security requirements. Risk Assessments (see Section 6) may highlight areas that require additional security requirements. The full set of security controls that must be used is the combination of the requirements set forth in this policy and the controls identified through the risk management process.

All Workforce Members share a common set of responsibilities for protecting Institutional Information and IT Resources, regardless of working location, device used, storage location (physical or cloud) or access method. Some Workforce Members carry additional security responsibilities based on their roles and functions.

1.1 Goals

This policy addresses UC's responsibilities and requirements to achieve six electronic information security goals:

1.1.1 Preserve academic and research collaboration.

UC is committed to preserving an environment that encourages academic and research collaboration through the responsible use of Institutional Information and IT Resources.

1.1.2 Protect privacy.

UC is committed to maintaining and protecting privacy for individuals. Privacy consists of: (1), an individual's ability to conduct activities without suspected or actual observation; and (2), the appropriate use and release of information about individuals.

1.1.3 Follow a risk-based approach.

UC is committed to using a risk-based approach, which allocates resources to protect Institutional Information and IT Resources based on threats and their likelihood of causing an adverse outcome. This approach balances UC's information security goals with its other values, obligations and interests.

1.1.4 Maintain confidentiality.

UC is committed to maintaining and protecting the confidentiality of Institutional Information. This requires the handling of information to ensure it will not be disclosed in ways that are inconsistent with authorized use and its original purpose.

1.1.5 Protect integrity.

UC is committed to protecting Institutional Information integrity. Integrity is the treatment of information to guard against improper modification or destruction. This includes ensuring the information is authentic.

1.1.6 Ensure availability.

UC is committed to maintaining and protecting the availability of Institutional Information and IT Resources. This requires the management of Institutional Information and IT Resources to ensure they are accessible and usable to meet UC's business and operational needs.

DRAFT

1.2 Sanctions and breach cost responsibility

The following disciplinary sanctions and cost recovery steps are authorized for confirmed and serious violations of this policy.

1.2.1 Violations and sanctions

Confirmed serious violations of this policy may result in sanctions, which are governed by:

- Policy on Student Conduct and Discipline if the student is part of the Workforce.
- Personnel Policies for Staff Members 3, 62, 63, 64 and II-64 pertaining to disciplinary and separation matters.
- As applicable, the Faculty Code of Conduct (APM - 015), University Policy on Faculty Conduct and the Administration of Discipline (APM - 016), and Non-Senate Academic Appointees/Corrective Action and Dismissal (APM-150).
- As applicable, collective bargaining agreements.
- As applicable, non-faculty medical staff disciplinary action policies.
- Other policies that specifically apply.

Confirmed serious violations of this policy may result in:

- The immediate restriction or suspension of computer accounts and/or access to IT Resources or Institutional Information as outlined in the UC Electronic Communications Policy.
- Employment or educational consequences, up to and including:
    - Informal verbal counseling and/or a written counseling memo and education.
    - Mandatory education and/or supplemental training.
    - Adverse performance appraisals.
    - Corrective or disciplinary actions.
    - Termination.

1.2.2 Costs of an Information Security Incident

Units will bear the direct costs that result from an Information Security Incident under the Unit's area of responsibility that resulted from a significant failure to comply with this policy. The costs include, but are not limited to: the response, containment, remediation, forensics, analysis, notification, litigation, penalties, regulatory fines and any other costs directly attributable to the Information Security Incident.

Section 2: Organizing Information Security

Objective: *Provide management direction and support for information security in accordance with UC requirements. Establish framework for managing exceptions and describe formal document types used to govern information electronic information security.*

DRAFT

2.1 Management direction for information security

Each Location must identify or appoint a Chief Information Security Officer (CISO). A Location may designate one or more people/roles to meet this provision, but must clearly and unambiguously make the appointment(s) to ensure scope and responsibility are understood.

Locations may create additional roles and assign responsibilities to implement this policy and the location ISMP. Locations must establish governance and processes to support the CISO responsibilities stated in this policy.

2.2 Exception process

While exceptions to an electronic information security policy or a standard may weaken protection of Institutional Information and IT Resources, they are occasionally necessary. Exception requests must be submitted to the CISO and follow the Location-approved exception process.

Units requesting an exception must explain:

- Why the exception is needed.
- The duration of the exception request.
- How any proposed compensating controls mitigate security risks that this policy would otherwise address.

Some exceptions require compensating controls. These exceptions are:

- Obligations created by an agreement, regulation or law.
- Where Institutional Information classified at Protection or Availability Level 3 or higher is involved (see “Section 8: Asset Management and Classification” for level details).
- Where IT Resources classified at Protection or Availability Level 4 are involved.

Units may also provide a cost benefit analysis when requesting an exception.

Exceptions must be approved by the CISO and a Unit Head with the level of authority that matches the risks identified. Locations may require additional approvals for exceptions.

For specific use cases, the CISO can define a standard exception plan to manage risks, implement compensating controls, and provide for periodic review.

Exception requests and decisions must be documented, periodically reviewed based on risk, and retained by the CISO as required by the UC Records Retention Schedule.

DRAFT

2.3 Policies, standards and supporting documents

Information security management requires a combination of policies and standards. Procedures and guidelines can be used to explain specific requirements and methods for implementation at a Location.

Locations may develop and approve Location-specific policies, standards, procedures, supporting guidelines, supporting checklists and supporting best practices to explain specific information security policy requirements and methods for implementation at the Location. Supporting documents may be more restrictive than this policy, but not less restrictive.

Document type	**Governance**	**Review cycle**
Systemwide Policy	University of California Policy Steering Committee	Schedule set forth by the University of California Office of the President Policy Office.
Standard	Systemwide information security standards are developed by working groups appointed by the Information Technology Leadership Council (ITLC). Standards development and approval must follow at least these steps: • Provide an opportunity for the Academic Senate and/or UC Academic Computing Committee to appoint a member to the working group. • Before the systemwide information security standard is issued, provide a timely consultation review with: o Academic Senate and/or UC Academic Computing Committee o Academic Personnel o Staff Human Resources and/or Labor Relations • Approve and record the approval and issuance of the standard. In exigent circumstances, the ITLC can issue or amend a standard on an interim basis and complete the consultation in arrears. Locations may develop additional standards using location governance.	Adhere to the documented periodic review cycle, but at least one review every three years.

DRAFT

Document type	Governance	Review cycle
Procedure	CIO-appointed committee, Unit Head or assigned designee	Adhere to the documented periodic review cycle, but at least one review every three years.
Supporting – Guide or Guideline	CIO-appointed committee, Unit Head or assigned designee	None - updated as needed.
Supporting - Checklist	CIO-appointed committee, Unit Head or assigned designee	None - updated as needed.
Supporting - Best Practice	CIO-appointed committee, Unit Head or assigned designee	None - updated as needed.

Section 3: Roles and Responsibilities

Roles and responsibilities are outlined in Part IV of this policy.

Section 4: Information Security Management Program Principles

***Objective**: Specify the principles that guide UC and each Location in the implementation, application and review of this policy and the ISMP.*

4.1 A goal-based approach is best.

To ensure sound financial and operational decisions, the goals listed in Section 1 must be used to scope, protect and make risk-based decisions about commensurate protection of Institutional Information and IT Resources.

4.2 Units are accountable for implementing information security.

The Unit Head is accountable for appropriately protecting Institutional Information and IT Resources, and managing information security risk in a manner consistent with this policy.

4.3 Decision-making rights correspond to risk level.

To protect UC and manage risk, information security and risk management decisions must be made at the level of financial, privacy, legal, reputation, brand or other organizational authority that matches the level of risk identified.

4.4 Security is a shared responsibility.

All Workforce Members are responsible for ensuring the protection of Institutional Information and IT Resources.

Understanding the risks, threats, costs and incidents associated with securing Institutional Information is a shared responsibility.

DRAFT

4.5 Security is embedded into the entire lifecycle.
Information security must be incorporated into the entire lifecycle for any system, service or software. This includes identifying, budgeting for, planning, developing, implementing and maintaining security processes and controls.

Section 5: Information Security Management Program

Objective: *Provide management direction and support of an overall Information Security Management Program in accordance with business requirements and relevant laws and regulations.*

5.1 Establish an Information Security Management Program
Locations must establish and implement an Information Security Management Program (ISMP). Multiple roles participate in executing the ISMP; see Section IV for additional details.

The ISMP must contain administrative, technical and physical safeguards designed to protect Institutional Information and IT Resources. Each Location ISMP must implement a risk-based, layered approach that uses preventative, detective and corrective controls sufficient to provide an acceptable level of information security.

5.2 Essential Information Security Management Program elements
Each Location must implement the following essential ISMP elements and carry out the supporting tasks.

5.2.1 Information security risk governance
Locations must establish an information security risk governance framework that:

- Establishes roles and responsibilities of the ISMP at the Location.
- Ensures implementation of the risk management process (see Section 6).
- Defines information security risk tolerances.
- Defines acceptable risk responses.
- Establishes an escalation protocol to manage residual risk that exceeds UC maximum tolerances.
- Advises on the allocation of resources in response to identified and prioritized risks.
- Reviews the ISMP annually to ensure it addresses changing business needs, operating environments, threat landscape, regulatory landscape and changes in technology.
- Documents review of the ISMP by the Cyber-risk Responsible Executive (CRE).

5.2.2 Unit security planning, execution and review
Units are responsible for implementing the Location ISMP for any Institutional Information and IT Resources they handle. Implementation must include:

- Budgeting to address information security risks.
- Documentation of plans, actions and reviews.
- Administrative controls.
- Technical controls.
- Physical controls.
- A layered approach using preventative, detective and corrective controls.
- Effectiveness reviews.

5.2.3 General security and awareness training

Locations must implement training, awareness campaigns, educational materials and related efforts to ensure all Workforce Members and students:

- Understand common security risks and security practices for protecting information and resources.
- Understand their roles and responsibilities in protecting Institutional Information and IT Resources, managing information security risk and reporting Information Security Incidents.

Workforce Member training must include how to comply with the Location incident reporting requirements.

5.2.4 Reporting on risk and the state of information security

Locations must implement a process for reporting risk and the state of information security to the Location leadership. The process must address:

- Frequency of reporting.
- Overall information security risk levels.
- Performance on past objectives.
- Reporting on significant changes in the environment or threat landscape and the plans to address those changes.

5.2.5 Operationalizing information security

The ISMP may address:

- Location-specific implementation of this policy.
- Assignment of responsibilities to a senior role or creation of an equivalent role.
- Information security budgeting and planning processes.
- Other Location requirements to operationalize this policy or address Location-specific requirements.

Section 6: Risk Management Process

Objective: *Ensure this policy can achieve its intended outcome(s) using a risk-based approach.*

DRAFT

6.1 Risk management minimum requirements

This section establishes minimum requirements for the UC risk management process. The Location risk management process must address the following:

- Identifying assets.
- Protecting assets.
- Detecting and evaluating Information Security Events.
- Responding to Information Security Incidents.
- Recovering from Information Security Incidents.
- Framing and assessing risk.
- Responding to risk once determined.
- Monitoring risk on an ongoing basis.
- Providing a feedback loop for continuous improvement.
- Monitoring security and compensating controls for effectiveness.

6.1.1 Risk Assessments

Risk Assessments must be completed for Institutional Information and IT Resources.

Risk Assessments may identify further security controls that must be implemented in addition to the controls required by this policy.

This section establishes minimum requirements for Risk Assessments. Risk Assessments must include:

- Identification of threats and vulnerabilities that could adversely affect Unit or Location operations, Institutional Information or IT Resources.
  - Cloud and Supplier services must be included in the Risk Assessment process for Institution Information classified at Protection Level 2 or higher.
- A risk rating scale that establishes a common perspective and ensures that Risk Assessments produce comparable and reproducible results across the Location.
- Rating of risks to determine the prioritization of mitigation. The risk rating and prioritization will determine the level of resources needed for compensating controls.
- Risk prioritization must take into account:
  - Protection Level (see Section 8.2.1, Classification of Institutional Information and IT Resources).
  - Availability Level (see Section 8.2.1, Classification of Institutional Information and IT Resources).
  - Analysis of the potential impact.
  - Specific vulnerabilities.
  - Specific threats.
  - Probability of adverse events.

6.1.2 Risk Treatment Plans

Risk management may include a Risk Treatment Plan, which is a pre-approved response plan to address pre-identified risks in a specific situation.

DRAFT

The CISO may pre-approve standard Risk Treatment Plan(s) in lieu of a full Risk Assessment. The CISO must establish when and how the Risk Treatment Plans are used and implemented.

Risk Treatment Plans must include at least the following:

- A baseline set of controls based on this policy.
- Criteria for selecting alternate controls (one set vs. another set) to manage specific risks.
- Response plans to address the prioritized risks, including implementing controls to reduce risk.
- Documented actions and decisions related to scoping, risk acceptance, residual risk, risk avoidance and risk transference.

6.1.3 Risk Assessments and Critical IT Infrastructure

The CISO must work with Location governance to identify Critical IT Infrastructure in scope for Risk Assessments.

IT Resources designated as Critical IT Infrastructure must undergo a specific Risk Assessment that includes selecting a specific set of controls appropriate for the IT Resources. The CISO must document and approve these controls.

6.1.4 Risk Assessment periodic review and updates

The Unit Information Security Lead must periodically review and adjust Risk Assessments and Risk Treatment Plans to manage risk. Reviews must occur at least:

- Once every three years, or
- Following major changes in the configuration/environment, or
- On a frequency to meet regulatory, contractual and legal requirements.

The Unit Information Security Lead must update Risk Assessments and Risk Treatment Plans when significant changes occur.

Section 7: Human Resource Security

Objective: *Ensure that Workforce Members understand their key responsibilities and are trained for their current roles or any roles for which they are considered. Ensure managers of Workforce Members communicate and facilitate strong information security practices.*

7.1 Prior to employment

Role	Key Responsibilities

Location Human Resources	Establish onboarding procedures that support information security:
	
	• In addition to background checks required by personnel policies for staff members, perform background checks for:
	  o Those with access to Institutional Information classified at Protection Level 3 or higher.
	  o Those with access to IT Resources classified at Availability Level 3 or higher.
	• Completing and documenting identify verification for access control.

Workforce Manager	When recruiting: • Establishes security duties of the position and includes them in the job description or appointment letter. • Follows the appropriate Location onboarding procedures related to information security.

7.2 During employment

Role	Key Responsibilities
Workforce Manager	Updates the information security elements of job descriptions and training requirements when job duties change. Reviews access rights annually and removes access that is no longer needed. Notifies appropriate Units and Location contact(s) in a timely manner when job responsibilities change in a way that affects Institutional Information and IT Resource access. Ensures Workforce Members complete security awareness training. Ensures IT Workforce Members have appropriate security skills and qualifications, and are educated on a regular basis, or receive training related to the security job requirements, policies, procedures, standards and best practices to maintain minimum standards of

DRAFT

	information security. Promptly addresses reported, suspected or actual policy violations.
Workforce Member	Follows applicable information security policies, procedures, standards and best practices to maintain minimum standards of information security. Completes assigned security training. Reports to their manager any access rights that are outside assigned roles or responsibilities. Reports or records to their Unit the use of any Supplier or cloud service outside of what is provided by UC or the Location when used to store or process Institutional Information. Reports to their manager any gaps in, or failure of, information security controls in the assigned area of responsibility. Does not attempt to gain unauthorized access, disrupt operations, gain access to confidential information security strategies or inappropriately alter Institutional Information. Reports possible unlawful action in accordance with UC's Whistleblower Policy to at least one of the following: ● The Locally Designated Official. ● The Workforce Member's immediate supervisor.

DRAFT

	● Other appropriate UC official.

7.3 Separation and change of employment

Role	Responsibilities
Location Human Resources (HR)	Location HR teams must establish separation and change of employment procedures that support information security and incorporate minimum security requirements set by the CISO. Employment procedures must include appropriate background checks when a Workforce Member moves into a critical position, or is granted access to Institutional Information or IT Resources classified at Protection Level 3 or higher as part of a job change.
Workforce Manager	Follows the appropriate Location separation procedures. Documents the steps taken to: ● Collect UC property, IT Resources and physical access keys/cards as applicable. ● Collect or ensure the return and/or secure deletion of Institutional Information. ● Revoke access. ● Ensure continued availability of Institutional Information required for business continuity. Ensures that information system access, including all internal, physical and remote access, is promptly revoked as appropriate. Documents approval by an appropriate Location official of any IT Resource access privileges retained after separation.
Workforce Member	Returns all UC property, IT Resources and physical access keys/cards. Returns all Institutional Information, token encryption keys and any copies. Surrenders UC-licensed software and tools.

DRAFT

7.4 Separation of duties

Workforce Managers must consider the principle of Separation of Duties when designing and defining job duties.

Workforce Managers must:

- Implement methods and controls in their area of responsibility that, to the extent feasible and appropriate, separate duties among Workforce Members so that requestor, approver and implementer are separated.
- Establish effective oversight of activities and transactions.

When functions cannot be separated, adequate administrative oversight or other compensating controls must be in place to mitigate identified risks.

Section 8: Asset Management

Objective: *Identify UC assets (Institutional Information and IT Resources) and define appropriate protection responsibilities.*

8.1 Responsibility for assets

This section identifies organizational assets and defines appropriate protection responsibilities. In the context of this policy, organizational assets include both Institutional Information and IT Resources.

8.1.1 Inventory of assets

The Unit Information Security Lead must maintain an inventory record for the lifecycle of Institutional Information and IT Resources classified at Protection Level 3 or higher handled by the Unit. The inventory record must contain at least:

- An identification of the asset.
- Identity of the Institutional Information Proprietor.
- Protection Level.
- Availability Level.
- Location of the Institutional Information or IT Resource.
- Configuration or security documentation.
- Identification of and adherence to retention requirements established in UC's Records Management Policies (RMP.)

8.1.2 Compliance with Proprietor Classification Level for Institutional Information and IT Resources

Units must comply with requirements for use and protection of Institutional Information and IT Resources based on the Classification Level set by the Proprietor.

8.1.3 Acceptable use of assets

Units must ensure that Workforce Members who are using or have access to Institutional Information and/or IT Resources:

- Comply with the applicable information security requirements as defined by this policy and standards.
- Use Institutional Information and access IT Resources in accordance with their job responsibilities.
- Comply with UC and Location Acceptable Use policies.

8.2 Institutional Information and IT Resource information security classification

Institutional Information must receive an appropriate level of protection in accordance with its classification.

8.2.1 Classification of Institutional Information and IT Resources

This policy addresses Institutional Information in electronic form. Other considerations may apply, including records management and privacy policies, and protection of paper records.

Proprietors must determine the Protection Level, summarized in the tables below, for Institutional Information and IT Resources under their area of responsibility.

Unit Information Security Leads and Proprietors must classify the Availability Level, summarized in the tables below, of Institutional Information and IT Resources under their area of responsibility.

Proprietors must comply with the UC Institutional Information and IT Resource Classification Standard.

Protection Levels and Availability Levels are used to select the security controls required by this policy and to drive key processes such as risk management.

Protection Level classifications:

Protection Level Classification	
Level	**Impact of disclosure or compromise**
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, the overall operation of the Location or essential services. (Statutory.)
P3 - Moderate	Institutional Information and related IT Resources whose

DRAFT

	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. (Proprietary.)
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.)
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 where the application of minimum security requirements is sufficient. (Public.)

Availability Level classifications:

Availability Level Classification	
Level	**Impact of loss of availability or service**
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.
A3 - Moderate	Loss of availability would result in moderate financial losses and/or reduced customer service.
A2 - Low	Loss of availability may cause minor losses or inefficiencies.
A1 - Minimal	Loss of availability poses minimal impact or financial losses.

8.2.2 Labelling of information

Units must identify Institutional Information and/or IT Resources under their control that require electronic or physical labeling.

8.2.3 Periodic review of classification
Units must review classification of Institutional Information and IT Resources periodically or when major changes occur.

8.3 Electronic media handling
Proper handling of electronic media is critical in preventing unauthorized disclosure, removal or destruction of Institutional Information.

8.3.1 Management of removable media
Units must encrypt Institutional Information classified at Protection Level 3 or higher when stored on removable media.

Units must physically and securely store removable media containing Institutional Information classified at Protection Level 3 or higher.

8.3.2 Disposal of electronic media
Units must dispose of electronic media containing Institutional Information classified at Protection Level 2 or higher, including damaged media and non-removable memory, in compliance with the UC Data Destruction Standard.

8.3.3 Physical transfer of electronic media
Units must protect electronic media containing Institutional Information against loss, unauthorized access, misuse or corruption during transportation.

Units must track and use secure methods for transfers of electronic media containing Institutional Information classified at Protection Level 2 or higher.

Section 9: Access Control

Objective: *Limit access to Institutional Information and IT Resources.*

Passwords and other authentication methods must comply with the UC Authentication Management Standard.

9.1 Business requirements of access control
Units must carefully define and manage access to Institutional Information.

9.1.1 Access control for Institutional Information
Access to Institutional Information must follow the Need to Know and Least Privilege principles.

Institutional Information classified at Protection Level 2 must have controls to prevent unauthorized access.

For Institutional Information classified at Protection Level 3 or higher, Proprietors must determine:

- Appropriate access rights.
- Restrictions for specific user roles.
- Restrictions for use by Units, Service Providers and Suppliers.
- Restrictions and allowances on the alternate uses and reuse of Institutional Information.

When granting access to Institutional Information classified at Protection Level 3 or higher, Units must:

- Segregate access rights management so that requestors, approvers and grantors are unique roles assigned to separate individuals, or implement compensating controls to address risk associated with the combination of duties.
- Maintain records that document changes to access rights and the related approvals.

9.1.2 Access to networks and network services

Access to networks and network services must follow the Least Privilege principle.

Network access to Institutional Information classified at Protection Level 4 must be routed through secure access control points.

Network access to Institutional Information classified at Protection Level 3 or higher must be monitored to detect unauthorized access.

Units granting guest or other access to networks and network services not otherwise covered under this policy must:

- Establish terms of use or acceptable use.
- Set minimum security requirements.
- Scope access and security requirements based on operational need and risk.

9.2 User access management

Units must limit access to authorized users and prevent unauthorized access to Institutional Information and IT Resources.

9.2.1 User accounts

Each Workforce Member and student must have a unique user account to distinguish that user from other users.

Workforce Members and students must not share user accounts, passwords or authentication secrets. Shared access for specific use cases must be approved through the exception process or by adopting a specific Risk Treatment Plan.

When access to Institutional Information or an IT Resource is no longer needed for UC business purposes, Units must disable or remove the access rights.

DRAFT

When access to all Institutional Information and IT Resources is no longer needed, Units must disable or remove the user account.

9.2.2 User account access rights

Units must have an approval process for granting access to Institutional Information and IT Resources. Access must be approved by the appropriate role, and the user must complete any required training prior to receiving access.

9.2.3 Management of privileged access rights

Privileged access must be assigned based on job function(s) and must include clear instructions for appropriate use.

Privileged accounts used to access Institutional Information or IT Resources must have an associated authentication credential that complies with the UC Authentication Management Standard.

Privileged accounts used to access Institutional Information and IT Resources must follow the Least Privilege Principle needed to perform the specific job function(s) and must only be used for the purpose(s) for which the access was authorized.

Privileged access accounts needed to perform installations, updates or other administrative activities must be documented and approved, and, if possible, only enabled to perform the specific administrative task(s), then disabled.

When privileged access is no longer needed for UC business purposes, the Unit must appropriately and promptly reduce or remove access.

9.2.4 Management of authentication information of users

When setting up accounts, passwords and other authentication secrets must be communicated securely to the Workforce Member.

Vendor default passwords and authentication secrets must be changed or disabled before connection to a production or generally accessible network.

9.2.5 Review of user access rights

Units must:

- Review access rights periodically, and remove or reduce rights where appropriate.
- Review access rights for Institutional Information and IT Resources classified at Protection or Availability Level 4 at least annually, and remove or reduce rights where appropriate.
- Review privileged accounts at least annually, when major changes occur, or as directed by the CISO, and remove or reduce rights removed where appropriate.

DRAFT

9.3 User responsibilities

Users must be accountable for safeguarding their passwords and authentication secrets and devices. Workforce Members must comply with the UC Authentication Management Standard.

9.4 System and application access control

Units must limit access to authorized users and prevent unauthorized access to Institutional Information and IT Resources.

9.4.1 System and IT Resource access

Units must manage access to IT Resources and associated administrative functions according the requirements set by the Proprietor.

9.4.2 Secure log-on

Log-on or authentication processes for all systems must comply with the UC Authentication Management Standard.

9.4.3 Password and authentication management system

Passwords and authentication management systems must comply with the UC Authentication Management Standard.

9.4.4 Use of service accounts and privileged utility programs

Service accounts must comply with the UC Authentication Management Standard.

Service accounts used to access Institutional Information and IT Resources must have an associated authentication credential that complies with the UC Authentication Management Standard.

Service accounts used to access Institutional Information classified at Protection Level 3 or higher, and IT Resources classified at Availability Level 4, must be disabled from interactive login or screen/user interface sessions when possible.

The installation of Utility Programs capable of overriding system and application controls on IT Resources that process or store Institutional Information classified at Protection Level 2 or higher must be approved through the change management process in this policy and must be included in the applicable Risk Assessment(s).

Section 10: Encryption

Objective: *Ensure appropriate physical access to protect UC Institutional Information and IT Resources.*

10.1 Encryption requirements

Units must select an encryption method approved for use by the CISO, and document the selection rationale.

DRAFT

Institutional Information classified at Protection Level 3 or higher must be encrypted when transmitted over a network.

Institutional Information classified at Protection Level 3 or higher must be encrypted when stored on removable or portable electronic media, laptops or mobile devices.

Institutional Information classified at Protection Level 4 must be encrypted when stored on any electronic media.

10.1.2 Security key and certificate management
Units and Service Providers must comply with the UC Encryption Key and Certificate Management Standard.

Section 11: Physical and Environmental Security

Objective: *Ensure appropriate access to protect UC IT Resources and Institutional Information.*

11.1 Secure areas
Units must document and define security perimeters and physical security to protect Institutional Information and IT Resources.

Units must implement and review at least these elements of physical security:

- Statutory, regulatory and contractual requirements.
- Institutional Information Classification.
- Area entry safeguards and controls protecting physical access to Institutional Information and IT Resources.
- Plans for ensuring that Institutional Information classified at Protection Level 3 or higher is not left unsecured where it can be accessed by unauthorized individuals.
- Administrative and physical controls on third-party access and supervision.

Physical access to secured areas must be based on job responsibilities or the Need to Know principle.

11.2 Equipment security
Keeping equipment secure helps prevent loss, damage, theft or compromise of assets, and interruption to UC operations.

11.2.1 Equipment physical protection
Workforce Members must protect IT Resources from unauthorized access, loss, theft or damage.

IT Resources must be protected based on at least these elements:

DRAFT

- Location standards.
- Location requirements for equipment disposal and reuse.
- Institutional Information contained on the device or electronic media, including during disposal or retirement.

11.2.2 Environmental requirements
Units must protect IT Resources from power failures and other disruptions caused by failures in supporting utilities or environmental controls.

11.2.3 Cabling security
Units must protect power cabling and cabling carrying Institutional Information or supporting information services from unauthorized physical access, interception, interference or damage.

11.2.4 Maintenance
Units must ensure Suppliers who service, maintain, handle or take off-site IT Resources or Institutional Information classified at Protection Level 2 and higher comply with Section III, subsection 15.

11.2.5 Removal of assets
IT Resources must be tracked according to Location inventory requirements. The tracking must include:

- Recording and labeling in accordance with approved Location asset management and inventory management requirements.
- Movement from one Location to another.

Institutional Information classified at Protection Level 3 or higher must not be taken or transmitted off-site unless authorized by the appropriate Workforce Manager or Institutional Information Proprietor.

Institutional Information classified at Protection Level 3 or higher must be adequately protected both on-site and off-site.

Section 12: Operations Management

Objective: *Ensure operational security to protect Institutional Information and IT Resources.*

12.1 Operational security and responsibilities
Units must ensure correct and secure operations of information processing facilities.

12.1.1 Documented administrative operating controls
Locations must document specific administrative operating controls to support the requirements of this policy, and the operation of IT Resource(s).

DRAFT

Documented administrative operating controls must include these elements:

- Security planning.
- Compensating technologies employed.
- Installation and configuration of systems.
- Normal processing.
- Error and exception handling.
- Defect reporting.
- Escalation.
- Special handling of media or output.
- System restart and recovery.
- Logging and monitoring in compliance with the UC Logging and Event Recording Standard.
- Data flows and data mapping.
- External IT Resources.
- Externally hosted Institutional Information.
- Critical dependencies between IT Resources and/or security tools.

12.1.2 Change management
Changes to IT Resources must be controlled and scoped through the Location change management process. This process must account for:

- Emergency changes.
- Normal changes.
- Standard changes.

The change management process must record:

- The specific change.
- The communication plan to stakeholders.
- The impacted IT Resources.
- The approval of the change.
- The date and time of the change.
- The impact on security.
- The back-out or restore plan.
- Result of the change.

12.1.3 Capacity management
Units must plan for:

- Future capacity requirements.
- Replacing or retiring unsupported IT Resources.
- Institutional Information retention and disposal requirements contained in the UC Records Management Policies (RMP).
- Decommissioning of IT Resources.

DRAFT

12.1.4 Development, testing and production environments

Units must identify the necessary level of separation between production, testing and development environments to prevent production availability or security control problems.

Changes to the production environment must be subject to the Location change management process.

Testing and development environments that contain Institutional Information must include all appropriate security controls identified for the production environment based on the Protection Level and Availability Level.

12.2 Protection from malware and intrusion

Any device connected to an authenticated or protected Location network must comply with the UC Minimum Security Standard.

Units must monitor IT Resources to detect signs of attack or compromise when any of the following are present:

- Institutional Information classified at Protection Level 2 and higher.
- IT Resources classified at Protection Level 3 or higher.
- IT Resources classified at Availability Level 3 or higher.

12.3 Backup

Institutional Information classified at Availability Level 3 or higher must be backed up and recoverable.

Retention of backups must comply with UC records retention requirements.

Backups must be protected according to the Protection Level of the Institutional Information they contain.

Removable backup media must meet the removable media requirements outlined in this policy.

Units must document and execute a plan to test restoration of Institutional Information from backups.

A backup catalog must be maintained and must show the location of each backup and retention requirements.

12.4 Logging and monitoring

Proper logging and monitoring is a required practice for recording events and generating evidence.

DRAFT

12.4.1 Event logging

Units must comply with the UC Logging and Event Recording Standard for IT Resources when storing, processing or transmitting Institutional Information.

Erasing, purging or trimming event logs outside must be approved through the change management process.

12.4.2 Protection of log information

Logs must be protected according to the Protection Level of the Institutional Information they contain and may not be released without proper authorization.

Logs must be retained according to external obligations as well as the requirements in the UC Records Retention Schedule, contracts, regulations, litigation hold or preservation orders.

12.4.3 Administrative logs

For Institutional Information classified at Protection Level 3 or higher, and IT Resources classified at Protection or Availability Level 4, Unit Information Security Leads must independently review privileged accounts periodically to ensure:

- Only authorized activity occurred.
- Anomalies are analyzed and corrective actions implemented.

For Institutional Information classified at Protection Level 3 or higher, Units must limit access to administrative logs using the Need to Know principle.

12.4.4 Clock synchronization

The clocks of IT Resources within an organization or security domain must be synchronized to a standard reference time source.

12.5 Control of operational software

Software installation, configuration changes and updates on production systems must be controlled through the Location change management process.

12.6 Technical vulnerability management and patch management

Units must only use supported and patched versions of hardware and software.

For IT Resources classified at Protection Level 3 or higher, Availability Level 4 or Critical IT Infrastructure, Units must establish and enforce minimum security configuration settings.

Units must:

- Establish and document the required patch frequency.
- Define applicable compensating controls to manage risks related to patch frequencies greater than 90 days.

DRAFT

Hardware or software that cannot be patched to current standards must be protected with compensating controls approved through the exception process or be removed from network access.

Units must regularly take the following steps:

- Assess vulnerabilities using up-to-date vulnerability scans and other sources that include third-party advisories and/or bulletins.
- Perform authenticated vulnerability scans for IT Resources that process or store Institutional Information classified at Protection Level 3 or higher.
- Perform authenticated vulnerability scans for IT Resources classified at Availability Level 4.
- Take appropriate action to patch or apply other controls.
- Document actions taken.

12.7 Information systems audit considerations

Units must support UC Internal Audit reviews, investigations, audits and other approved reviews, including those performed by Suppliers.

Units must plan and control audits to minimize adverse effects on production systems and business processes.

Audit tests must not alter audit logs or production Institutional Information.

Audit activities must not reduce security controls below what is appropriate for the Institutional Information or IT Resource Protection or Availability Level.

Auditor access to Institutional Information classified at Protection Level 3 or higher must be logged and recorded.

Section 13: Communications Security

Objective: *Ensure the security of Institutional Information in transit on networks and between parties.*

13.1 Network security management

IT Resources processing Institutional Information classified at Protection Level 3 or higher must be on segmented networks restricted to similarly classified IT Resources, and must have the ingress and egress points protected by appropriate network security controls, and/or intrusion detection/prevention tools/technologies approved by the CISO.

IT Resources processing Institutional Information classified at Protection Level 3 or higher must turn off or disable unused ports, protocols and services.

DRAFT

IT Resources processing Institutional Information classified at Protection Level 3 or higher must use secure versions of network services.

Network devices used to control access to Institutional Information classified at Protection Level 4 must:

- Use the most restrictive rules possible.
- Allow only authorized connections.
- Detect and log unauthorized access or access attempts.
- Review the network access rules.

Units using an external network service provider to interconnect with the Location network must:

- Have a Risk Assessment or Risk Treatment Plan that addresses the specific use case approved by the CISO.
- Obtain approval from the Location CIO for the use of the external network service provider.

Protected wireless networks must:

- Use encryption approved by the CISO.
- For wireless networks transmitting Institutional Information classified at Protection Level 2 or higher, implement segmentation or equivalent software/policy-defined networking to ensure the connection(s) between protected and unprotected networks have access controls and/or intrusion detection/protection technology.

13.2 Information transfer

The transfer of Institutional Information classified at Protection Level 3 or higher between UC Locations, Suppliers, or to external entities/organizations must use appropriate security controls approved by the CISO and Institutional Information Proprietor.

Section 14: System Acquisition, Development and Maintenance

Objective: *Ensure security by design and throughout the IT Resource and Institutional Information lifecycle.*

14.1 Security requirements of information systems

Units must identify system security and management requirements in the planning phase and prior to development or acquisition of a system.

System security requirements must include:

- The elements described in the UC Secure Software Configuration Standard.

DRAFT

- The Risk Assessment or Risk Treatment Plan.
- The Protection Level and Availability Level.
- The UC Minimum Security Standard.

Software developed in-house that stores, processes or transmits Institutional Information classified at Protection Level 2 or higher must be developed in compliance with the UC Secure Software Development Standard.

For Institutional Information and IT Resources classified at Protection Level 4, Units must conduct penetration testing at a minimum:

- At least once every three years.
- After a major change occurs.

14.2 Security in development and support processes

Information security must be designed and implemented within the development lifecycle of information systems.

Units must maintain documentation showing security planning and requirements during all phases of development or acquisition, from initiation through implementation, and ongoing maintenance phases.

Version control is required for production source code and configurations.

Access to source code and configurations related to Institutional Information classified at Protection Level 3 or higher must be restricted to approved Workforce Members.

Before software or systems are moved into production, all application/program access methods utilized in development or testing, other than the formal user access methods or formally defined interfaces, must be:

- Deleted, or
- Disabled, or
- Formally documented by the Unit as a production feature in the Risk Assessment.

Section 15: Supplier Relationships

Objective: *Ensure vendor relationships are covered by appropriate security requirements and controls.*

15.1 Information security in supplier relationships

Agreements with Suppliers must contain security requirements that are consistent with this policy and supporting standards for the protection of, and access to, Institutional Information and IT Resources (Appendix - Data Security and Privacy, the purchasing-approved replacement or the CISO-approved equivalent).

DRAFT

15.2 Supplier service delivery management

Units must ensure Supplier agreements:

- Incorporate into the purchase agreement the applicable Institutional Information and IT Resource security requirements (UC Purchasing's Appendix - Data Security and Privacy).
- Consider the term of the agreement and changes in information security requirements.
- Receive approval from the CISO on the information security requirements for Institutional Information or IT Resources classified at Protection Level 3 or higher, Availability Level 4 or Critical IT Infrastructure.

Suppliers subject to the Payment Card Industry (PCI) Data Security Standard must sign, or have incorporated into the purchase agreement, the applicable PCI security requirements, terms and conditions.

Suppliers who qualify as a Business Associate under HIPAA/HITECH must sign a UC-approved Business Associate Agreement (BAA).

Suppliers subject to other terms and conditions specified in law or regulation must have the applicable terms included in the agreement.

15.2.1 Unit responsibilities when using suppliers

Units must work with their central Procurement departments to ensure agreements and other arrangements with persons or Suppliers conform to the requirements of this policy.

Units using Suppliers must:

- Use only approved and disclosed access methods.
- Comply with the applicable UC Minimum Security Standard.
- Complete a Risk Assessment.
- Ensure Supplier access to IT Resources or Institutional Information is consistent with UC security policies.
- Notify Suppliers when Workforce Members separate if the Supplier facilitates access to IT Resources.
- Ensure that Suppliers report Breaches and Information Security Incidents to the CISO.
- Report observed Supplier security lapses to the CISO.
- Clearly document the responsibilities of each party.
- Ensure review and adjustment of applicable security requirements upon agreement renewal, taking into account changes to:
    - Institutional Information.
    - IT Resources.

  - Policy.
  - Law and regulation.

- As appropriate, obtain assurance from a third party audit report, or other documentation acceptable to UC, demonstrating that appropriate information security safeguards and controls are in place.
- Follow UC records retention requirements contained in UC's Records Management Polices (RMP.)

Units using Suppliers must ensure Suppliers **do not**:

- Share with anyone passwords or authentication secrets that provide access to Institutional Information or IT Resources.
- Use passwords or other authentication secrets that are common across customers or multiple unrelated UC sites.
- Create backdoors or alternate undisclosed access methods for any reason.
- Access systems when not authorized to do so.
- Make unauthorized changes.
- Reduce, remove or turn off any security control without approval from Unit Information Security Lead.
- Create new accounts without Unit approval.
- Store, harvest or pass through UC credentials (username, password, authentication secret or other factor).
- Use or copy the Institutional Information for non-authorized purposes.

Section 16: Information Security Incident Management

Objective: *Ensure a consistent and effective approach to the management of Information Security Incidents, including communication on Information Security Events and compromise details.*

16.1 Management of Information Security Incidents and corrective action

Incident management requires a quick, effective and orderly response.

16.1.1 Location Information Security Incident response plan

Each Location must develop and maintain a documented Information Security Incident response plan, which must implement the required elements outlined in the UC Privacy and Data Security Incident Response Program Standard.

16.1.2 Reporting Information Security Events

Workforce Members must promptly report any known or suspected Information Security Incidents, Information Security Events, threats or vulnerabilities associated with Institutional Information or IT Resources to the Workforce Manager, Unit Head or CISO.

DRAFT

Workforce Managers and Unit Heads must promptly report Information Security Incidents involving Institutional Information classified at Protection Level 3 or higher to the CISO.

The Location must develop a method for students to report any known or suspected Information Security Incidents, Information Security Events, threats or vulnerabilities associated with Institutional Information or IT Resources.

The CISO must report Information Security Incidents involving Institutional Information Classified at Level 3 or higher to the Campus Privacy Officer.

16.1.3 Response to Information Security Incidents

Response to Information Security Incidents must follow the Location Information Security Incident response plan.

16.1.4 Learning from Information Security Incidents

The Location must perform a root cause investigation, develop a corrective action plan, and develop a preventive action plan when Information Security Incidents:

- Result in an Institutional Information Breach, or reasonably would have resulted in an Institutional Information Breach if not contained (near misses).
- Compromise IT Resources classified at Protection Level 3 or higher.
- Compromise IT Resources classified at Availability Level 3 or higher.

Section 17: Information Security Aspects of Business Continuity Management

Objective: *Maintain information security during adverse situations and ensure information security is embedded in UC's business continuity and/or disaster recovery processes.*

17.1 Information security and business continuity

Units must plan, implement, test and review the continuity of information security as an integral part of the organization's business continuity and disaster recovery plans.

IT Resources classified at Availability Level 4 must be included in emergency and disaster recovery planning.

Section 18: Compliance with External Requirements

Objective: *Avoid compromise of Institutional Information and IT Resources.*

18.1 Compliance with legal and contractual requirements

Workforce Members and Units must meet the obligations related to information security, intellectual property, records, privacy, personal information and encryption stated in:

- Laws.
- Governmental regulations.
- Agreements, contracts or external obligations.
- Grants.

Unit Heads must report to the CISO any non-compliance with legal and contractual requirements related to information security.

18.2 Information security reviews

Units must perform periodic reviews of information security practices, make corresponding adjustments to the application of this policy, and update applicable Risk Assessments.

18.2.1 Independent review of information security

Location auditors, or contracted third-party auditors, must periodically audit and report to management on compliance with this policy and supporting UC standards.

18.2.2 Demonstrating compliance with security policies and standards

Units and Service Providers must use and demonstrate an Evidence-Based Approach to compliance with this policy.

18.2.3 Technical compliance review

CISOs or their designees must define and execute a method to periodically review compliance with this policy and related UC standards, or as defined by the Risk Assessment.

IV. COMPLIANCE / RESPONSIBILITIES

Role	Responsibilities	Notes
Chancellors, Health System Executive, Lawrence Berkeley National Laboratory Director, UC Chief Operating Officer, Vice President of the Division of Agriculture and Natural Resources	Appoint responsible parties to implement this policy at their Locations.	--
Cyber-risk Responsible Executive (CRE)	Ensures the responsible parties understand and execute their responsibilities under this policy. Ensures the Location-wide adoption of the ISMP covered in “Section 5:	--

DRAFT

Role	Responsibilities	Notes
	Information Security Management Program," and an information security risk management strategy. Reviews the Location's overall information security Risk Assessments and identifies key risks affecting the Location. Evaluates the Location's level of cyber risk to make decisions about risk mitigation and risk acceptance. Approves the Location policy exception process. Participates in systemwide initiatives related to information security and information security risk management. Evaluates information security risk and ensures appropriate funding for information security.	
UC Systemwide Chief Information Security Officer	Collaborates with Location officials to ensure implementation of this policy. Supports this policy systemwide and facilitates regular communication among Locations to address consistent implementation of this policy throughout UC.	May be appointed by the UC Executive Vice President and Chief Operating Officer to act as CISO for assigned Office of the President Locations.
Chief Information Officer (CIO)	Provides operational oversight for the delivery of information technology	Senior IT executive, IT Leadership Council Member.

DRAFT

Role	Responsibilities	Notes
	services that meet the requirements of this policy. Plans and directs information security Risk Assessments for the Location. Provides management oversight for information security planning, implementation, budgeting, staffing, program development and reporting. Sets operational priorities and obtains alignment with the CRE and Location leadership.	
Chief Information Security Officer (CISO)	Assists the Location in the interpretation and application of this policy. Provides management and execution oversight of the ISMP through collaborative relationships with CRE, CIO, academic and administrative officials, using Location governance structure and compliance strategies. Reports Information Security Incidents to UCOP, appropriate Location leadership and the Location CRE. Manages the Location exception process for this policy.	May also be called an "Information Security Officer (ISO)" or "Campus Information Security Officer (CISO)" at some Locations.
Unit Head	Oversees the execution of this policy within the Unit.	A Unit can be an IT, academic, research,

DRAFT

Role	Responsibilities	Notes
	Assigns one or more individual(s) with oversight of the execution of information security responsibilities within the Unit. This role is called the Unit Information Security Lead. Identifies and inventories Institutional Information and IT Resources managed by the Unit. Ensures Risk Assessments are complete and Risk Treatment Plans are implemented. Specifies the Protection Level and Availability requirements to Service Providers who manage IT Resources on behalf of the Unit. Through the risk management process, ensures that protection of Institutional Information and IT Resources managed by Service Providers meets the requirements of this policy. Through the risk management process, ensures that Institutional Information and IT Resources managed by Suppliers meet the requirements of this policy. Reports Information	administrative or other entity operating within UC. A Unit Head is characterized by having budget control and/or control or authority over IT Resources and/or Institutional Information. See the glossary. Unit Heads may delegate specific information security responsibilities to Workforce Members under their area of responsibility, Service Providers or Suppliers. The Unit Head must ensure this delegation of responsibility is clear and unambiguous. Any Unit information security responsibilities not expressly delegated to, and accepted by, a Service Provider or Supplier remain the responsibility of the Unit Head.

DRAFT

Role	Responsibilities	Notes
	Security Incidents to the CISO. Reports to the CISO any information security policy or standard that is not fully met by the Unit, or by a Service Provider managing Institutional Information or IT Resources on behalf of the Unit. Ensures the above responsibilities are included in the overall Unit planning and budgeting process.	
Service Provider	Delivers information technology services that comply with this policy. Documents and delivers IT services in compliance with this policy, other UC policies and applicable Location policies. Notifies the Unit Head of any policy provisions that are unmet or require additional controls by the Unit. Supports Units in completing Risk Assessments related to the services provided. Coordinates with Units to implement appropriate security measures. Coordinates with Units to respond to potential and	Can be a central IT group, another Unit, another UC location, or UC service center providing specific IT services to a Unit. Service Providers can be Units for the purposes of this policy. Service Providers are internal UC entities for the purposes of this policy. External suppliers are covered under this policy in section 15.

DRAFT

Role	Responsibilities	Notes
	confirmed Information Security Incidents.	
Institutional Information Proprietor	Assumes overall responsibility for establishing the Protection Level classification, access to, and release of a defined set of Institutional Information. Classifies Institutional Information under their area of responsibility in accordance with this policy. Establishes and documents rules for use of, access to, approval for use, and removal of access to the Institutional Information related to their area of responsibility. Notifies Units, users, Service Providers and Suppliers of the Institutional Information Protection Level. Approves Institutional Information transfers and access related to their areas of responsibility. Notifies Units, Service Providers and Suppliers of any changes in requirements set by the Institutional Information Proprietor.	The Institutional Information Proprietor is responsible for their defined set of Institutional Information regardless of the Unit holding the data. Responsibilities of this role may affect Unit, Service Provider and Supplier requirements.
Workforce Manager	Complies with this policy.	See Glossary. Typically managers or supervisors.

DRAFT

Role	Responsibilities	Notes
Workforce Member	Complies with this policy.	See Glossary. This is a broad term encompassing all individuals who perform work for UC in any capacity.
Researcher	Complies with all responsibilities of Workforce Members. Uses a Location pre-approved Risk Treatment Plan, or uses a Risk Assessment to ensure the information security requirements are met. Identifies the appropriate Institutional Information Protection Level defined in this policy for research data. Identifies and meets confidentiality and data security obligations based on laws, regulations, policies, grants, contracts and binding commitments (such as data use agreements and participant consent agreements) relating to research data. Creates and maintains evidence that demonstrates how security controls were implemented and kept up to date during the research projects. Develops and follows an information security plan that manages security risk over the course of their	

DRAFT

Role	Responsibilities	Notes
	project. Ensures Suppliers who store or process Institutional Information during the project follow UC policy for written contracts. Ensures Supplier agreements include approved terms supporting the information security controls specified in this policy and applicable UC purchasing requirements.	
Unit Information Security Lead	Provides oversight and execution of information security responsibilities within the Unit.	The Unit Head assigns this role to Workforce Member(s) to carry out Unit responsibilities under this policy. The Unit Head can also perform this role.

V. REQUIRED PROCEDURES

The standards referenced in this policy specify additional requirements that can change more frequently than this policy and/or provide details to implementing the requirements of this policy.

Using the standards governance outlined in Section III, 2.3, ITLC is responsible for developing, implementing, revising and consulting on standards in support of this policy. These include but are not limited to:

1. UC Authentication Management Standard
2. UC Data Destruction Standard
3. UC Encryption Key and Certificate Management Standard
4. UC Institutional Information and IT Resource Classification Standard
5. UC Logging and Event Recording Standard
6. UC Minimum Security Standard
7. UC Secure Software Configuration Standard
8. UC Privacy and Data Security Incident Response Plan Standard
9. UC Secure Software Development Standard

Note: These are goverend by section 2.3 – Standards. In the final they will hyperlink to the on-line standard.

VI. RELATED INFORMATION

DRAFT

This policy is based on and ties to the International Organization for Standardization and the International Electrotechnical Commission (ISO) 27000:2013 document series. Section III, subsections 1-6 are based on ISO 27001:2013. Section III, subsections 7-18 are based on ISO 27002:2013. The numbering and mapping of subsections 7-18 match ISO 27002:2013.

The sections contained in this document overlap in some areas because of the comprehensive nature of the ISO 27000:2013 framework. The Chief Information Security Officer (CISO) at each Location is a resource for interpreting this policy and addressing complex or outlying issues.

VII. FREQUENTLY ASKED QUESTIONS

Note: FAQs will be developed prior to policy issuance. FAQs are not live yet! Sample/draft guides are posted.

Additional resources to guide the understanding and use of this policy are on the systemwide information security website: https://security.ucop.edu/guides/index.html

VIII. REVISION HISTORY

Date	***Description***
February 1, 1985	First issued as an IS bulletin - Guidelines for Security of Computing Facilities.
November 12, 1998	IS-3 Reissued as Electronic Information Security.
April 18, 2003	IS-3 Sections IV and V revised.
February 8, 2005	IS-3 revised. Included new provisions to compliance with HIPAA. Changed scope to the entire University enterprise, changed encryption, and other standards.
July 27, 2007	Revision to IS-3 Electronic Information Security.
February 3, 2011	Minor revision to IS-3 Electronic Information Security.
March 1, 2011	Added requirement to follow the UC Privacy and Data Security Incident Response Plan.
TBD, 2017	Major rewrite to comply with academic research/grant requirements, Department of Education requirements outlined in the July 29, 2015 Dear Colleague Letter, conform to cyber insurance underwriting, updated conform to the Office of Civil Rights guidance on HIPAA compliance, conform to PCI 3.X, adapt to changes in security landscape and adopt a standards based approach to information security (ISO 27001 and 27002.)

DRAFT