BFB-IS-3: Electronic Information Security

Responsible Officer:	Chief Information Officer & VP - Information Technology Services
Responsible Office:	IT - Information Technology Services
Issuance Date:	10/25/2019
Effective Date:	10/25/2019
Last Review Date:	9/10/2019
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. Note: This policy does **not** generally apply to students who are not Workforce Members. • All use of Institutional Information, independent of the location (physical or cloud), 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

TABLE OF CONTENTS

I. POLICY SUMMARY

Information security is of the utmost importance to the University of California. In an increasingly collaborative world that depends upon shared electronic information, it is essential that the University of California implement a policy to guide protection and availability.

UC's revised and updated Electronic Information Security Policy (IS-3) allows it to protect user confidentiality; to maintain the integrity of all data created, received or collected by UC (Institutional Information); to meet legal and regulatory requirements; and to ensure timely, efficient and secure access to information technology resources (IT Resources).

IS-3 simplifies the process of cyber risk management at a systemwide level and prepares UC for a world in which information security is increasingly critical.

Goals

1. Preserve academic freedom and research collaboration.
2. Protect privacy.
3. Follow a risk-based approach.
4. Maintain confidentiality.
5. Protect integrity.
6. Ensure availability.

Principles

1. Policy goals guide decisions.
2. Location Units ("Units") are accountable for implementing information security.
3. Risk level determines the position that is assigned decision-making rights.
4. Security is a shared responsibility.
5. Security is embedded in the lifecycle of systems, services and software.

IS-3 applies to 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). The policy also applies to all Workforce Members, Suppliers, Service Providers and other authorized users.

Systemwide Consistency, Location-specific Flexibility

IS-3 establishes a framework that ensures all UC Locations follow the same approach to reduce and manage cyber risk, protect information and support the proper functioning of IT Resources. This consistent approach also positions UC Locations to collaborate on cyber security. While promoting systemwide consistency and collaboration, the policy also supports local flexibility and control. Key features supporting local control include an exception process and a Risk Treatment Plan, a tool that creates a flexible and scalable approach to cyber security.

Protecting UC's Electronic Assets

Protection Level and Availability Level classifications (see Glossary) guide the implementation of the policy. These levels range from 1, the lowest, to 4, the highest. When the classification is high, more effort goes into protecting the asset. These classifications also inform IS-3's risk-based approach to security (see below).

IS-3 also has a special classification of Critical IT Infrastructure (see Glossary) that helps UC identify and allocate resources to protect the most important systems that, if compromised, would result in significant damage to or unauthorized use of Institutional Information or IT Resources.

A Standards- and Risk-based Approach

IS-3 follows both a standards- and risk-based approach to information security to ensure that UC meets industry, government and regulatory requirements while also

properly scoping controls and making appropriate investment decisions. The policy incorporates a subset of controls from the international standards ISO 27001 and ISO 27002 that align with and support UC's mission of research, teaching and public service. IS-3 also addresses legal requirements associated with HIPAA, the Payment Card Industry (PCI) and other state and federal regulations and includes requirements needed to qualify for certain grants that are essential to UC research funding (NIST 800-171). Additionally, IS-3's risk-based approach guides the allocation of resources by evaluating risk and assessing the cost and benefit of risk management.

Security is a Shared Responsibility

IS-3 defines the roles and responsibilities of Unit, Unit Head, Unit Information Security Lead (UISL), Service Provider and Supplier.

CISO: The Chief Information Security Officer (CISO) is responsible for security functions throughout a Location, including assisting in the interpretation and application of this policy. The CISO has many other responsibilities, including approving exceptions, helping Units manage cyber risk, approving Risk Treatment Plans and participating in a Location's cyber risk governance.

Unit: A point of accountability and responsibility that results from creating/collecting or managing/possessing Institutional Information or installing/managing IT Resources. A Unit is typically a defined organization, such as the school of engineering, or a set of departments, such as student affairs. Because UC is a highly decentralized and independent federation of organizational units, the policy provides Units with the flexibility and responsibility to manage cyber risk.

Unit Head: A generic term for dean, vice chancellor or person in a 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 heads have important responsibilities to ensure effective management of cyber risk.

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 Assessment and Risk Treatment plans; devising procedures for the proper handling, storage and disposal of electronic media within the Unit; and reviewing access rights.

Service Provider: A UC internal organization that offers IT services to Units. Service Providers typically assume most of the security responsibility and help Units understand Unit responsibilities with respect to cyber security.

Supplier: An external, third-party entity that provides goods or services to UC. Section III Subsection 15 describes what Suppliers must do. UC has specific contract terms that clarify the responsibilities of Suppliers and protect UC.

Policy Structure and Organization

The policy text (Section III) is divided into 18 subsections.

- The first five subsections cover goals, organizational elements of information security and governance, the exception process, roles and responsibilities and the Information Security Management Program and principles.
- Subsection 6 describes the risk management process.
- Subsection 7 outlines security in human resource management.
- Subsection 8 informs users how to classify, account for and manage assets.
- The final subsections, 9 through 18, provide technical and administrative controls scoped according to Protection and Availability Level.

Information Security in a Changing World

UC is a leader in research, teaching, public service, patient care and the development of knowledge through inquiry, investigation and collaboration. Information security will continue to play a more and more critical role in the process of knowledge production and information sharing. IS-3 allows UC to remain a world leader by ensuring a successful approach to cyber risk management and incident response.

II. DEFINITIONS

A comprehensive glossary of terms can be found at https://security.ucop.edu/policies/it-policy-glossary.html.

For ease of reference, here are the most commonly used terms in this policy:

CISO: A role responsible for security functions throughout a Location, including assisting in the interpretation and application of this policy.

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

IT Resources: A term that broadly describes IT infrastructure, software and/or hardware with computing and networking capability. These include, but are not limited to: portable computing devices and systems, 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 media, Logical Media, biometric and access tokens and other devices that connect to any UC network. This includes both UC-owned and personally owned devices while they store Institutional Information, are connected to UC systems, are connected to UC Networks or used for UC business.

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

Service Provider: UC groups or organizations providing specific IT services to a Unit.

Supplier: An external, third-party entity that provides goods or services to UC.

Unit: A point of accountability and responsibility that results from creating/collecting or managing/possessing Institutional Information or installing/managing IT Resources. A Unit is typically a defined organization or set of departments.

Unit Head: A generic term for dean, vice chancellor or person in a similarly senior role who has the authority to allocate budget and is responsible for Unit performance and administration. 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 (UISL): 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. These activities are performed in consultation with the Unit Head.

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

Workforce Member: An 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 levels.

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 its 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. 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, providing Locations with the following four methods of identifying applicable security controls to manage cyber security risk:

- Conduct a Risk Assessment – see Part III, Section 6.
- Use a Risk Treatment Plan – see Part III, Section 6.1.2.
- Use this policy and related standards to identify applicable controls.
- Some combination of the above.

When conducting Risk Assessments or designing Risk Treatment Plans, Locations and/or Units must evaluate information security risk using the full set of security controls and requirements set forth in this policy and related standards.

All Workforce Members share a common set of responsibilities to protect 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 establishes the framework for UC to achieve six electronic information security goals:

1.1.1 Preserve academic freedom and research collaboration.

UC is committed to preserving an environment that encourages academic freedom 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]

1.1.3 Follow a risk-based approach.

UC is committed to following a risk-based approach to information security, 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 that 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 the integrity of Institutional Information. Protecting integrity requires guarding against the improper modification or destruction of information. This includes ensuring that 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 that they are accessible and able to meet UC's Business and operational needs.

---

[1] See http://www.ucop.edu/ethics-compliance-audit-services/compliance/privacy/index.html for more information about UC's work to protect the privacy of individuals. This work informs IS-3's goal of privacy protection.

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:

- Policies Applying to Campus Activities, Organizations and Students (PACAOS), if the student is part of the Workforce (see "Workforce Member" in Glossary).
- 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:

- 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 may bear some or all of UC's direct costs that result from an Information Security Incident under the Unit's area of responsibility if the Information Security Incident resulted from a significant failure of the Unit to comply with this policy. These 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.

A significant failure to comply may affect the Unit's or the Location's ability to seek cyber insurance reimbursement under Business and Finance Bulletin BUS-80 - Insurance Programs for Information Technology Systems.

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 electronic information security.*

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 make the appointment(s) to ensure that scope and responsibility are understood.

Locations may create additional roles and assign responsibilities in order 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 standard may weaken protection of Institutional Information and IT Resources, they are occasionally necessary and permitted for Part III, Sections 7 to 18.

Units must follow a risk-based approach when requesting an exception to the controls specified in Part III, Sections 7 to 18. 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.
- When Institutional Information classified at Protection or Availability Level 3 or higher is involved (see Section 8: Asset Management and Classification for level details).
- When 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 and pre-approve a standard exception plan to manage risks, implement compensating controls and provide for periodic review using an approved Risk Treatment Plan or a full Risk Assessment.

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.

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 or the designated working committee (e.g., 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.

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 Policy goals guide decisions.

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 for managing information security risk in a manner consistent with this policy.

4.3 Risk level determines decision-making rights.

To protect UC, 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 and 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.

4.5 Security is embedded in the lifecycle of systems, services and software.

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.[2]

Section 5: Information Security Management Program

***Objective**: Provide management direction and support for 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 Compliance Responsibilities 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.
- Guides the allocation of resources in response to identified and prioritized risks.
- Reviews the ISMP annually to ensure that it addresses changing UC Business needs, operating environments, threat landscape, regulatory landscape and changes in technology.
- Documents review of the ISMP by the Cyber-risk Responsible Executive (CRE).

[2] See also the Electronic Communications Policy, http://policy.ucop.edu/doc/7000470/ElectronicCommunications, for important information needed to plan the administration, technical and operational implementation of security controls.

5.2.2 Unit security planning, execution and review

Units are responsible for implementing the Location ISMP for 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 that all Workforce Members:

- 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 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 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 that this policy achieves its intended outcome(s) using a risk-based approach.*

When conducting Risk Assessments or designing Risk Treatment Plans, Locations must evaluate cyber risk against the full set of security controls and requirements set forth in this policy and related standards. Locations may add requirements or modify requirements to meet risk tolerances.

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 using the controls in this policy (Part III, Sections 7 to 18) and referenced standards or Location-approved alternatives.
- 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 and prioritizing investments/budgets to address identified risks.
- Monitoring risk on an ongoing basis.
- Providing a feedback system for continuous improvement.
- Monitoring security and compensating controls for effectiveness.
- Noting clearly who is responsible for the functions listed above when working across Locations or Units or with third parties.

6.1.1 Risk Assessments

Units must complete Risk Assessments for Institutional Information and IT Resources classified at Protection Level 3 or higher, or use an approved Risk Treatment Plan.

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 for Institutional 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.

The CISO may pre-approve standard Risk Treatment Plans 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 standard 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, approved exceptions, 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 full Risk Assessments.

Units must conduct a specific Risk Assessment for IT Resources that are designated as Critical IT Infrastructure. The risk assessment must include 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 that Workforce Managers communicate and facilitate strong information security practices.*

7.1 Prior to employment

Role	**Key Responsibilities**

Location Human Resources (HR)	Establishing onboarding procedures that support information security. These include:
	• Conducting background checks in accordance with Section 7.5 for:
	  o Non-academic Workforce Members in Critical Positions.
	  o Non-academic Workforce Members with access to Institutional Information classified at Protection Level 3 or higher.
	  o Non-academic Workforce Members with access to IT Resources classified at Availability Level 3 or higher.
	• Completing and documenting identity verification for access control.

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

7.2 During employment

Role	Key Responsibilities
Workforce Manager	Updating the information security elements of job descriptions and training requirements when job duties change. Reviewing access rights annually and removing access that is no longer needed. Notifying 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. Ensuring that Workforce Members complete security awareness training. Ensuring that 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 and best practices to maintain minimum standards of information security. Promptly addressing reported, suspected or actual policy violations.
Workforce Member	Following applicable information security policies, procedures, standards and best practices to maintain minimum standards of information security. Completing assigned security training. Reporting to their manager any access rights that are outside assigned roles or responsibilities. Reporting to their Unit or records 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. Reporting 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. Reporting 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. • 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 cyber security requirements set by the CISO. Employment procedures must include background checks as described in Section 7.5 when a Workforce Member moves into a critical position, and/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	Following the appropriate Location separation procedures. Documenting 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 UC Business continuity. Ensuring that information system access, including all internal, physical and remote access, is promptly revoked as appropriate. Documenting approval by an appropriate Location official of any IT Resource access privileges retained after separation.
Workforce Member	Returning all UC property, IT Resources and physical access keys/cards. Returning all Institutional Information, token encryption keys and all copies. Surrendering UC-licensed software and tools.

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 the roles of requestor, approver and implementer are independent.

- 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.

7.5 Background checks

Location HR must develop and implement pre-employment screening procedures in accordance with university policy and applicable labor agreements for non-academic Workforce Members, including appropriate background checks that anticipate risks stemming from access to Institutional Information or IT Resources. Such cyber risks might include:

- Financial fraud.
- Identity theft.
- Medical fraud.
- Cyber related crimes.
- Crimes related to the performance of specific job duties.

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 and defines appropriate protection responsibilities for organizational assets. 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 procured or managed by the Unit and classified at Protection Level 3 or higher. The inventory record must contain at least:

- An identification of the asset (name, asset tag, service tag or other unique identifier).
- 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 related 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 related to a breach or compromise, the overall operation of the Location or operation of essential services. (Statutory.)
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: students, patients, research subjects, employees, community, 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.)
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 for which 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 may result in minimal impact or minor financial losses.

8.2.2 Labeling 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 the 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 order to prevent unauthorized disclosure, removal or destruction of Institutional Information.

8.3.1 Management of electronic media

Units must encrypt Institutional Information classified at Protection Level 3 or higher when stored on portable media.

Units must securely store portable 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 electronic media and non-removable memory, in compliance with the UC Institutional Information Disposal 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.*

Units must comply with the UC Account and 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

Units must ensure that access to Institutional Information follows the Need to Know and Least Privilege principles.

Units must ensure that Institutional Information classified at Protection Level 2 or higher has 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 use 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.

Units must route network access to Institutional Information classified at Protection Level 4 through secure access control points.

Units must monitor network access to Institutional Information classified at Protection Level 3 or higher 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.

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 all required training prior to receiving access.

9.2.3 Management of privileged access rights

Units must assign privileged access based on job function(s) and must include clear instructions for appropriate use.

Section 10: Encryption

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

10.1 Encryption requirements

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

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

Units must encrypt Institutional Information classified at Protection Level 3 or higher when stored on portable electronic media or portable computing devices.

Units must encrypt Institutional Information classified at Protection Level 4 when stored on any electronic media.

10.1.1 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 physical access to protect UC Institutional Information and IT Resources.*

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 and/or where unauthorized individuals can access it.
- Administrative and physical controls on third-party access and supervision.

Units must ensure that physical access to secured areas is based on job responsibilities.

11.2 Equipment security

Keeping equipment secure helps prevent the loss, damage, theft or compromise of assets and the interruption of 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:

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

11.2.2 Environmental requirements

Units must protect IT Resources classified at Availability Level 4 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 that Suppliers who service, maintain, handle or take off-site IT Resources or Institutional Information classified at Protection Level 2 or higher comply with Part III, Section 15.

11.2.5 Removal of assets

Units must track IT Resources 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.

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

Units must ensure that Institutional Information classified at Protection Level 3 or higher is adequately protected both on- 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).

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 electronic media or output.
- System restart and recovery.
- Logging and monitoring in compliance with the UC Event Logging 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

Locations must control and scope changes to IT Resources through their 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.

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.

Units must subject changes to the production environment to the Location change management process.

Units must ensure that testing and development environments that contain Institutional Information 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

Units must ensure that any device connected to an authenticated or protected Location network complies 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 or higher.
- IT Resources classified at Protection Level 3 or higher.
- IT Resources classified at Availability Level 3 or higher.

12.3 Backup

Units must ensure that Institutional Information classified at Availability Level 3 or higher is backed up and recoverable.

Units must comply with UC Records Retention Schedule for retention of backups.

Units must protect backups according to the Protection Level of the Institutional Information they contain.

Units must ensure that portable backup media meet the portable media requirements outlined in this policy.

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

Units must maintain a backup catalog that shows the location of each backup and retention requirements.

12.4 Logging and monitoring

Proper logging and monitoring are required practices for recording events and generating evidence.

12.4.1 Event logging

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

Units must obtain approval for erasing, purging or trimming event logs through the change management process.

12.4.2 Protection of log information

Units must protect logs according to the Protection Level of the Institutional Information they contain and may not release them without proper authorization.

Units must retain logs according to external obligations as well as the requirements in the UC Records Retention Schedule, contracts, regulations, litigation holds 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 that:

- Only authorized activity occurred.

- Anomalies are analyzed and corrective actions are 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

Units must synchronize the clocks of IT Resources within an organization or security domain to a standard reference time source.

12.5 Control of operational software

Units must obtain approval for software installation, configuration changes and updates on production systems 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 longer than 90 days.

Units must protect IT Resources that cannot be patched to current standards with compensating controls approved through the exception process or remove the IT Resource 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.

Units must ensure that audit tests do not alter audit logs or production Institutional Information.

Units must ensure that audit activities do not reduce security controls below what is appropriate for the Institutional Information or IT Resource Protection or Availability Level.

Units must log and record auditor access to Institutional Information classified at Protection Level 3 or higher.

Section 13: Communications Security

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

13.1 Network security management

Units must place IT Resources processing Institutional Information classified at Protection Level 3 or higher on segmented networks restricted to IT Resources also classified at Protection Level 3 or higher. Units must protect the ingress and egress points via appropriate network security controls and/or intrusion detection/prevention tools/technologies approved by the CISO.

Units must authenticate administrator access to IT Resources that process Institutional Information classified at Protection Level 3 or higher through a managed access control point.

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

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

Units must ensure that network devices used to control access to Institutional Information classified at Protection Level 4:

- 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 a Supplier for network services to interconnect the Location network with the public Internet 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 to use the Supplier for access to the public Internet.

Units must ensure that protected wireless networks:

- Use encryption approved by the CISO.

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

13.2 Information transfer

Units must ensure that the transfer of Institutional Information classified at Protection Level 3 or higher between UC Locations, to Suppliers, or to external entities/organizations 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 lifecycle of IT Resources and Institutional Information.*

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

Units must ensure that software developed in-house that stores, processes or transmits Institutional Information classified at Protection Level 2 or higher is 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:

- 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.

Units must ensure that access to source code and configurations related to Institutional Information classified at Protection Level 3 or higher is restricted to authorized Workforce Members.

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

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

Section 15: Supplier Relationships

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

15.1 Information security in supplier relationships

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

15.2 Supplier service delivery management

Units must ensure that Supplier agreements:

- Incorporate into the purchase agreement the applicable Institutional Information and IT Resource security requirements (UC Appendix – Data Security and Privacy or the CISO-approved equivalent).
- Consider the term of the agreement and changes in information security requirements.
- Receive approval from the CISO on the information security requirements for 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 by 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 that 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 that 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.
- Document clearly 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.
    - Laws and regulations.
- 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 that Suppliers **do not**:

- Share 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 the appropriate 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 Cybersecurity Incident Response Standard.

16.1.2 Reporting Information Security Events

Workforce Members must promptly report 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.

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

Locations must develop a method for students to report 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 Protection Level 3 or higher to the Location privacy officer.

16.1.3 Response to Information Security Incidents

Response to Information Security Incidents must follow the Location Information Security Incident Response Plan.

Section 17: Information Security Aspects of Business Continuity

***Objective**: Maintain information security during adverse situations and ensure that 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 Unit's business continuity and disaster recovery plans.

Units must include IT Resources classified at Availability Level 4 in emergency and disaster recovery planning.

Section 18: Compliance with External Requirements

***Objective**: Ensure compliance with legal, statutory, regulatory or contractual obligations related to information security.*

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

The Location CRE must ensure that Location auditors or contracted third-party auditors periodically examine 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 vice chancellors, 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 that the responsible parties understand and execute their responsibilities under this policy. Ensures the Location-wide adoption of the ISMP covered in Section 5: 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.	--

Role	Responsibilities	Notes
UC Systemwide Chief Information Security Officer	Ensures implementation of this policy in coordination with Location officials. 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 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.	Senior IT executive, IT Leadership Council member.
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 structures 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.

Role	Responsibilities	Notes
Unit Head	Oversees the execution of this policy within the Unit. 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 that 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 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.	A Unit can be an IT, academic, research, 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 Glossary for more information. 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 that 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.

Role	Responsibilities	Notes
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 confirmed Information Security Incidents.	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.
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 of 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.

Role	Responsibilities	Notes
Workforce Member	Complies with this policy.	See Glossary. 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-approved Risk Treatment Plan or conducts a Risk Assessment to ensure that 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 current throughout the project. Develops and follows an information security plan that manages security risk over the course of their project. Ensures that Suppliers who store or process Institutional Information during the project follow UC policy for written contracts. Ensures that 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.

Additional resources to guide the understanding and use of this policy are on the systemwide information security website: Systemwide Information Technology Policies, Standards and Guides.

V. PROCEDURES

The standards referenced in this policy specify additional requirements that can change more frequently than this policy and/or provide details regarding the implementation of the policy's requirements.

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

VI. RELATED INFORMATION

Industry Standard Based Approach

This policy is based on and ties to the International Organization for Standardization and the International Electrotechnical Commission (ISO) 27000:2013 document series. Part III, Sections 1-6 are based on ISO 27001:2013. Part III, Sections 7-18 are based on ISO 27002:2013. The numbering and mapping of Sections 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 CISO at each Location is a resource for interpreting this policy and addressing complex or outlying issues.

These UC resources inform implementation of this Policy:

1. Electronic Communications Policy.
2. Privacy principles and practices at UC.
3. Systemwide Information Technology Policies, Standards and Guides.
4. Systemwide Information Security Resources.

VII. FREQUENTLY ASKED QUESTIONS

Additional resources to guide the understanding and use of this policy are on the systemwide information security website: Systemwide Information Security Policies and

Standards.

VIII. REVISION HISTORY

October 25, 2019: Technical update. Made a set of changes for the consistent use of the terms “portable media,” “portable computing device,” and “electronic media.” Removed duplicate word in III.2. Fixed a numbering error in III.10.1. Clarified encryption requirement in III.10 by removing extra words. 16.1.2 changed “campus” to “Location.”

July 1, 2018: Major rewrite to comply with academic research/grant requirements, Department of Education requirements outlined in the July 1, 2016 Dear Colleague Letter, conform to cyber insurance underwriting, updated to conform to the Office of Civil Rights guidance on HIPAA compliance, conform to PCI 3.X, align to NIST 800-171, adapt to changes in security landscape and adopt a standards-based approach to information security using ISO 27001 and 27002. The revised policy replaces IS-2, IS-10 and the Incident Response Guide.

This Policy was also remediated to meet Web Content Accessibility Guidelines (WCAG) 2.0.

March 1, 2011: Added requirement to follow the UC Privacy and Data Security Incident Response Plan.

February 3, 2011: Minor revision to IS-3 Electronic Information Security.

July 27, 2007 :Revision to IS-3 Electronic Information Security.

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.

April 18, 2003: IS-3 Parts IV and V revised.

November 12, 1998: IS-3 Reissued as Electronic Information Security.

February 1, 1985: First issued as an IS bulletin - Guidelines for Security of Computing Facilities.