UCI Information Security Standard

Version 1.1

1. General Overview

1.1. Introducing the UCI Information Security Standard

The UCI Information Security Standard (ISS) is the UCI implementation of the UC IS-3 policy and associated standards. Requirements contained in ISS are tailored for use at UCI using UCI terms and tools where applicable and are based on the requirements documented in IS-3 and on requirements established for systems and data at UCI. Compliance with UCI ISS helps ensure compliance with both UC IS-3 and any additional security requirements at UCI.

1.2. Scope of UCI ISS

The Minimum Security Requirements outlined in Section 14.1 of UCI ISS apply to all systems connecting to the UCI network regardless of ownership. All other sections of UCI ISS apply to Workforce Members, Researchers, Suppliers, Service Providers, and other authorized users of Institutional Information and IT Resources and applies to all use of Institutional Information regardless of physical location, ownership of any device or account that is used to store, access, process or transmit Instructional Information.

1.3. Goals of UCI ISS

The requirements in UCI ISS establish the framework for adequately protecting UCI systems and data while preserving the academic and research missions of the university. Information security goals include:

- Preserving academic freedom and research collaboration
- Protecting individual privacy needs including autonomy privacy
- Maintaining confidentiality of information against unauthorized disclosure
- Protecting system and information integrity from unauthorized changes
- Ensuring availability of systems and data to meet UC operational requirements
- Following a risk-based approach which balances security needs with other UC goals

1.4. UCI ISS is a Minimum Standard

UCI ISS is a minimum set of requirements needed to meet UC and UCI information security requirements. Additional controls may be required for specific use cases or as needed to meet regulatory requirements or additional threats to UC systems and data.

1.5. Periodic Updates

UCI ISS will be reviewed at least annually and be updated as needed to adapt to changes in UC security requirements including UC IS-3, changes in UC academic, research and business needs, changes to the regulatory landscape, changes in technology, and to adapt to changing threats to UC and UCI systems and data. Units must update Unit Information Security Management Plans and Risk Assessments to adjust to changing UCI ISS security requirements.

1.6. Violations, sanctions, and breach cost responsibility

Confirmed and serious violations of ISS may result in sanctions governed by the appropriate UC and UCI policies. This may include employment or educational consequences which may involve additional mandatory training, informal or formal reprimands, adverse performance appraisals, corrective or disciplinary actions, and termination.

Systems in violation of ISS may be removed or otherwise restricted from the campus network following the published campus Vulnerability Management Program (VMP) as needed to protect UCI systems and data. User accounts, application, system or data access may also be disabled or restricted as needed to address vulnerabilities, compromises, or significant non-compliance with ISS.

Units may be directly responsible for direct costs associated with an Information Security Incident that resulted from a significant failure to comply with UCI ISS.

1.7. Glossary

Terms used in UCI ISS are defined in the UC IS-3 Glossary.

2. Organizing Information Security

2.1. CISO Governance

UCI has appointed a Chief Information Security Officer who, in addition to other duties, is responsible for the overall governance and implementation of UCI ISS.

2.2. Risk Assessment Process

Using a risk-based approach, Units must document compliance with UCI ISS by completing the appropriate Risk Assessment as required in ISS Section 6.1 using templates in the UCI compliance tool, OneTrust. Using this tool, Units must document compliance with the controls, identify any gaps and associated risks, document any action items to address those risks including any compensating controls, and seek approval for any security exceptions or acceptance of risks that will not be addressed within the next calendar year.

Full compliance with UCI ISS will take significant time and effort to complete and Units are not expected to address all compliance gaps at once. A prioritized approach to address the most serious risks or risks that can be quickly addressed is suggested. While full compliance with ISS is important, it is also critical for Units to understand and document their security gaps and associated risks to make informed decisions on how to prioritize security remediation over time.

2.3. Exception Process

Units must use an approved security exception and risk acceptance process when Units are unable to meet the requirements of UCI ISS. Gaps in individual UCI ISS controls from a Risk Assessment typically are documented and accepted as part of the OneTrust risk workflow. Significant risks or risks identified outside of the Risk Assessment process should use the documented Security Exception Request form and process.

At a minimum, security exceptions must be approved by the CISO and a Unit Head with the level of authority that matches the risks identified. Security exceptions involving significant risks or risks that involve more than one Unit may require additional approvals or escalation. For specific use cases, the CISO may define pre-approved exception plans or approved compensating controls.

Exception requests and decisions must be documented, reviewed, and if needed, renewed at least annually.

2.4. Unit Security Governance

Unit Heads must designate one or more Unit Information Security Leads (UISL) who have the responsibility and authority to tactically coordinate, implement, and document the security activities within a Unit. At UCI we split the UISL role between an Administrative UISL role and Technical UISL role, who represent security leadership for the business operations and IT operations, respectively. Unit Heads and UISLs must work together to define the security strategies and priorities within a Unit.

Units must develop written procedures and guidelines to document their methods to comply with UCI ISS requirements.

3. Roles and Responsibilities

Roles and Responsibilities used in UCI ISS are defined in the UCI Roles & Responsibilities.

4. Information Security Management Program Principles

4.1. Risk Decisions

To ensure sound financial and operational decisions, Units must consider the goals outlined in UCI ISS Section 1.3 to scope, protect and make risk-based decisions about the appropriate protection of Institutional Information and IT Resources. Risk management decisions must be made at a level of financial, privacy, legal, reputational, or other authority that matches the level of risk identified.

4.2. Unit Head Accountability

Unit Heads are accountable for appropriately protecting Unit Institutional Information and IT Resources and must manage information security risk in a manner consistent with UCI ISS.

4.3. Shared Responsibility

All Workforce Members are responsible for the protection of Institutional Information and IT Resources and understanding the risks, threats, costs, and requirements associated with securing systems and data as outlined in UCI ISS.

4.4. Security must be embedded in IT activities

The security requirements outlined in UCI ISS must be incorporated into the entire lifecycle of any IT project, system, application, or service. Units must ensure project plans and system lifecycles include appropriate budget, planning, and staffing to implement the security requirements outlined in UCI ISS.

5. Information Security Management Program

5.1. UCI ISMP

The UCI CISO and CRE must establish and implement a documented campus Information Security Management Program (ISMP) that details the campus governance framework and administrative, technical, and physical processes in place that adequately protect UCI systems and data. The UCI ISMP must describe the campus implementation of the overall risk process including risk levels, acceptable risk tolerances, the process for security exceptions, and processes for formal risk acceptance and escalation. Campus security priorities should be identified to provide guidance to Units in prioritizing their own compliance activities.

5.2. Unit ISMP

Units must establish and implement a documented Unit ISMP that details their compliance to the UCI ISMP and associated Unit Risk Assessments. This includes allocating budget for Unit security activities, implementing appropriate Unit governance and staffing to meet Unit security requirements, conducting Risk Assessments, detailing the administrative, technical, and physical controls in place to protect Unit systems and data, documenting any control gaps and identified risks, documenting any action items, security exceptions and formal risk acceptance.

5.3. ISMP Review

The CRE and CISO must review the UCI ISMP and Units must review the Unit ISMP at least annually and update it as needed to adapt to changes in UC administrative, academic, and research needs, changes to the threat landscape, changes to regulatory compliance requirements, and changes in technology. The CISO or CRE may review Unit ISMP documentation as needed.

5.4. Training and Support

UCI and Units must implement a process to ensure that all Workforce Members receive appropriate security awareness training and complete the annual UC security awareness training requirements. Units must ensure that Workforce Members in the Unit receive any additional security training that may be required to meet Unit Security needs, regulatory or legal requirements, that they understand their roles in securing UC systems and data, and they understand how to comply with UCI incident reporting procedures.

5.5. Risk Reporting

The CISO must update the CRE and other UCI leadership on campus compliance activities at least annually. This security report will include information from OneTrust on the state of completed and outstanding risk assessments, overall risk levels and common risks identified across the Units, progress on action items and other remediation activities, and a summary of accepted risks across the Units. Reporting to leadership must also include any major changes to the threat landscape or regulatory requirements and other security metrics as needed.

6. Risk Management Process

6.1. Risk Assessments

6.1.1. Units must complete Risk Assessments or use an approved Risk Treatment Plan, as described in ISS Section 2.2, for Institutional Information and IT Resources classified at Protection Level 3 or higher or for Critical Infrastructure. Risk Assessments or Risk Treatment Plans must be completed before any new IT Resources classified at Protection Level 3 or higher are put into production.

6.1.2. The UISL must update Risk Assessments and Risk Treatment Plans at least once every two years or when major changes to the environment or configuration occur or when required to meet legal, regulatory or contractual needs.

6.1.3. Units must document any gaps found in the Risk Assessment or Risk Treatment Plan and develop a plan and timeline to remediate the gaps or implement appropriate compensating controls to reduce risk. Any gaps not part of an approved remediation plan must be approved through the documented risk exception process.

6.1.4. The CISO must work with UCI Leadership 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.

7. Human Resource Security

7.1. Prior to Employment

7.1.1. When recruiting a new position, Workforce Managers must document any IT security duties of the position in the job description or offer letter. Job descriptions must be kept up to date when staff roles and responsibilities change or the security requirements of the position change. Workforce Managers must consider the principle of Separation of Duties when designing and defining job duties and establish effective oversight. When functions cannot be separated, adequate administrative oversight or other compensating controls such as logging/alerting must be in place to mitigate identified risks.

7.1.2. UCI HR or Unit HR Managers must complete identity verification of all new hires before UCI accounts are provisioned and access is provided to Institutional Information or IT Resources.

7.1.3. Workforce Managers must follow the appropriate UCI and Unit onboarding procedures when provisioning new accounts, implementing role-based access controls, and providing access to Institutional Information or IT Resources.

7.2. Background Checks

7.2.1. UCI HR and Unit HR must develop and implement appropriate pre-employment screening procedures in accordance with university policy and applicable labor agreements. Screenings must be performed for new hires and when a Workforce Member moves into a position requiring a background check as part of a job change. Screening must address risk due to financial fraud, identity theft, medical fraud, criminal activity, or other risks typical to the position. Please see UCI policy 300-10: Background Check Procedures for further detail.

7.2.2. Working with UCI HR and Unit HR, Workforce Managers must at a minimum, ensure that background checks are conducted for:

- Non-academic Workforce Members in Critical Positions.
- Non-academic Workforce Members with access to Institutional Information or IT Resources classified at Protection Level 3 or higher
- Non-academic Workforce Members with access to IT Resources classified at Availability Level 3 or higher.

7.3. Security Training and Awareness

7.3.1. Workforce Managers must ensure that Workforce Members complete all required UC, UCI, and Unit security awareness training. At a minimum, this includes the annual UC Cyber Security Awareness Training but Units may require additional security awareness training specific to Unit functions and job duties. Additionally, many research grants and contracts require specific training and will need to consult the grant or contract language to ensure any required training is completed.

7.3.2. UCI Merchants and Workforce Members who handle Payment Card information must complete UCI PCI security awareness training upon hire and at least annually. Each Merchant must train their employees on specific procedures for processing credit cards and incident response for their credit card operations.

7.3.3. Workforce Managers must ensure that Workforce Members have the appropriate cybersecurity skills and receive appropriate cybersecurity training on a regular basis to adequately protect Institutional Information and IT Resources. Additional training must be provided when the security requirements of job duties change.

7.4. Change of Employment

7.4.1. Workforce Managers must update the information security elements of job descriptions and training requirements when Workforce Member job duties change. A background check may be required 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.

7.5. Separation

7.5.1. Workforce Managers and Workforce Members must follow the appropriate UCI and Unit separation procedures to ensure that:

- All UCI property including IT Resources, physical keys and keycards, and authentication tokens are returned.
- All copies of Institutional Information are returned or securely deleted.
- All accounts and role-based access controls are revoked as appropriate.
- Units retain access to all Institutional Information and IT Resources previously under the control of the Workforce Member.
- Any access privileges retained after separation are documented detailing any terms and conditions and expiration dates of access. All continued access must be approved by the appropriate Unit official.

7.6. Workforce Manager and Workforce Member Responsibilities

7.6.1. 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 UC and UCI. This include the systemwide UCOP IS-3 requirements and the UCI Information Security Standard, including associated guidance documentation, and all relevant UCI policies and procedures.
- Comply with the applicable security requirements of laws, governmental regulations, agreements, grants, contracts, or external obligations. Legal obligations may include the California Information Practices Act (IPA), the Family Educational Rights and Privacy Act, (FERPA), and the Health Insurance Portability and Accountability Act (HIPAA). Please refer to your specific agreements, grants and contracts for additional security requirements which may apply.
- Use Institutional Information and access IT Resources in accordance with their job responsibilities and not attempt to gain unauthorized access, disrupt operations, gain access to confidential information security processes or inappropriately alter Institutional Information.
- Comply with the UC Electronic Communications Policy (ECP), the UCI 800-15: UCI Guidelines for the UC Electronic Communications Policy, and the UCI 714-18 Computer and Network Use Policy.

7.6.2. Workforce Members are responsible for:

- Completing assigned security training.
- Reporting to their manager any access rights that are outside the assigned roles or responsibilities for their position.
- Reporting to their Unit the use of any Supplier or cloud service outside of what is provided by UC or UCI when used to store or process Institutional Information. Use of Suppliers or cloud services must be approved when used to store or process Institutional Information and have appropriate UC agreements in place. Personal accounts are not to be used to store or process Institutional Information. Please refer to UCI ISS Section 15, Supplier Relationships for additional requirements.

- Reporting to their manager any gaps in or failure of any information security controls in their assigned area of responsibility. Suspected security incidents must be reported using the Unit Incident Response Plan or by following UCI Security Incident procedures.
- Reporting possible unlawful action in accordance with UCI's Whistleblower Policy.

7.6.3. Workforce Managers must promptly address reported, suspected or actual policy, legal, or contractual violations to their UISL. Unit Heads must report to the CISO any non-compliance with legal and contractual requirements related to information security.

8. Asset Management

8.1. Inventory of IT Resources and Institutional Information

8.1.1. The Unit Information Security Lead (UISL) must maintain an inventory of Institutional Information and IT Resources procured or managed by the Unit and classified at Protection Level 3 or higher or for Critical Infrastructure. The inventory record must contain at least:

- An identification of the asset such as hostname, static IP address, asset tag, or other unique identifier.
- The physical location of the Institutional Information or IT Resource. For cloud resources, identification of the Supplier and geographic region is sufficient. The inventory must be updated when IT resources are physically moved or transferred to a Supplier.
- The identity of the Institutional Information Proprietor.
- The identities of the Workforce Members or roles who are responsible for the management and security of the IT Resource or Institutional Information. This may include but is not limited to, system administrators, DBAs, application programmers, etc.
- The Protection Level and Availability Level of the Institutional Information or IT Resource. The Classification Decision Tree can be used to help make classification decisions.
- Security documentation of the controls being used on the IT Resource to conform with this standard. This should include system build and hardening procedures and system operation and monitoring procedures. Please see UCI ISS Section 12 for specific documentation requirements.

8.1.2. Proprietors and/or UISLs must document all Institutional Information and IT Resources classified at Protection Level 3 or higher in the UCI Protected Data & Systems Inventory.

8.2. Classification of Institutional Information

8.2.1. Proprietors must determine and document the Protection Level for Institutional Information and IT Resources under their area of responsibility. This includes any Institutional Information that they create, store, process, or transmit. The Classification Decision Tree can be used to help make classification decisions.

8.2.2. UISLs and Proprietors must classify the Availability Level of Institutional Information and IT Resources under their area of responsibility.

8.2.3. If Institutional Information with higher Protection and/or Availability Levels also contains some lower-level information, the Institutional Information must be secured to meet the requirements of the highest Protection or Availability Level. If the Protection or Availability level cannot be determined or is unknown, the Institutional Information must be secured to Protection Level 4 and/or Availability Level 4 as appropriate.

8.2.4. Proprietors must document and communicate the Protection and Availability Levels and any additional usage requirements or restrictions for the Institutional Information to any UISL, Unit, Workforce Member, or Supplier given access to the Institutional Information. These usage requirements may include detailing the authorized use of the Institutional Information by the Unit and restricting any additional use or distribution of the information without Proprietor authorization. Units must comply with requirements for the use and protection of Institutional Information and IT Resources based on the classification level set by the Proprietor.

8.2.5. Both Proprietors and Units must review and update the classification of Institutional Information and IT Resources annually or when major changes occur. Major changes would include new features, use cases, or data elements are introduced or removed. Such a review should also determine whether access to the Institutional Information is still needed or whether access can be

removed or limited. Updates to the UCI Protected Data & Systems Inventory must be made as needed.

8.3. Secure Disposal of IT Resources and Institutional Information

8.3.1. Proprietors and Units must periodically review the Institutional Information stored in their Unit and securely dispose of information that is no longer used or needed for business purposes. Before disposing of or sanitizing electronic media containing Institutional Information, Workforce Members must verify that there are no record holds applying to the Institutional Information and the destruction of Institutional Information complies with Unit data retention needs and the UC records retention schedule. A records hold may be required in cases of ongoing litigation, an official investigation, an ongoing audit, or a pending Public Records Act request. Contact the UCI Records Manager in DFA for questions and assistance with records retention requirements.

8.3.2. Electronic media containing Institutional Information classified at Protection Level 2 or higher must either be securely destroyed or undergo a CISO approved sanitation process to ensure that Institutional Information is irretrievable before the media is reused. When disposing of or sanitizing electronic media containing Institutional Information whose Protection Level classification cannot be determined, it must be disposed of as if it contained information classified at Protection Level 4.

8.3.3. Workforce Members disposing of Institutional Information classified at Protection Level 3 or higher must update the UCI Protected Data & Systems Inventory as appropriate and IT Resources must be securely erased or destroyed before disposing or reusing the media. See the OIT data destruction guidelines for details.

9. Access Control

9.1. General Access Control Principles

9.1.1. Units must limit access to Institutional Information, IT Resources, networks, and network services to authorized individuals and ensure that such access follows the Need to Know and Least Privilege principles. The decision to grant access to Institutional Information must be based on a business need as well as applicable UCI and Unit policies. Proprietors must consider obligations under federal and state laws and consult their CISO and Privacy and Compliance Officers if they have any questions.

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

9.1.3. When granting access to Institutional Information classified at Protection Level 3 or higher, Units should use the principle of separation of duties to segregate access rights management so that requestors, approvers and grantors are unique roles assigned to separate individuals. If this cannot be accomplished, compensating controls such as increased logging, auditing and alerting must be used to address the increased risk associated with the combination of duties. Records that document changes to access rights and the related approvals must be maintained.

9.1.4. Units granting guest or other access to networks and network services not otherwise covered under this policy must establish terms of use and scope access and security requirements based on operational need and risk. All guest access must comply with the minimum standards in UCI ISS Section 14.1.

9.1.5. Proprietors must determine and communicate the appropriate use, access rights, use restrictions, and security requirements for the use of Institutional Information classified at Protection Level 3 or higher by Units, Service Providers, and Suppliers. This would include requirements for how the information should be used but also whether it can be re-used for other purposes or transferred to others without the approval of the Proprietor. With Suppliers, these requirements will be documented in contract language such as Appendix DS. Similar guidance should be communicated to campus Units and Service Providers who are granted access to the information.

9.2. General Account Management

9.2.1. Each Workforce Member and student must have a unique user account on each UCI IT Resource to distinguish that user from other users and provide accountability. Units should use UCINetIDs wherever possible.

9.2.2. Workforce Members must not use UCI user account names (such as user@uci.edu) as the primary identifier on non-UC accounts created for non-UC purposes.

9.2.3. When access to Institutional Information or an IT Resource is no longer needed for UC business purposes, UISLs must disable or remove the account and/or access rights. At a minimum, this includes changes of job duties or employment.

- For accounts that have access to Institutional Information or IT Resources classified at Protection Level 3 or higher and/or Availability Level 3 or higher access must be removed in five (5) days or less.
- For accounts that have access to Institutional Information or IT Resources classified at Protection Level 1 or 2 and/or Availability Level 1 or 2 access must be removed in thirty (30) days or less.

9.2.4. Units must review accounts and access rights at least annually and remove access that is no longer needed. Accounts that have not been accessed for 180 consecutive days must be reviewed and access removed if no longer needed.

9.3. Functional Account Management

Functional accounts (such as group UCINetIDs and shared local accounts) are shared accounts that can be accessed and used by multiple individuals.

9.3.1. Each functional account must have at least one designated owner who is responsible and accountable for the management and appropriate protection of account credentials and access. The functional account owner must document:

- The purpose of the account
- A list of all individuals who have access to the account
- All of the IT Resources and applications where the functional account is used.

9.3.2. Functional Accounts must be reviewed at least once per year to validate continued use and access needs. Functional accounts must be disabled or deleted when no longer needed.

9.3.3. Workforce Members must use functional accounts only for their intended business function.

9.3.4. The use of Functional Accounts should be done through auditable processes (such as “sudo”, etc.) so that account usage can be linked to individual personal accounts. Where this is not possible, direct logins through shared passwords are permitted provided passphrases are stored securely, are distributed on a need-to-know basis, access to the passphrases are controlled and auditable, and passphrases are changed when anyone with access to the account/passphrase leaves or separates. Enterprise tools such as Secret Server or LastPass Enterprise should be used to control access to Functional Account credentials where possible.

9.3.5. Functional accounts must not be used to access any Institutional Information or IT Resources classified at Protection Level 4 and/or Availability Level 4 without processes and logging in place to ensure accountability.

9.4. Service Account Management

Service Accounts are intended for automatic processes such as batch jobs or applications.

9.4.1. Each Service Account must have at least one designated owner who is responsible and accountable for the management and appropriate protection of account credentials and access. The service account owner must document:

- The purpose of the account
- A list of all individuals who have access to the account
- All of the IT Resources and applications where the service account is used

9.4.2. Service Accounts must be reviewed at least once per year to validate continued use and access needs. Service accounts must be disabled or deleted when no longer needed.

9.4.3. IT Workforce Members must ensure that Service Accounts are only used for system processes and not used for interactive use.

9.4.4. IT Workforce Members must use unique service account credentials for each logical part of the software/system.

9.4.5. Service Account credentials must be stored securely and access to the credentials must be controlled and auditable. Enterprise tools such as Secret Server or LastPass Enterprise should be used to control access to credentials where possible.

9.5. Privileged Account Management

Privileged Accounts are used to configure, manage, or significantly change the behavior of an IT Resource.

9.5.1. IT Workforce Members must configure accounts on IT Resources with separate accounts for privileged and unprivileged access. Documentation must be maintained as to which users were granted access to Privileged Accounts. UISLs must ensure Privileged Accounts have a strictly defined scope of access and are not used for day-to-day tasks such as email, web browsing, etc. Use of Privileged Accounts should be limited for as long as necessary to complete the task that requires the additional privileges.

9.5.2. Privileged Accounts should either be created and assigned uniquely to individuals or by using a mechanism for granting access to Privileged Accounts using a privilege escalation mechanism which logs privilege escalation use. When use of privilege escalation is not feasible and privileged account passphrases must be shared with multiple individuals (e.g., network appliance, switch or router passphrases), the sharing must be justified and approved following the appropriate risk exception process. The use, management and tracking of privileged account access must be auditable using enterprise tools such as Secret Server or LastPass Enterprise.

9.5.3. When privileged access is no longer needed for UC business purposes, UISLs must ensure that Workforce Members appropriately and promptly reduce or remove access.

9.6. Guest, Supplier, and Affiliate Account Management

9.6.1. All non-Workforce Member user accounts (user accounts for those who are not Workforce Members) and guest accounts with access to UC Institutional Information classified at Protection Level 2 or higher must comply with the UCI ISS. This includes accounts and passphrases used by parents, guardians and benefactors of students for purposes of paying fees, expenses or similar functions.

9.6.2. Procedures for accounts and passphrases for guests and affiliates must be set by the CISO.

9.7. Authentication and Passphrase Management

9.7.1. All non-privileged account passwords must be a minimum length of 8 characters, contain letters, numbers, and special characters, cannot be a previously used passphrase, and must not contain a part of your first name, last name or account name.

9.7.2. All privileged account passwords must have at least 12 pseudo-random characters.

9.7.3. Units must use a CISO-approved method for authenticating users to IT Resources and applications. Wherever possible, Units should use enterprise authentication services provided by OIT such as Active Directory or Kerberos for systems and Shibboleth for web applications.

9.7.4. Workforce Members must not share user account passphrases, PINs, or tokens with others. Units, Service Providers and Workforce Managers must not request or require a Workforce Member to share the passphrase to a user account.

9.7.5. Workforce Members must report any compromise or unauthorized disclosure, use or compromise of any passphrase or other authentication device to the UISL and to the CISO using the UCI Incident Response Process.

9.7.6. Accounts used to access Institutional Information or IT Resources classified at Protection Level 3 or higher and IT Resources classified at Availability Level 3 or higher must use multifactor authentication. UCI Duo should be used where possible.

9.7.7. If multifactor authentication cannot be implemented as required for an IT Resource, the documented risk exception process must be followed and user account passphrases must be changed on a regular basis of annually or less or on a schedule defined by a Risk Assessment, Risk Treatment Plan, or as defined by the CISO.

9.7.8. Workforce Members accessing Institution Information classified at Protection Level 3 or higher or IT Resources classified at Availability Level 3 or higher must not use the "remember your password" option in browsers or other applications. The use of an approved password manager can be used if this functionality is needed.

9.7.9. The use of password managers or software applications designed to manage user passwords and passphrases securely must undergo a risk assessment and be approved by the CISO. LastPass Enterprise is the preferred solution for enterprise use at UCI.

9.7.10. The IT Workforce Member responsible for an IT Resource must ensure the IT Resource or application is configured to do one or more of the following in response to ten (10) or more failed login or security question response attempts:

- Lock the account to prevent additional attempts
- Progressively delay the next attempt (rate limiting)
- Present a challenge, such as a CAPTCHA.
- Require an out-of-band authorization code.
- Use other risk-based or adaptive authentication techniques to identify whether user behavior falls within typical norms.

9.7.11. IT Workforce Members implementing or managing security challenge questions must:

- Use at least three (3) questions
- Avoid, as a means of authentication, knowledge-based challenge questions whose answers are likely to be available from public sources
- Ensure that questions are not predicable and that each user is presented random questions from the set of available questions.
- UISLs implementing systems or applications using this feature must review the application and challenge questions with the CISO.

9.7.12. Workforce Members must change passphrases immediately if independently discovered, if publicly disclosed, if a suspected compromise has occurred, if their device has been lost or stolen, or if notified to do so by OIT Information Security. This includes discovery of either plain text and/or hashed passwords or passphrases.

9.7.13. Contracts, regulatory requirements and other compliance requirements may require specific controls on accounts, authentication, use of multifactor authentication and/or passphrase change frequency. In all cases, Workforce Members must follow the strongest requirements.

9.7.14. Workforce Members storing passphrases for Wi-Fi, e-mail and other applications on single-user devices must use a compliant PIN or passphrase and encryption to secure access to the device (e.g., laptops, mobile phones, tablets, etc.).

9.7.15. Passphrases and PINs must be encrypted or securely hashed when stored electronically.

9.7.16. When communication of passphrases is required (e.g., communication of a shared account passphrase) Workforce Members must:

- Use a secure communication channel.
- Not send passphrases or other secrets in plain text using email or with the file the passphrase protects. Temporary or onetime passwords may be communicated using SMS, email, an out-of-band authorization code or during a phone call (but not via voicemail).
- Passphrase reset links or codes must have a limited lifespan of 24 hours or less.
- All temporary passphrases or access codes must be unique and not easily guessed

9.7.17. When a Workforce Member creates, takes control of or resets the passphrase for an account, the IT Resource must require the user to create a passphrase that complies with this Standard. In cases when the preceding requirement is not technically possible, the initial passphrase must be unique, must comply with the passphrase complexity requirements of this Standard and must be communicated securely.

9.7.18. Units must have proper auditable procedures in place to maintain custody of service account "shared secrets" in the event of an emergency and/or if the super-passphrase holder is unavailable. UISLs must ensure that shared secrets are changed after emergency use.

9.7.19. Workforce Members must not use UC passphrases for social media, shopping or other personal applications.

9.8. Web Session Length

9.8.1. Web applications providing access to IT Resources classified at Protection Level 2 or higher or Institutional Information classified at Protection Level 2 or higher must implement a web session inactivity timeout to terminate inactive or idle web sessions after a maximum defined period of 15 minutes for Protection Level 4, one hour for Protection Level 3, and nine hours for Protection Level 2, or as defined by an appropriate Risk Treatment Plan approved by the CISO.

9.8.2. Web applications providing access to IT Resources classified at Protection Level 2 or higher or Institutional Information classified at Protection Level 2 or higher must implement a maximum session length of no more than nine hours.

10. Encryption

10.1. General Encryption Requirements

10.1.1. Units must use an encryption method based on a risk assessment for their use case and approved by the CISO. See OIT encryption guidance.

10.1.2. Approved encryption methods must meet the following minimum standards:

- Symmetric - AES (128 bits or higher)
- Asymmetric/Public-Private key pair - RSA (2048 bits or higher)

10.1.3. IT Workforce members must use a minimum of TLS 1.2 or later for communications where authentication credentials are being exchanged or when Institutional Information classified at Protection Level 3 or higher is transmitted. Only secure ciphers should be configured.

10.2. Encryption at Rest

10.2.1. Units must fully encrypt all portable computing devices including laptops, tablets and phones. See OIT encryption guidance for recommended laptop encryption products.

10.2.2. Units must encrypt all Institutional Information classified at Protection Level 3 or higher when stored on any portable media including thumb drives, portable disk drives, backup tapes or optical media. Encryption can be implemented at the device, folder, or file level as appropriate. Even when encrypted, portable media must be securely stored.

10.2.3. Units must encrypt all Institutional Information classified at Protection Level 4 when stored on any electronic media such as disk drives or cloud storage. Encryption can be implemented at the device, folder, or file level as appropriate.

10.3. Encryption in Transit

10.3.1. Units must ensure that all authentication and Institutional Information classified at Protection Level 3 or higher is encrypted using secure protocols when transmitted over a public or general use mixed Protection Level network. Encryption is not required for Institutional Information transmitted over physically secure private networks such as dark fiber, data center backup networks or secure networks behind load balancers and firewalls using the appropriate risk assessment process or as approved by the CISO.

10.3.2. Units must ensure an encrypted connection (i.e. HTTPS, SSH or cryptographically strong protocol) must be used for all authentication sessions and all subsequent access.

10.3.3. IT Workforce Members must either disable unencrypted protocols when encrypted protocols are available or provide a redirect to force connections to use the encrypted protocol. HTTPS must be used instead of HTTP connections for all publicly exposed web services. HTTP may be used over physically secure private networks such as dark fiber, data center backup networks or secure networks behind load balancers using the appropriate risk assessment process or as approved by the CISO.

10.4. Database encryption

10.4.1. IT Workforce Members must enable Transparent Data Encryption (TDE) capabilities for databases storing Institutional Information classified at Protection Level 3 or higher. Column level encryption can add additional protection but must implement a CISO-approved method.

10.5. Encryption Key Management

10.5.1. Workforce Members must protect private encryption keys to prevent their unauthorized disclosure. Private keys must:

- Physically and logically be kept secure, stored in an encrypted key store, security token or encryption keyring. Access to private keys controlling access to Institutional Information protected at Protection Level 4 must be logged and auditable and should use a privileged access management tool.
- Only be shared with authorized individuals limited to those who have a need-to-know based on job responsibilities. Auditable procedures must be in place to provide access to private keys in the event of an emergency.
- Never be stored on the same IT Resource as the Institutional Information being protected unless using an additional CISO-approved method.
- Never be reused to encrypt other unrelated Institutional Information.

10.5.2. Workforce Members generating private keys must:

- Use a key size of AES 128 bit or greater for symmetric key encryption.
- Use a secure random key generation mechanism.
- Generate keys on the IT Resource itself or, if transmission of a private key is required, distribute keys manually using a public key transport mechanism or using a previously distributed or agreed-upon key-encrypting key.

10.5.3. For private keys protecting Institutional Information classified at Protection Level 3 or higher, UISLs must ensure that keys are changed keys at least annually or when Workforce Members with access to private keys separates or changes roles.

10.5.4. Workforce members must backup the private key associated with any encryption at rest of Institutional Information. The UISL must ensure that private keys are placed in escrow using at least one CISO-approved role or a CISO-approved key management tool.

10.5.5. Workforce Members handling Institutional Information classified at Availability Level 3 or higher must test key recovery or business continuity/disaster recovery of keys at least once annually.

10.5.6. Workforce Members must have a documented process in place to change encryption keys immediately if the key becomes compromised or is discovered by any unauthorized person or party. Workforce Members must report any compromised key to the CISO using the UCI Incident Response Process.

10.5.7. Private keys must be securely revoked and/or deleted when they are no longer needed or when key destruction is used to ensure secure cryptographic erasure of data.

10.6. Certificates

10.6.1. Self-signed certificates must not be used for any production service or used for testing IT Resources processing, storing or transmitting Institutional Information classified at Protection Level 3 or higher.

10.6.2. IT Resources with factory-installed self-signed certificates can only be used on protected private networks.

10.7. Web Server Certificate Management

10.7.1. Web server certificates must use digital certificates using a key size of 2048 bits or greater signed by a CISO-approved certificate authority (CA). Web server certificates must use a new public-private key pair each time the certificate is requested or renewed. The UCI Certificate Service should be used where possible.

10.7.2. Expiration dates for web server certificates for IT Resources classified as Critical Infrastructure or hosting Institutional Information classified at Protection Level 4 must not exceed 1 year. All other web server certificates must not exceed 2 years.

10.7.3. Web server certificates must not use wildcard certificates for top level domains or subdomains for IT Resources accessing Institutional Information classified at Protection Level 3 or higher.

10.8. Code Signing Certificate Management

10.8.1. Workforce Members handling code signing certificates must:

- Protect access to these certificates with multifactor authentication
- Restrict access to authorized Workforce Members who have a need-to-know based on job responsibilities.

11. Physical and Environmental Security

11.1. General Requirements

11.1.1. Workforce Members must physically secure IT Resources and Institutional Information to provide protection from unauthorized access, loss, theft or damage. Units must provide guidance to Workforce Members to ensure that portable computing devices and portable media containing Institutional Information classified at Protection Level 3 or higher are securely stored.

11.1.2. All physical access to secured areas must be based on job responsibilities.

11.1.3. Units must document the authorized secure storage locations and physical security measures appropriate to protect Institutional Information and IT Resources. Required physical security measures must be appropriate and consistent with:

- Statutory, regulatory and contractual requirements
- Controls based on Institutional Information Protection Level and Availability Level Classification
- Administrative and physical controls on third-party access and supervision.
- Secure storage area entry controls, logging and auditing.

11.1.4. Units must ensure correct and secure operations of information processing facilities such as data centers, including:

- Protecting IT Resources classified at Availability Level 4 from power failures and other disruptions caused by failures in supporting utilities or environmental controls.
- Protecting power cabling and cabling carrying Institutional Information or supporting information services from unauthorized physical access, interception, interference or damage.

11.2. Transportation and Transfers

11.2.1. 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, UISL or Proprietor. If taken off-site, Units must provide guidance to ensure Institutional Information is adequately protected.

11.2.2. Units must track IT Resources and update asset location in inventory documentation as needed. Units must track and use secure methods for transfers of electronic media containing Institutional Information classified at Protection Level 2 or higher.

12. Operations Management

12.1. General Operations Management Requirements

12.1.1. UCI Units must document specific administrative operating controls to support the requirements of the UCI ISS, and the operation of Unit IT Resource(s). In addition, Units must plan for future capacity requirements, replacing or retiring unsupported IT Resources, and the decommissioning of IT Resources.

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

12.1.3. Units must ensure that testing and development environments that contain Institutional Information include all appropriate security controls required for the production environment based on the Protection Level and Availability Level.

12.2. IT Resource Hardening

12.2.1. IT Workforce Members must implement recommended hardening scripts or controls for software and operating systems processing or storing Institutional Information classified at Protection Level 3 or higher or Availability Level 3 or higher. Where possible, a standard benchmark framework

must be used such as the Center for Internet Security Benchmarks. Where a standard benchmark cannot be used, hardening procedures must be documented and auditable.

12.2.2. For IT Resources classified at Protection Level 3 or higher, Availability Level 4 or Critical IT Infrastructure, Units must configure and enforce the required minimum security configuration settings defined in UCI ISS Section 14.

12.2.3. IT Workforce Members must remove or disable default user or system accounts and/or credentials. Where default accounts must be used, passphrases must be changed from the system defaults and a strong passphrase must be used before the system is connected to the UCI network.

12.2.4. Only network services needed to support documented business needs must be enabled. All other services must be disabled or removed.

12.2.5. UCI network access must be limited to devices that need access for the approved use case on each network. The minimum security requirements documented in UCI ISS Section 14 must be implemented for all devices and users connecting to the UCI network.

12.2.6. An encrypted connection (i.e. HTTPS, SSH or cryptographically strong protocol) must be used for all authentication sessions and all subsequent access.

12.2.7. Unauthenticated access or anonymous logins may be permitted for Institutional Information classified at Protection Level 1. IT Workforce Members must ensure that unauthenticated or anonymous connections are not allowed for applications hosting Institutional Information classified at Protection Level 2 or higher.

12.2.8. IT Workforce Members using software that is processing or storing Institutional Information classified at Protection Level 3 or higher must comply with the logging requirements in UCI ISS Section 12.7.

12.2.9. IT Workforce Members must install and enable security agents as required on OIT managed systems or other systems as required by the CISO or Units.

12.2.10. Units must regularly review IT Resource security and logging configuration settings based on risk to ensure they remain configured appropriately.

12.3. Change Management

12.3.1. Units must obtain approval for software installation, configuration changes and updates on production systems using the Unit's documented change management process. This change management plan must provide documented procedures for emergency, normal and standard changes (ITIL) or follow the OIT change management process for emergency, comprehensive, and routine changes.

12.3.2. Change management processes must document:

- The specific change and any impact to security
- How the change will be communicated to stakeholders
- The impacted IT Resources and user groups
- The time, date, and expected duration of the change
- How the change will be tested and any criteria for deciding whether to accept or back out the change.
- A back out plan for restoring the previous system state.
- The approval of the change
- The result of the change

12.4. Patching

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

12.4.2. Units must take a prioritized approach to installing available security patches to operating systems and applications and document patch installation frequency. Critical and high-risk vulnerabilities must be patched as soon as possible, not later than 14 days. Units must document and implement applicable compensating controls to manage risks related to patch frequencies greater than 30 days.

12.4.3. IT Workforce Members must ensure that installation, management, and patching of operating systems and software comply with the Minimum Security requirements in UCI ISS Section 14.

12.4.4. Units must protect IT Resources that cannot be patched to current standards with compensating controls approved through the risk exception process or remove the IT Resource from the UCI network or UCI managed cloud services.

12.5. Backup and Recovery

12.5.1. Units must ensure that Institutional Information classified at Availability Level 3 or higher is backed up and recoverable and encrypted when stored on portable media. Backup recovery must be tested at least annually.

12.5.2. IT Workforce Members must develop, implement and test a backup and archival method that meets with UCI and Unit business needs and complies with the UC Records Retention Schedule for retention of backups.

12.5.3. Units must protect backups according to the Protection Level of the Institutional Information they contain and must ensure that portable backup media meet the portable media protection and encryption requirements outlined in the UCI ISS.

12.5.4. Units must maintain a backup catalog that shows the location of each backup image or media and the corresponding retention requirements.

12.6. Vulnerability Management

12.6.1. Units must document and implement procedures to comply with the UCI Vulnerability Management Program. Vulnerable IT Resources may be removed from the UCI network until the vulnerabilities are addressed. VMP requirements include:

- Routinely monitoring Supplier or third-party patch advisories and bulletins to assess vulnerabilities.
- Assessing vulnerabilities using OIT Information Security provided vulnerability scan reports.
- Taking a prioritized approach to patch or apply other compensating controls to address the vulnerabilities.
- Documenting actions taken.

12.6.2. All IT Resources that process or store Institutional Information classified at Protection Level 3 or higher or for IT Resources classified at Availability Level 4 must implement regular agent-based or authenticated Tenable vulnerability scanning and have a documented process to remediate any findings.

12.6.3. Penetration testing must be conducted for Institutional Information and IT Resources classified at Protection Level 4 at least once every three years or when a major change occurs.

12.7. Logging

12.7.1. Logging Plan

- UISLs must establish and document a logging plan for their Unit. The plan must include:
  - A method to inventory systems that are required to log events for information security purposes.
  - Steps to manage cyber risk by assessing risk levels and resources for logging.
  - The level of logging detail required based on the Protection Levels of the IT Resource.
  - Log storage locations, both local and centralized. Logs forwarded to Service Providers and Suppliers must be identified, and expected roles, responsibilities and service responsibilities identified.
  - Log access requirements and procedures, ensuring that any privacy concerns are being met.
  - Processes for log monitoring and alerting.
  - Time synchronization.
  - Periodic testing to ensure logging and alerting is configured and functioning as expected.
  - Documented gaps and mitigations where logging requirements cannot be met.
- Units processing, storing or transmitting Institutional Information classified at Protection Level 3 or higher must submit and review their logging plan with the CISO at least annually.

12.7.2. General Logging Requirements

- IT Workforce Members must include event sources that are needed to manage cyber security risk in the Unit's logging implementation. Event sources include but are not limited to access control systems; authentication systems; databases; network devices; security services, devices, or systems; servers; or applications. Logging detail must include account creation and privilege escalation activity.
- Units must comply with the UC Event Logging Standard when storing, processing or transmitting Institutional Information classified at Protection Level 3 or higher.
- For Institutional Information classified at Protection Level 3 or higher, event logging must use CISO-approved logging tools and frameworks.
- All transmissions of logs must require secure protocols and reliable mechanisms.
- For IT Resources classified as Critical Infrastructure, Protection Level 3 or higher, or Availability Level 3 or higher, a copy of log data must be sent to a separate logical logging device that is protected with at least the same level of control as the IT Resource.
- Logs containing Institutional Information classified at Protection Level 3 or higher must require the same security controls as the Institutional Information they contain. Logs must never contain Protection Level 4 personal identifiers (e.g., Social Security Numbers (SSN), personal account numbers, financial account numbers, credit card numbers, etc) or clear text authentication credentials (e.g., passphrases, passwords, secret questions).
- When possible, IT Workforce Members acting as system administrators on IT Resources classified at Protection Level 3 or higher and Availability Level 3 or higher must not have permission to erase, deactivate or modify logs of their own activities.
- Units must ensure that the amount and type of information logged should be commensurate with the security needs of the Institutional Information and/or IT Resource and balances the needs of privacy and confidentiality.

12.7.3. Log Timestamps

- Units must ensure that the system clocks of IT resources within the Unit are synchronized using NTP or other UCI approved time synchronization method.
- Timestamps must be included in logs and not be truncated or abbreviated in any way and must use UTC or use a time zone offset that corresponds to local time.

12.7.4. Access to Logs

- 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 ensure that all access to logs is only available to authorized Workforce Members on a need-to-know basis.
- Units must ensure that access to logs is consistent with the UC Electronic Communications Policy and UCI 800-15: UCI Guidelines for the UC Electronic Communications Policy.

12.7.5. Log Monitoring Requirements

- Units must monitor all IT Resources to detect signs of attack or compromise.
- Units must have appropriate logging and monitoring in place for IT Resources to detect signs of attack or compromise for Resources classified at Protection Level 3 or higher or Availability Level 3 or higher.
- As required and scoped by the CISO, Units must configure IT Resources processing, storing or transmitting Institutional Information classified at Protection Level 3 or higher to provide log data to a Security Incident and Event Management system (SIEM).
- For Institutional Information classified at Protection Level 3 or higher, and IT Resources classified at Protection or Availability Level 4, UISLs must independently review privileged accounts periodically to ensure that only authorized activity occurred.
- For Institutional Information classified at Protection Level 2 or higher and IT Resources classified at Availability Level 3 or higher, actions performed by privileged user accounts in performance of their duties must be logged and reviewed by a peer (e.g., other admin, InfoSec

professional, etc.) based on risk in order to determine the appropriateness of the actions performed.

- As required and scoped by the CISO, Units must configure IT Resources processing, storing or transmitting authentication information to provide authentication log data to a Security Incident and Event Management system (SIEM).

12.7.6. Log Retention

- IT Workforce Members must document their implemented log retention schedule. Log retention must be based on the UC Records Retention Schedule, contracts, regulations, litigation holds, preservation orders, or any other external requirements.
- Units must obtain approval for erasing, purging or trimming event logs through the Unit change management process.
- All erasing, purging, or trimming of event logs must follow documented procedures that comply with data retention requirements. Unit change management processes must be followed for any changes outside of the documented procedures.

12.8. Cloud Services

12.8.1. Workforce Members must understand and set file sharing and cloud access controls and features so that only intended parties have access to Institutional Information.

12.8.2. IT Workforce Members must understand and set local and cloud access controls and features so only intended parties have access to configuration options.

13. Communications Security

13.1. Network Security

13.1.1. Units must route network access to Institutional Information classified at Protection Level 4 through secure access control points such as firewalls, secure proxies, etc.

13.1.2. Multifactor authentication is required for IT Resources that store, process or transmit Institutional Information classified at Protection Level 3 or higher.

13.1.3. Devices or servers must not be configured to bridge one security classification to another in an unauthorized manner (also known as split tunneling) or bridge networks that are intended to be segmented (also known as network bridging). If bridging is authorized, the specific use cases must be documented.

13.1.4. IT Workforce Members must install public facing applications storing or processing Institutional Information classified at Protection Level 3 or higher so that the database server is logically separated from the web server and application server.

13.1.5. IT Workforce Members must place systems on appropriately approved and segmented networks which are designed for the appropriate protection of the Institutional Information and IT Resources.

13.1.6. 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 approved by the CISO.

13.1.7. Units must ensure that any device connected to a UCI wired or wireless network complies with the Minimum Security Standards documented in Section 14.

13.1.8. Units must ensure that network access to Institutional Information classified at Protection Level 3 or higher is monitored to detect unauthorized access.

13.1.9. Units must turn off or disable unused ports, protocols and services for all UCI IT Resources.

13.1.10. Units must ensure that all UCI IT Resources use secure versions of network services including encrypted network services where available.

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

- Allow only authorized connections and use the most restrictive rules possible.
- Log and detect unauthorized access or access attempts.
- Review firewall and other network access rules at least annually or when systems or architectures change.

13.1.12. Units must obtain approval from the UCI CIO and complete an appropriate Risk Assessment or Risk Treatment plan approved by the CISO before using a Supplier for network services to interconnect the UCI network with the public Internet.

13.1.13. Units must ensure that use of protected wireless networks use encryption approved by the CISO and implement appropriate access control, segmentation, and intrusion detection technology when transmitting Institutional Information classified at Protection Level 2 or higher.

13.1.14. SMTP e-mail servers on UCI networks must require user authentication to relay e-mail messages between correspondents who are not on campus. This authentication requires a user ID and password; authentication via IP address or domain name is not sufficient without a documented security exception process.

13.1.15. Proxy servers connected to UCI networks must require authentication using a user ID and password. Authentication via IP address or domain name is not sufficient without a documented and approved security exception process. Any proxy server that is accessible off campus must ensure that users meet the requirements used to control access to UCI licensed intellectual property.

13.2. Secure Transfer

13.2.1. 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 encryption and other appropriate security controls approved by the CISO and Institutional Information Proprietor.

14. System Acquisition, Development and Maintenance

14.1. Minimum Security Standards for All IT Resources Connected to the UCI Network

14.1.1. **Anti-malware**: Anti-malware software must be installed and running up-to-date definitions. Both real-time protection and regular full scans must be performed. IT Resources classified at Protection Level 3 or higher should use an OIT supported Endpoint Protection product.

14.1.2. **Patching**: Supported security patches must be applied to all operating systems and applications. The patching process should be automated. For UCI owned devices, the patching process should be logged and auditable using an enterprise patch management tool such as Bigfix.

14.1.3. **Local admin or Administrator**: Non-privileged user accounts must be used for daily activities and only elevated to root or Administrator when necessary.

14.1.4. **Encryption**: All portable computing devices must be encrypted. If device level encryption is not supported, Institutional Information classified at Protection Level 3 or higher must be encrypted at the file, folder, or filesystem level.

14.1.5. **Session Timeouts**: Computing devices used to store, or access Institutional Information or IT Resources classified at Protection Level 2 or higher must employ lockout/screen-lock mechanisms or session timeouts to block access after a defined period of inactivity of 15 minutes. Re-authentication is required before returning to interactive use.

14.1.6. **Passwords, PINs and Locking**: Computing devices must be secured with a strong password, PIN, smart card, or biometric lock compliant with UCI minimum passwords requirements and the requirements listed in ISS Section 9.7.3.

14.1.7. **Physical Security**: Devices and Institutional Information must be physically secured to protect against loss and theft.

14.1.8. **Backup and Recovery**: Institutional Information classified at Availability Level 3 or higher must be backed up and recoverable. Backups must be physically protected and encrypted according to the classification level of the information they contain. Units must ensure that the backup plan is consistent with business needs, regulatory requirements and the UC Records Retention Schedule.

14.1.9. **Portable Media Encryption**: Portable media containing Institutional Information classified at Protection Level 3 must be encrypted and safely stored.

14.1.10. **Host-based Firewalls**: If host-based firewall software is available on a device, it must be running and configured to block all inbound traffic that is not explicitly required for the intended use of the device

14.1.11. **Purchasing Approval and Inventory**: Make sure devices and Supplier Services can be adequately secured before making a purchasing decision. Ensure that IT Resources and Institutional Information are recorded in the appropriate Unit or UCI inventory.

14.1.12. **Supported Operating Systems**: Run a version of the operating system that is supported by the vendor and that patches and updates are available.

14.2. Additional Minimum Security Standards for Servers, Appliances, and Applications Connected to the UCI Network

14.2.1. **Network services** must be secured as follows:

- Only network ports and protocols needed to support approved IT services must be enabled. All other services must be disabled or removed.
- Network access must be limited to systems that need access for the approved use case.
- An encrypted connection (i.e. HTTPS, SSH or cryptographically strong protocol) must be used for all authentication sessions and subsequent access

14.2.2. **Network Bridging**: Devices or servers must not be configured to bridge one security classification to another in an unauthorized manner (also known as split tunneling) or bridge networks that are intended to be segmented (also known as network bridging. If bridging is authorized, the specific use cases must be documented.

14.2.3. **Changing default passwords**: All default passwords included as part of the initial setup of any system must be changed as soon as practical, and in all cases prior to the system being moved to production. If no password is set, one must be set that meets the UCI Password Policy.

14.2.4. **Limit Access to Authorized Users**: Access to Institutional Information and IT Resources must be limited to authorized users.

14.3. Secure Software Configuration

14.3.1. Units must establish, document and maintain a security plan for each application, set requirements for business processes, and design security into all architectural layers. Data flow and network diagrams must be created and maintained.

14.3.2. Units must analyze new and existing software and technology to determine security risks and review the design against known risks and attacks.

14.3.3. IT Workforce Members must configure software so that appropriate security controls are enabled; logging and auditing features are enabled and provide information to support the detection of malicious action, the application is resistant to compromise, and comply with the UC Secure Software Configuration Standard.

14.4. Software Development

14.4.1. Workforce Members writing code or developing applications must comply with the UC Secure Software Development Standard and UCI Secure Software Development Guidance.

14.4.2. IT Workforce Members and the applications they develop and implement must not handle, store or manage user credentials directly, and must use CISO approved UCI authentication services.

14.4.3. Workforce Members writing code or developing applications must perform an appropriate Risk Assessment or Risk Treatment Plan before putting new code into production.

14.5. Security Planning

14.5.1. 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. Prior to the development or acquisition of a system, Units must include planning for system security requirements including:

- The planned Protection Level and Availability Level of the IT Resources and the Institutional Information stored or processed on them.
- Compliance with the Minimum Security requirements in UCI ISS Section 14.
- Plans for conducting the appropriate Risk Assessment or Risk Treatment Plan and addressing any documented gaps.

14.5.2. Units must plan and budget for supporting security personnel, processes, and tools to manage cyber security risk and implement required security controls.

15. Supplier Relationships

15.1. Contracts and Agreements

15.1.1. Units must select and use Suppliers who can adequately secure Institutional Information throughout the terms of the agreement. Units using Suppliers must:

- Negotiate an Appendix DS with the Supplier whenever Institutional Information is shared with the Supplier or the Supplier has access to IT Resources. Security responsibilities of each party must be clearly documented.
- Ask the Supplier to provide security compliance documentation such as a HECVAT, a security plan, or a CISO approved security questionnaire and, as appropriate, obtain assurance from a third-party audit report such as a SOC 2 report, or other documentation demonstrating that appropriate information security safeguards and controls are in place.
- Work with OIT Information Security to complete a risk assessment of the Supplier using the documentation provided to ensure the Supplier has security protections in place consistent with UC security requirements. At a minimum, these must comply with the minimum security requirements in UCI ISS Section 14. Any gaps must be documented in the Supplier review and the documented risk exception process must be followed prior to purchase.
- Ensure that the agreement includes any additional terms and conditions specified in law, regulation, grant or contract that may be applicable.
- The use of Suppliers for Critical IT Infrastructure must use the security requirements approved by the CISO.

15.1.2. Units using Suppliers who qualify as a Business Associate under HIPAA/HITECH must also negotiate a Business Associate Agreement (BAA) as part of the contract.

15.1.3. Units using Suppliers subject to the Payment Card Industry (PCI) Data Security Standard must follow UCI policy 704-14: Policy on Credit and Debit Card Acceptance and Security.

15.1.4. Ensure Supplier agreements have adequate business continuity and disaster recovery plans to meet UCI compliance and availability needs.

15.2. Compliance Requirements when using Suppliers

15.2.1. IT Workforce Members must secure Supplier remote access with multifactor authentication and unique credentials used only by that Supplier.

15.2.2. Units must monitor Supplier compliance throughout the term of the agreement. Units must:

- Ensure that Supplier access to IT Resources or Institutional Information remains consistent with UC security policies and only uses approved access methods. Additional security reviews must be done at contract renewal to document any Supplier compliance requirement changes and to ensure compliance requirements are still being met. Contracts and risk assessments must be adjusted accordingly to take into account any changes in business practices, scope and type of Institutional Information collected or exchanged, UCI IT Resources being accessed, and any legal or policy changes.
- Ensure that Suppliers report Breaches and Information Security Incidents to the UCI CISO.
- Ensure that Suppliers notify Units of any changes to Supplier security controls as documented in Appendix DS.
- Report any observed Supplier security lapses to the CISO via the documented Unit incident response plan.

15.2.3. Units using Suppliers must ensure Suppliers do not:

- Create new accounts without approval, use UC credentials beyond agreed uses, or share with anyone passwords or authentication credentials that provide access to UCI Institutional Information or IT Resources.
- Use passwords or other authentication credentials that are common across Supplier 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 to UCI Institutional Information or IT Resources.
- Reduce, remove or turn off any UCI IT Resource security control without approval from UISLs.
- Use or copy UCI Institutional Information for non-authorized purposes.

16. Information Security Incident Management

16.1. OIT Information Security must develop, document, maintain, and follow a master campus Information Security Incident Response Plan, which implements the required elements outlined in the UC Cybersecurity Incident Response Standard. This Incident Response Plan details the steps the campus will take when informed of a potential security incident from campus Units, Workforce Members, Suppliers, third-parties, or by internal security monitoring and alerts.

16.2. OIT Information Security must develop and socialize a standard method for Workforce Members and Students to report a potential security incident.

16.3. Units must develop, document and maintain a Unit Security Incident Response Plans which details how IT Resources and Institutional Information within the Unit are monitored and which events, alerts and potential security incidents are defined as Routine Incidents and can be handled internally and which potential security incidents are defined as Significant Incidents and need to be escalated to the OIT Information Security for further triage.

16.4. 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 OIT Information Security.

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

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

17. Information Security Aspects of Business Continuity

17.1. Business Continuity

17.1.1. Units must comply with the business continuity requirements described in BFB-IS-12.

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

17.1.3. 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.

18. Compliance with External Requirements

18.1. Workforce Members and Units must meet the obligations related to information security, intellectual property, records, privacy, personal information and encryption required in laws, government regulations, agreements, contracts, and grants.

18.2. Units and Service Providers must use and demonstrate an evidence-based approach to compliance with UCI ISS and any external requirements and be able to provide documentation and evidence of compliance as required by UCI or any external requirements.

18.3. Units must perform periodic reviews, at least annually, of information security practices, make corresponding adjustments to the application of UCI ISS, and update applicable Risk Assessments as required to comply with UCI ISS and any external requirements.

18.4. The UCI Cyber-Risk Responsible Executive (CRE) must ensure that UCI auditors or contracted third-party auditors periodically examine and report to management on compliance with UCI ISS and supporting UC policy and standards.

18.5. 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.