Information Security Guideline

Definitions can be found in Administrative Policy Statement 2.4, Information Security and Privacy Roles, Responsibilities, and Definitions.

1 Purpose

Administrative Policy Statement (APS) 2.6, Information Security Controls and Operational Practices, states that the University of Washington (University) shall implement and maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of institutional information, infrastructure technology, and information systems that it creates, receives, maintains, or transmits.

The purpose of this Information Security Guideline is to elaborate on the controls and practices, as well as provide examples to help individuals with information security or privacy responsibilities make informed decisions related to their organization's assets and corresponding security plan. This guideline along with the other resources published by the University Chief Information Security Officer (CISO) and Privacy Assurance and Systems Security Council (PASS Council) provide organizations with options to manage their risks and prioritize limited resources while maximizing their results.

This Guideline is intended to be flexible to meet the education, research, patient care, and service needs of the University while also addressing the multitude of legal and regulatory requirements that impart a duty on the University. In combination with other resources, it represents a due care position consistent with the information security and privacy risk management approach overseen by the CISO and PASS Council on behalf of the University.

This document is a living document and will be reviewed and revised as necessary. Check the CISO webpage to make sure you have the latest version.

2 Scope

This Guideline is applicable to all the University.

3 Security Plan

Intention
The executive heads of major University organizations are responsible for managing the risks associated with their assets. They, or their designee(s), must document and implement an Information Security Plan (Plan) that demonstrates due care in securing their assets by meeting the intention of the controls in APS 2.6.

Clarification
The Plan must address each of the requirements in the policy and include the following:

- Delegate Plan responsibilities to the appropriate people (e.g. information assurance liaisons, system owners, system operators).
- Describe the organization's approach to implementing the Plan (e.g. by department, by functional area, or by asset type).
- Include a Plan implementation timeline and milestones.
- Document critical assets and the controls that are implemented for each of them.

- Describe alternate or compensating controls and the rationale for selecting them.

An asset is defined broadly to include any hardware, software, or data that supports information-related activities. An asset can be owned or controlled; it has intrinsic value or can be used to produce value. Human beings, through the labor they provide can also be considered to be assets.

The nature of each asset largely determines what controls need to be implemented to protect it. Therefore, it is necessary to identify and value assets in order to select appropriate controls. Each asset is valued based on the potential harm to the organization, the University, and the individuals it serves if the asset were compromised by a loss of confidentiality, integrity, or availability. Controls can then be selected for individual assets or a group of assets based on their value to the University and the resultant level of risk that is acceptable to the executive head. Not all controls are appropriate for all assets, and it is the suite of controls that determine the overall level of protection for managing the risk of the asset.

Consider the following when developing a Security Plan:

- One size doesn't fit all – Some departments or individual assets may require their own Plan because of specific regulatory requirements (e.g. HIPAA, FISMA; see Section 11, Additional Information), or because their environment is very different from the parent organization.
- Centralized services – Organizations that utilize centralized services (e.g. UWNetID authentication) can reference the service that addresses a particular requirement and note where the lines of responsibility and accountability begin and end for the organization and the centralized service.
- Outsourcing – If you are working with a third party to provide information services, reference the service that addresses a particular requirement and the location of the signed contract. Note where the lines of responsibility and accountability begin and end for the organization and the outsourced service.
- Be efficient and effective - Identify your critical assets and choose controls.
- Don't over analyze – Avoid lengthy or overly descriptive digressions on if or how assets can be compromised.
- Map asset dependencies – An asset may be critical because of its own value or because other assets depend on it.
- Draw a picture – Consider drawing a picture of your assets and how they interact.
- Use existing sources – Asset information may already exist. If possible use this information rather than recreate it.

4 General Operational Controls

4.1 A change and configuration management process

Intention

The intention of this requirement is to document, review, and approve changes (including emergency changes) while minimizing defects, disruptions, and unauthorized exposures.

Clarification

The goal of a change management process is to effectively and efficiently identify, evaluate, make decisions, prioritize, communicate, and document changes to assets. Change is inevitable; a good operational practice is to accept change, plan for it and control it appropriately.

Change management involves the following steps:

1. Establish a process for evaluating and making decisions about the change.
2. Manage risks introduced by the organization's approach to change management as well as the risks associated with each change.
3. Establish accountability for the authorization and implementation of different types of changes.
4. Communicate the change to individuals who are impacted by the change. Because most systems are interrelated, a change made to one system can have major impacts on others.
5. Document essential risks, decisions, and authorizations for the change.
6. Implement the change.
7. Verify the change was as expected and address any unintended consequences/outcomes of the change
8. Continuously improve the change management process based on lessons learned from the change.

Remember that one size doesn't fit all. Different change and configuration management processes can be implemented for different portions of the organization, for a group of similar assets, or for an individual asset. The benefits of effective and efficient processes often outweigh the costs of unintentional outages or data loss that may result from not appropriately managing change.

Examples

- Ensure that changes to systems and applications are authorized, planned, announced, and documented before being implemented.
- Ensure that roles and responsibilities are defined and documented.
- Prior to implementing changes, develop a plan to reverse or remove changes should problems arise.
- Monitor changes to the information system, and conduct security impact analyses to determine the effects of the changes.
- Prior to change implementation, and as part of the change approval process, analyze changes to the asset for potential security impacts.
- After the change is implemented, check the security features to verify that they are still functioning properly.
- Audit activities associated with configuration changes.

4.2 A flaw remediation process

Intention

The intention of this requirement is to identify, report, and correct potential vulnerabilities.

Clarification

Software flaws, and the vulnerabilities resulting from such flaws, introduce potential attack vectors that put your organization's information assets at risk. The purpose of this requirement is to limit the organization's exposure to flaws that have been announced and confirmed, and flaws that have been discovered and/ or reported to the organization.

Organizations should implement a process that identifies information assets potentially affected by announced software flaws and establishes a mechanism for reporting flaws to accountable parties (system owner and operators). This process should include an assessment of the potential risks and impact of the flaw, flaw mitigations, and it should result in a remediation strategy. Finally, the process should ensure that remediation efforts (fixes, alternate mitigating controls, etc.) are applied in a timely manner.

Information assets affected by announced software flaws, and the vulnerabilities resulting from those flaws, must be identified and reported to the appropriate individuals (system owners and operators). Those individuals must ensure that newly released patches, service packs, and hot fixes are promptly installed. In some cases, a contractor may do this, but the organization is still responsible for seeing that it is done. Patches, service packs, and hot fixes should be tested for effectiveness and potential side effects on information assets and dependent assets before installation. Remediation actions must be incorporated into the change and configuration management process so they can be tracked and verified and to prevent reoccurrence.

Examples

- Ensure that information asset flaws and vulnerabilities are identified, assessed, and prioritized.
- Ensure flaws and vulnerabilities are corrected in a timely manner and in accordance with the change and configuration management process.
- Implement a process for that leverages the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases for identifying potential flaws.
- Identify, report, and correct information asset flaws.
- Test patches, service packs, and hot fixes for effectiveness and potential side effects on information assets and dependent assets before installation.
- Incorporate flaw remediation into the configuration management process.
- Install software updates automatically.
- Organizations that choose to automate flaw remediation practices should apply appropriate controls to reduce the unintended uses of this control.

4.3 A malicious code and unauthorized software countermeasure process

Intention

The intention of this requirement is to implement and regularly update mechanisms that prevent, detect, and remove malicious code and unauthorized software.

Clarification

Malicious software in this context includes software that causes disruption, gathers data, or gains unauthorized access to systems or institutional information. The organization should employ malicious code protection mechanisms at critical entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware). To be effective, malicious code protection mechanisms must be updated, preferably in an automated fashion, whenever new releases are available (in accordance with organizational configuration management procedures).

One often-overlooked issue is licensed software - which must be used in accordance with contract agreements and copyright laws. For software protected by quantity licenses, the organization should consider employing a tracking system to control distribution.

In organizations where it is not feasible to restrict software to only authorized and approved software, a strong education program is needed to encourage safe behaviors.

Examples

- Ensure that anti-virus software is installed, running, and regularly updated.

- Implement mechanisms to detect and address unauthorized software.
- Comply with software usage restrictions.
- Centrally manage malicious code protection mechanisms.
- Automatically update malicious code protection mechanisms.

4.4 A data protection and destruction process

Intention
The intention of this requirement is to protect against the unintended exposure of Confidential or Restricted information in all forms.

Clarification
UW Confidential or Restricted information can reside on both digital media (e.g., magnetic diskettes and tapes, external/removable hard drives, flash drives, compact disks, digital video disks, email, electronic files) and non-digital media (e.g., paper, microfilm). Digital media also includes portable and mobile computing and communication devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones, telephone voicemail, tablets). Media containing UW Confidential or Restricted information must be protected until it is no longer needed, at which time it must be sanitized using approved procedures. Sanitization is a procedure to remove information from media so there is reasonable confidence that the information cannot be recovered.

Organizations should document and mark media that requires restricted access, which individuals are authorized to access the media, and the specific measures taken to restrict access. Documentation should also include retention instructions and any specific measures required during transport outside of controlled areas. A controlled area is any space with physical and procedural protections that are sufficient to meet the requirements established for protecting the information in the space.

Examples
- Implement strict records retention schedules, and remove/destroy records (including email/attachments) once the retention period has passed.
- Implement mechanisms to encrypt UW Confidential information at rest on selected storage devices.
- Implement procedures for handling and storing media that contains UW Confidential or Restricted data.
- Implement procedures for transporting media that contains UW Confidential or Restricted data outside of designated areas.
- Restrict access to media and devices to authorized individuals.
- Attach labels to media indicating the access, distribution, and handling warnings.
- Implement procedures in accordance with NIST Special Publication 800-88 to sanitize media that contains UW Confidential or Restricted data prior to disposal, release, or reuse.

4.5 Secure development practices

Intention
The intention of this requirement is to implement a life cycle methodology that includes information security considerations.

Clarification
For the purpose of this requirement, development is defined as building, integrating, or enhancing an information system.

A System Development Life Cycle (SDLC) is a model for the development and maintenance of an application, software, or system. The intention of a SDLC is to produce a product that is cost-efficient, effective, reasonably secure, and of high quality. It is important to include security considerations at each stage of the SDLC. A SDLC usually contains the following stages: planning/analysis, development, testing, and release. In the planning and analysis stage, the purpose of the product is determined, goals are established, and a set of requirements is developed. You should also consider the unintended uses of the system and impacts on other systems and practices. Identify the security risks and any mitigating controls (e.g. logs, access control, backups etc.). In the development stage, the product is coded/built/produced while attempting to meet all of the requirements. You should document dependencies, data generated and data consumed, and you should follow secure coding best practices. In the testing stage, the product is tested to ensure that it performs as expected. Include testing for vulnerabilities and confirm proper functioning of security controls. Once the product meets requirements and is deemed ready for use, establish a role back plan before the product is pushed to full release. It will now enter the maintenance stage. In the maintenance stage the product falls under the flaw remediation process and the change and configuration process.

One security consideration during the SDLC is to pay attention to the structure and content of error messages. Error messages should only be revealed to authorized personnel, and should provide timely and useful information without revealing potentially harmful information that could be used by adversaries. Another consideration is that sensitive information (e.g., account numbers, social security numbers, and credit card numbers) should not be written to logs or administrative messages. Input validation is a very important security consideration. Checks for accuracy, completeness, validity, and authenticity of input information should be accomplished as close to the point of origin as possible. Check the valid syntax of inputs (e.g., character set, length, numerical range, acceptable values) and verify that inputs match specified definitions for format and content. Inputs passed to interpreters should be screened to prevent the content from being unintentionally interpreted as commands. Also, integrity checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) should be used to automatically monitor the integrity of the information and the application/software/system that hosts it.

Many Web application vulnerabilities are a direct result of improper input validation and output filtering, which leads to numerous kinds of attacks, including cross-site scripting (XSS), SQL injection, command injection, buffer overflows, and many others. Whenever an application needs to gather information from a user or a browser, that information must be validated carefully to remove potential attack strings. Likewise, data sent back from the Web server to a browser should be filtered to make sure that exploits that an attacker has managed to sneak onto a Web server aren't returned back to unwitting consumers who visit the site.

Examples

- Identify and implement web development and secure coding guidelines that address information security and privacy risks.
- Minimize the use of production data in test and development environments.
- Manage test and development environments that use production data as if they were production environments.
- Identify and remediate vulnerabilities in applications and systems before they go into production.
- Perform in-depth testing (e.g. code reviews or penetration tests) of applications and systems before they go into production.

- Ensure that contracts, agreements, or memorandums of understanding with third party developers include adequate terms and conditions (e.g. Data Security Agreement).
- Manage information assets using a development life cycle methodology that includes information security considerations.
- Require that developers create and implement a configuration management plan that controls changes during development; track security flaws, require authorization of changes, and provide documentation of the plan and its implementation.
- Require that developers create a security test and evaluation plan, implement the plan, and document the results.
- Identify and handle error conditions without providing information that could be exploited by adversaries.
- Check input information for accuracy, completeness, validity, and authenticity.
- Restrict to authorized personnel the capability to input information to the asset.
- Detect and protect against unauthorized changes to software and information.
- Handle and retain output from the information asset in accordance with University policy and applicable laws and regulations.
- Use well-known and carefully vetted validation code.
- Specify variable types.
- Don't define all possible bad characters; instead accept only good ones.
- Filter and limit the size of all input.
- Filter on the server side.
- Canonicalize before filtering.
- Utilize and choose the appropriate output encoding.
- Conduct a secure code review and penetration test.

4.6 Backup and recovery processes for critical information and software

Intention
The intention of this requirement is to implement regular and secure backups in order to minimize disruption and effectively restore information assets.

Clarification
The backup and recovery plan defines procedures intended to reduce the chance of data loss and interruption to operations, and to allow recovery as quickly as possible if such events do occur. Backup and recovery processes and procedures vary according to the needs of the organization and must be developed and periodically reviewed by the appropriate personnel. Verification of the backup and restore processes is essential. Test processes thoroughly with as many simulated failures as possible. Testing can demonstrate the true time required to restore data and can uncover hardware problems that do not show up with software verifications. The frequency of backups, the transfer rate of backup information to the storage site, and the time to resume operations need to be consistent with the organization's recovery time objectives and recovery point objectives. Equipment and supplies required to resume operations within a defined time period need to either be available at the alternate site or contracts need to be in place to support delivery to the site.

The backup and recovery plan should:

- Define roles and responsibilities
- Identify situations where problems might occur
- Classify the severity of problems

- Determine system dependencies so you have a clear understanding of the impact of a failure
- Define acceptable downtime
- Define backup frequency
- Define backup media, labeling, storage location, and retention period
- Include procedures for periodic backup of system configuration and data
- Include procedures for testing backup and recovery processes
- Define a schedule for periodic testing of backup and recovery processes
- Determine which systems have the highest priority for recovery

While integrity and availability are the primary concerns for backups, protecting their confidentiality is also an important consideration. Backup media must be stored and transported in a safe and secure manner and access to backup media must be restricted to authorized personnel. Controls, such as encryption (at rest, and over the wire), access controls, and physical security should be implemented to protect backups that contain sensitive data. Obsolete backup media must be disposed of in a safe and secure manner, in accordance with University policy.

High availability solutions often introduce increased complexity. If the system includes automated failover capability, "no-op" scenarios should be tested in addition to the fail-over scenario. For example, confirm that loosing a redundant failover environment does not negatively impact the production environment.

Examples

- Conduct backups based on needs and requirements (e.g. systems, data, frequency, incremental vs. full, and schedule).
- Encrypt backup media to protect the confidentiality and integrity of the information.
- As needed, based on criticality of system, application, and/or data, test backups to verify media reliability and information integrity.
- Configure an alternate storage site that is geographically separated from the primary storage site so as not to be susceptible to the same hazards, and to facilitate timely and effective recovery operations. Initiate necessary agreements to permit the resumption of information system operations for critical mission/business functions within a defined time period.
- Conduct backups of user-level and system-level information and protect backup information at the storage location.
- Test backup information to verify media reliability and information integrity.
- Include a full recovery and reconstitution of the information system as part of contingency plan testing.
- Obtain alternate telecommunications services that do not share a single point of failure with primary telecommunications services and develop service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.
- Require primary and alternate telecommunications service providers to have adequate contingency plans.
- Implement regularly scheduled downtime to reduce communication costs and potential negative impacts, when maintenance, troubleshooting, or upgrades are needed.

4.7 A business continuity and disaster recovery plan

Intention

The intention of this requirement is to establish plans and procedures to continue operations after an incident.

Clarification

For most organizations, information assets are necessary to accomplish their mission. Because of this, it is critical that these assets are able to operate effectively and without excessive interruption. By establishing adequate business continuity and disaster recovery plans and procedures, systems, services, and data can be restored quickly and effectively following a disruption. Business continuity encompasses the activities that are performed by an organization daily to maintain service availability, consistency, and recoverability. Disaster recovery is a subset of business continuity and is the process by which you resume business after a disruptive event. Business continuity and disaster recovery plans need to include how workforce members will communicate, where they will go, and how they will keep doing their jobs. Business and technology subject matter experts need to work together to determine which assets and business processes are most critical to the organization. Together they decide who is responsible for declaring a disruption and what steps need to be taken to mitigate its effects. Contingency plans and procedures must be consistent with University policies, as well as applicable laws and regulations. The contingency plan can be included as part of the information security plan for the organization.

Examples

- Identify critical assets and, as needed, establish a business continuity and disaster recovery plan that addresses purpose, scope, roles, responsibilities, contact and coordination information, capacity planning, and activities associated with restoring systems after a disruption or failure.
- Identify essential personnel and establish procedures and provisions to support these individuals.
- Coordinate business continuity and disaster recovery plan development with external organizations with (upstream or downstream) dependencies.
- Designated individuals within the organization review and approve the business continuity and disaster recovery plan and distribute copies to key contingency personnel.
- Train workforce members in their business continuity and disaster recovery roles and responsibilities and provide refresher training at least annually.
- Periodically review and update the business continuity and disaster recovery plan.
- Rehearse and periodically test the business continuity and disaster recovery plan.
- Coordinate contingency plan rehearsal and testing with external organizations with (upstream or downstream) dependencies.
- Incorporate simulated events and automated mechanisms into business continuity and disaster recovery training to facilitate effective response and to provide more realistic training.
- If applicable, rehearse and test the business continuity and disaster recovery plan at any alternate site(s) to familiarize workforce members with the facility and available resources and to evaluate the site's capabilities to support contingency operations.

4.8 Information security technical architecture standards

Intention

The intention of this requirement is to establish documented quality and consistent practices to support the integration of business, institutional information, application, and technology requirements.

Clarification

The purpose of having technical architecture standards is to improve efficiency and reduce complexity in the development of technology solutions while ensuring that information security requirements are met and resources are used effectively. This enables organizations across the University to consistently and effectively deliver a diversity of services. Architecture standards can cover a range of technology

subjects including software, hardware, networks, applications, data, security, identity and access management, development, and project management. Architecture standards do not necessarily have to apply to all information systems, but should apply to systems that provide critical services to the organization, provide critical services to multiple organizations, or provide services on which other systems and services are dependent.

Architecture standards should improve the coordination, scheduling, and forecasting of development and implementation. They should simplify integration and enhance information sharing while reducing complexity, redundancy, and procurement costs. They should provide greater reliability, long-term sustainability, and consistent services. An important thing to remember when creating architecture standards is to consider the unintended consequences of the technology in question.

Examples

- Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security.
- Make available (to authorized personnel) adequate documentation for the information system.
- In addition to providing administrator and user guides, include documentation describing the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

4.9 System build and maintenance standards

Intention

The intention of this requirement is to establish quality and consistent practices to support the building and maintaining of reliable systems.

Clarification

It is important that solicitation documents (e.g., Request for Information, Request for Proposal) for information systems and services include the Data Security Agreement to ensure that vendors are aware of general University security requirements. They should also include any specific organizational security controls; design and development processes; test and evaluation procedures; and required documentation. Whenever possible, use tested, evaluated, and validated products, services, and vendors.

System baseline configuration documentation is an important part of system validation and should describe the final state the system at the time of release. Don't wait until after release to create this document. Include diagrams, screenshots, tables, and pictures as necessary. Make sure that the system owner and operator confirm the document matches the system. It is important to capture all the details of the initial configuration of the system so that it can be used for change management and system recovery. The document should allow someone to reproduce the last configuration of the system quickly, confidently, and with minimal disruption. System build standards and baseline configurations can also improve the ability to detect intrusions and to understand information security risks.

Baseline configuration documents may contain network interface configuration, disk partition scheme, installed software, a hardware inventory, authentication method, OS version, subsystems, users and groups, privileged accounts, daemons, file permissions, audit and logging settings, and a list of individuals responsible for system with contact information.

Examples

- Establish common technologies and practices for hardware, software, and system purchases, installs, and maintenance.
- Establish common baseline configurations for hardware, authorized software, and systems in order to meet organizational needs.
- Establish common maintenance processes and procedures.
- Develop, disseminate, and periodically review a system and services acquisition process that includes information security considerations and that addresses purpose, scope, roles and responsibilities, management commitment, and coordination details.
- Include the Data Security Agreement in information system acquisition contracts that involve UW Confidential and restricted data.
- In solicitation documents, require that appropriate documentation be provided describing the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

4.10 Acceptable use standards

Intention

The intention of this requirement is to establish and document appropriate and effective practices related to the use of institutional information, infrastructure technology, and information systems.

Clarification

Information assets are deployed to provide a set of capabilities. Security issues often arise when those assets are used in unintended or unanticipated ways. Acceptable use standards define the appropriate uses of information assets and the user's personal responsibility for the use of the asset. This includes complying with University policies, as well as applicable laws and regulations. Acceptable use standards should be based on the principle that information resources are provided to support the University's mission. They should give examples of what users can do and cannot do, and state what rights they have when they access University information resources.

Examples

- Develop and implement an organizational acceptable use standard that informs workforce members of their responsibilities related to information, infrastructure technology, and information systems. For an example, please see Appendix A.
- Implement a system use message before granting system access. The system use message remains on the screen until the user takes explicit actions to log on to the information system. For an example, please see Appendix A.

5 Technical Security and Access Controls

5.1 A remote access process

Intention

The intention of this requirement is to appropriately manage access to University assets located within a defined trust boundary from outside of that boundary.

Clarification

Section 5.5, Network, system, and application level protection measures, explains what a security boundary is and how to define one. In this context, remote access refers to the ability to access an organization's assets by an authorized user (or a process acting on behalf of a user) from a location outside of a defined trust boundary. Opening up remote access should be done with care. Remote

access services can be a useful tool for attackers to bypass firewalls and other boundary controls. Organizations need to evaluate their security capabilities and weigh the risk of whether or not they want to allow remote access. You should carefully consider who (or what) needs remote access and restrict remote access to certain users, user groups, times, or client configurations. Increasingly, Web-based access means that the need to remotely access another computer may not always be required.

When you are considering enabling remote access, think of security in several parts. There's the server allowing remote access, the network traffic between the server and the client, the authentication, and the client.

Examples

- Ensure that remote access to an asset is authorized prior to allowing the connection and document usage restrictions and allowed methods of remote access.
- Employ controls (e.g. VPN) to protect the confidentiality of remote access sessions.
- Route remote administrative access to a secure zone through a single managed access control point (e.g. bastion host).
- Monitor for unauthorized remote access and establish a means to rapidly disconnect remote users and disable further remote access.
- Disable insecure remote access methods and require strong authentication.
- Establish a means to control remote access sessions (e.g. session time-outs, limited access times).
- Authorize the execution of privileged commands via remote access only for compelling needs and document the rationale for such access in the security plan.
- Implement client side controls (e.g., remote wipe, whole disk encryption) to protect data at rest.

5.2 Cryptographic controls for protecting data

Intention

The intention of this requirement is to use cryptographic methods to reduce the likelihood that institutional information is read, modified, or otherwise utilized by an unauthorized individual.

Clarification

The confidentiality and integrity of UW Confidential and Restricted data should be protected using cryptographic controls. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Encrypting information prior to transmission protects from unauthorized disclosure. Creating cryptographic hashes can alert you that there has been an unauthorized modification of information. Digital certificates issued by a trusted third party allow servers to establish secure communications with other servers and services. Digital signatures help protect against an individual falsely denying having performed a particular action (non-repudiation).

Examples

- Encrypt transmissions from one secure area to another through the use of SSL or other industry acceptable methods to protect the confidentiality of data.
- Protect confidentiality of data at rest using mechanisms such as encryption and appropriate authentication methods.
- Where possible, implement full-device encryption and appropriate authentication methods to protect the confidentiality of data on mobile devices.
- Protect the integrity of data using mechanisms such as hashes or electronic signatures.
- Use digital signatures to protect against non-repudiation.
- Use signed hash functions to monitor the integrity of files.

5.3 An access authorization process for all users and information systems

Intention
The intention of this requirement is to manage who or what has access to an asset as well as the type of access that is permitted.

Clarification
The purpose of access authorization is to manage, control, and audit subjects' (users, systems, etc.) access to and use of information assets. It includes processes and technical controls for assigning, managing and revoking privileges (e.g. group memberships, system access, service subscriptions). Account and identity management is also required to implement access control (see section 9). Access control models (see below) and access enforcement mechanisms control access between subjects and assets. Since information systems can host many interfaces, access enforcement mechanisms can also be employed at the interface level.

An access control model should employ the principle of least privilege; meaning subjects are only granted the minimum access necessary to accomplish necessary tasks and functions. It should also employ the principle of separation of duties, reducing the potential for the abuse of authorized privileges by separating business functions and system functions, separating unique system functions (e.g., system administration, configuration management, development, quality assurance, and security), and ensuring that the people managing access control do not also perform audit functions. The access control model should be selected appropriately to protect assets based on their level of risk.

An access control process should document criteria for granting and revoking privileges, define responsibility for assigning, managing, and revoking privileges, and establish a clear access provisioning and de-provisioning process. It should clearly communicate the access being granted. It should also maintain accountability by limiting the use of shared credentials to only cases where alternate solutions are not technically feasible. When necessary alternate mitigating controls should be used to maintain accountability. The process should implement a safety net for removing access based on known institutional transitions (affiliation change, job change, etc.)

Organizations should choose, document, and implement a suitable access control model, some examples include:

- **Attribute-Based Access Control** – a rule set of attributes associated with subjects, objects, targets, initiators, resources, or the environment defines the conditions under which access may take place.
- **Discretionary Access Control** - restricts access to objects based on the identity of subjects or groups to which subjects belong. Subjects with certain privileges can pass those privileges on to other subjects.
- **Identity-Based Access Control** - access to objects is based on the identity of the user (or a process acting on behalf of a user).
- **Nondiscretionary Access Control** - restricts access to objects based on the identity of subjects or groups to which the subjects belong. Subjects with certain privileges cannot pass those privileges on to other subjects.
- **Role-Based Access Control** - permissions are based on defined functional roles. Permissions may be inherited.

The following UW-IT access management services are available for your consideration:

- **ASTRA** - Provides enterprise authority management and privilege management services; UW 'delegators' and 'authorizers' use the ASTRA Web site to manage the authority and assign authorizations; consuming applications use the ASTRA Web service to obtain the authorizations assigned to a specific user (UW NetID) or application.
- **UW Groups service** - Provides enterprise group management for access control, collaboration, and messaging; it supports groups usage throughout the UW by making it easier to identify, define, and reuse groups in many systems and applications; group memberships comprise UW NetIDs, federated IDs, DNS names, as well as other UW Group IDs.
- **UW Subscriptions (Uniform Access) service** - Provides access to many central UW computing services such as UW Email, Web Publishing, Odegaard Learning Commons, UW Libraries off-campus proxy; enables provisioning and de-provisioning of access based on UW NetIDs and university affiliations (e.g., student, employee, alumni); supports UW NetID service activation and deactivation of services.

Examples

- Document and implement an appropriate access control model for information assets.
- Build an automated safety net process that reviews users affiliations and determines whether they are still employed at the UW.
- Provide administrators that are both a user and an admin of a system with two separate accounts, a user account, and an administrative account and define appropriate uses for both.
- Create groups that represent specific roles. In applicable information systems grant the privileges associated with those roles to the groups. Then establish a process for adding, reviewing and removing individuals in those groups based on eligibility for those roles.
- Establish a periodic audit of access granted and revoked.
- Enforce a limit on embedding data types within other data types.
- Explicitly authorize access to security functions (e.g. creating system accounts, granting privileges) and security-relevant information (firewall rule sets, cryptographic keys) and require that users with that access use non-privileged accounts when accessing non-security functions.
- Periodically review account privileges to determine if those privileges are still valid.

5.4 An authentication mechanism for all authorized users and information systems

Intention

The intention of this requirement is to validate the identity of a user when they use an asset.

Clarification

Authentication is the process of verifying the identity and authenticity of a user, system, or process. Authentication involves verifying something the user knows (e.g., passwords, pins, security questions), something the user has (e.g., tokens, private keys), or something the user is (e.g., finger print, iris scan). For added assurance organizations often employ a combination solutions from these three categories to authenticate users.

Each authentication type has different potential strengths and weaknesses. For example, “something you know” can be stolen or forgotten, “something you have” can be stolen or lost, and “something you are” can be faked or changed.

Authentication credentials, whether they are the password, a token seed, or biometric information, must be treated as UW Confidential and protected accordingly.

When implementing password controls there are a number of key considerations:

- When passwords are issued it should be done in a way that confirms the identity of the individual. For example, if a one-time password or access code is used, that same code should not be used for more than one transaction.
- Passwords should be resistant to guessing attacks using complexity rules, length requirements, or controls that restrict the number of guesses based on the entropy of the password.
- Passwords should be stored in a secure manner, using industry standard hashing algorithms. If the password is stored in a reversible encryption strong controls should be put in place to restrict access to the decryption keys.
- Passwords and other authentication tokens should be encrypted during transmission over the network.
- Audit and education controls should be put in place address social engineering attacks such as phishing.
- Default passwords, often present in vendor systems or software must be changed.

When implementing system-to-system authentication some important considerations include:

- Use industry standard authentication mechanisms (e.g., x.509 Certificates, Oauth)
- Reset authentication secrets when there is staffing turnover among system operators that have access to those secrets.
- Establish processes for identifying and removing system's access when it is no longer needed or authorized.

The following UW-IT authentication services are available:

- **Kerberos** - Provides UW NetID authentication using the Kerberos network authentication system; also known as the "u.washington.edu" Kerberos realm.
- **Web Authentication Services** - Provides UW NetID authentication and single sign-on (SSO) to participating Web sites; provides a trusted Web site (weblogin.washington.edu) for entering and verification of user credentials; supports "federation" via InCommon and SAML protocols; software options include Pubcookie and Shibboleth (preferred) for Apache and Microsoft IIS Web servers.
- **Token Authentication Service** - Provides multi-factor authentication using Entrust tokens as a 2nd authentication factor for access to more sensitive UW applications.
- **UW Windows Infrastructure** - Provides an Active Directory forest for Kerberos and NTLM authentication for all UW NetIDs; also known as the "netid.washington.edu" Kerberos realm.

Examples

- Require that users and services authenticate using credentials to provide accountability.
- Use group, shared, or generic accounts and passwords only in special circumstances and with additional controls.
- Implement procedures to identify and assess suspicious behavior (e.g., accessing information that is not typically accessed, accessing more information than is routinely accessed, or accessing information from suspicious network addresses).
- Establish mechanisms (e.g. account lockout) to inhibit or slow password guessing.
- Ensure that default passwords are changed upon system installation.
- Protect authentication methods from unauthorized disclosure and modification.
- Establish minimum password entropy (length, complexity, unpredictability), minimum and maximum lifetime restrictions, and reuse conditions for passwords.

- Restrict access to privileged system functions.
- Obscure authentication error messages to protect from possible exploitation by unauthorized individuals.
- Employ multifactor authentication and replay-resistant authentication mechanisms for access to privileged accounts.
- Implement procedures for authenticator distribution, lost/compromised or damaged authenticators, and for revoking authenticators.
- Change authenticators for group accounts when membership changes.
- Require re-authentication or step up authentication to access more sensitive capabilities or data.

5.5 Network, system, and application level protection measures

Intention
The intention of this requirement is to implement layers of controls that reduce the likelihood that an attacker is able to compromise an asset or disrupt the organization.

Clarification
The boundaries between internal and external networks are disappearing as a result of increased interconnectivity and the huge growth in mobile technologies. Despite the loss of the perimeter, effective multi-layered defenses still include carefully configured boundaries segregating networks with different control needs. A security boundary can be defined as a set of systems that are under a single administrative control. Internal firewalls, Virtual Local Area Networks (VLAN), router Access Control Lists (ACL), proxies, and IDSs, can provide layers of separation and can hinder an attacker's progress and limit the damage they can do to only a section of the network.

An often-overlooked security control is the limitation of open network ports and services. Attackers constantly scan for accessible network services that are vulnerable to exploitation. Web servers, mail servers, file and print services, and domain name system (DNS) servers are sometimes installed and enabled automatically as part of a software package, often without the installer's knowledge. Sometimes obsolete or insecure services and protocols are still enabled on systems. It is a good practice to inventory your critical assets for available ports and services. If there is no business need for them, you should disable them. Consider completely uninstalling unnecessary software so that an attacker cannot restart these services.

Another good control layer to implement is to separate system management and user interfaces on critical assets. This could be a separate management VLAN or a physically out-of-band management interface. This also includes having separate user and administrative accounts.

In some cases, you may want to consider Information flow controls. These controls regulate information transfer within and between information systems. Flow enforcement occurs in boundary devices (e.g., gateways, routers, firewalls) that employ rules and provide a packet-filtering capability or content-filtering capability. Restrictions can include: keeping sensitive information from being transmitted in the clear, blocking external traffic that looks like it's internal, denying web requests that don't go through a proxy server, and limiting data transfers based on data structure and content.

Pay attention to data sharing relationships that cross trust boundaries. It is a good idea to document and periodically review publisher and consumer requirements. The CISO has created the Memorandum of

Understanding and System Description (internal), and the Data Sharing Agreement (external vendor or third party) to help manage these relationships.

Examples

- Define and establish appropriate security boundaries and layers of controls for information assets.
- Implement internal network segmentation (e.g., firewalls, VLANs, ACLs) based on business use and different control needs.
- Implement procedures to define and manage data sharing (see Section 11, Additional Information) between information assets across security boundaries.
- Ensure that critical assets provide only essential capabilities by disabling all unnecessary services and protocols and uninstalling unneeded software.
- Separate user and system management functionality on critical assets (e.g. separate out-of-band management interface).
- Manage critical assets using two-factor authentication and encrypted sessions.
- Implement host-based firewalls on end user systems when available.
- At network interconnection points (e.g., Internet gateways, inter-organization connections, and internal network segments), only allow those ports and protocols with a documented business need. All other ports and protocols should be blocked by default.

6 Monitoring Controls

6.1 A baseline measurement process for application, system, and network activity

Intention

The intention of this requirement is to understand what is normal activity in order to be able to identify what is abnormal activity.

Clarification

It is essential to establish a baseline of the expected behaviors of information systems, hosts, networks, and other critical assets to be able to monitor for abnormal behavior. Collect information that is measureable and relevant to the intended use of the asset. Keep in mind that what is normal for one asset may not be for another.

Examples

- Create a baseline of host events such as: services starting/stopping, ports opening/closing, files being accessed/created/deleted, and permissions successfully/unsuccessfully changed.
- Create a baseline of network events such as: traffic protocols, volume of traffic, timing of traffic, and traffic latency.

6.2 A monitoring capability for critical systems

Intention

The intention of this requirement is to detect disruptions, malicious activity, or anomalies to critical systems.

Clarification

Organizations should monitor critical assets to ensure that they are available and performing as intended. Baseline measurements can be used to determine if anomalous activity is taking place. In addition, file integrity checking can determine if files have been accessed or altered without permission.

As with many controls, alerts must be reviewed and assessed on a regular and timely basis to be effective.

Examples

- Implement a method to monitor and assess activity that varies from baseline measurements.
- Implement file integrity checking to monitor for content changes.

6.3 An intrusion detection mechanism

Intention

The intention of this requirement is to monitor and assess host and network traffic in order to identify attacks and take appropriate actions.

Clarification

Intrusion Detection/Prevention Systems (IDS/IPS) can detect attacks and in the case of IPS prevent some of them. Network IDS/IPS examine network traffic for known attack patterns or anomalies. These events can be alerted on or the traffic can be prevented from reaching its destination. Host based IDS/IPS examine events on a host and can similarly alert on or block actions. IDS/IPS are only as good as their signatures and their ability to handle the volume of traffic or events. Systems that rely on alerting only are only effective if they are monitored continuously. They should be considered as an additional layer of protection to a firewall, but they are by no means foolproof.

Examples

- Ensure that an intrusion detection/prevention system is deployed and maintained on hosts or the network and that alerts are continuously monitored and assessed.

6.4 Logging processes of networks, systems, and applications

Intention

The intention of this requirement is to capture information associated with network, system, and application activities in order to detect anomalies, address operational issues, and support incident response processes.

Clarification

A lack of adequate logging can allow attackers to hide their activities on compromised machines. Without complete logs and regular analysis of them, an attack may go unnoticed for months or years without anyone in the target organization knowing. Attackers rely on the fact that organizations rarely look at logs, so they don't know that their systems have been compromised. Sometimes logs are the only evidence of a successful attack. Detailed logs can also prove invaluable for responders, enabling them to determine exactly what happened when and if sensitive data was accessed or altered.

Examples

- Ensure that successful/unsuccessful login attempts are logged.
- Ensure that successful/unsuccessful service creation events are logged.
- Ensure that successful/unsuccessful attempts to access a resource (e.g., a file or directory) without the appropriate permissions are logged.
- Ensure that system clocks are synchronized to a central time source.
- Ensure that logs are in a standardized format and include such things as date, timestamp, source addresses, destination addresses, and other useful elements of each transaction.
- Ensure that logs are regularly reviewed and events, alerts, advisories, anomalies, etc. are assessed and addressed.

- Ensure that the actions associated with accounts can be uniquely traced so individuals can be held accountable for their actions.
- Ensure that system audit logs are created, protected, and retained to enable monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate activity.
- Ensure that logs are kept for a sufficient period of time and that systems have adequate storage space for the logs generated.
- Consider writing logs to a write-only device or a dedicated logging server so that an attacker cannot tamper with the logs.

7 Physical Controls

7.1 Physical protection and access processes for buildings that house critical information technology and systems

Intention
The intention of this requirement is to physically protect facilities that house critical information assets, to limit access to these areas, and to document these practices.

Clarification
It is important to consider physical security because one of the least technical methods of exploitation is to breach physical security. Without appropriate physical security other security measures may be ineffective. A physical perimeter can be established in many ways, such as: using locked doors that require an access code, cameras, motion detectors, magnetic card swipes, biometrics, and professional security guards. Better yet, use a combination of two or more of these. Don't forget to track access activity and ensure workforce members are properly trained to identify and report suspicious activity.

Examples
- Implement physical barriers and access authorization (e.g. locked door, turnstile, access card reader) at designated entry/exit points to facilities that contain information assets.
- Implement mechanisms to protect information assets against environmental hazards (e.g. Uninterruptable Power Supply, water sensors, smoke sensors).
- Implement mechanisms for timely monitoring of physical and environmental controls.
- Implement mechanisms that limit access to authorized individuals and that detect and record unauthorized access.
- Escort visitors and maintain visitor access logs.
- Monitor and regularly review access logs.
- Implement a security awareness program for all workforce members.
- Implement a security ID card for building access.
- Verify individual access authorization before granting access to the facility.
- Secure keys, combinations, and other physical access devices.
- Change combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.
- Document and test physical security processes and procedures including: purpose, scope, roles and responsibilities, and identification of designated areas.

7.2 A physical protection process for critical information systems and institutional information

Intention
The intention of this requirement is to safely store and protect media and devices containing University data from physical compromise, theft, or destruction.

Clarification
Information assets themselves may require physical protections in addition to the physical controls for the buildings that house them. For example, protections might include locked rooms within the facility, locked containers, and encrypted media or devices. Encryption can provide confidentiality and integrity protections depending upon the mechanisms used.

Examples
- Protect information assets with physical barrier(s) (e.g., locked container or room) when not under direct individual control.
- Implement additional physical access controls for areas where there is a concentration of information system components (e.g., server rooms, media storage areas, communications centers).
- Implement tamper detection/prevention mechanisms for hardware components.

8 Asset Identification Controls

8.1 A process to identify, inventory, assign ownership, and classify institutional information and information systems using the following information classification scheme:

- UW Public Information
- UW Restricted Information
- UW Confidential Information

Intention
The intention of this requirement is to understand what data is stored, processed, or transmitted by organizational assets so the assets can be managed effectively and securely.

Clarification
As part of the process of creating a Plan, organizations need to discover what information assets they possess. Then they can determine appropriate asset owners and document not only who they are but also what they are responsible for and where the asset is located. Classifying information assets will help determine what controls are appropriate for each asset.

Examples
- Establish a process to discover and classify University Data.
- Use the change control process to classify new assets and update the asset inventory.
- Make assigning ownership and updating the asset inventory a part of the procurement process.
- Use an automated discovery tool to find systems connected to the organization's network(s), and then assess those systems to determine the associated information.

9 Account and Identity Management Controls

9.1 Identity and eligibility verification and registration process

Intention
The intention of this requirement is to ensure users are who or what they say they are and that access is uniquely and appropriately assigned based on job duties or functions.

Clarification
Subjects (e.g. users, systems) must be properly vetted before being given access to critical systems and UW Confidential or Restricted data. This includes:

- An identity verification and registration process that accurately verifies and securely collects identifying information about eligible registrants.
- A process for verifying the user (e.g., photo ID, address of record) and clearly tying that user's information to information registered in the system.
- A process for initially issuing and reissuing credentials that assures that only that user has access to the credential.

UW-IT offers the UW NetID service to address this requirement.

Examples

- Establish accounts in a way that verifies the individual's full name, data of birth, and current address of record.
- Store a record of registration information and process followed to establish access.
- Verify that the individual looks like the same person on a government issued photo ID and establish that the information on that ID is correctly registered in the system.
- Establish mechanisms for verifying eligibility for an account.
- Use a unique onetime password or other mechanism for establishing a new password to guarantee only the user will know his or her password.

9.2 User and system account life cycle management process

Intention
The intention of this requirement is to ensure that the necessary account life cycle information is available and access is appropriately established, maintained and terminated based on job duties or function.

Clarification
A person, computer, or system may have many different roles during their time at the UW. The goal of this requirement is to manage and represent the information associated with the account to provide accurate and timely information for access control decisions. You will need a way to distinguish between different account types (e.g., personal, shared, administrative, etc.) and to define their appropriate use. You will also need to establish a mechanism for identifying major changes - such as job or affiliation changes and for re-evaluating an account's access. Finally, you will want to establish a process for identifying and canceling accounts that are no longer needed or used. See Section 5 for more information on creating access management controls.

Examples

- Establish defined account types (e.g. individual, group/shared, system, application, guest/anonymous, and temporary), expectations, and limitations for account use.
- Implement processes for creating, activating, modifying, disabling, and removing accounts.
- Review accounts on a regular basis to identify inactive or unknown accounts and disable any account that cannot be associated with an owner.

- Establish a process tied to institutional affiliation information that identifies when a workforce member leaves the UW.
- Only enable temporary accounts during the time needed.

10 Maintenance and Approval

The Privacy Assurance and Systems Security Council shall review and endorse this Information Security Guideline document at least every three years or more frequently as needed to respond to changes in the regulatory environment, prior to being sent for final approval by the University Chief Information Security Officer.

11 Additional Information

Controls in this document were derived after reviewing the laws and regulations that impart a duty on the UW and from industry best practices such as NIST SP 800-53 and PCI DSS.

For additional information see:

Privacy Assurance and Systems Security Council
Office of the University Chief Information Security Officer

For information on laws and regulations that apply to specific data see:
Information Security and Privacy Laws and Regulations

12 Appendix A

12.1 Example Acceptable Use Standard

Do:

- Use resources only for authorized purposes.
- Protect your NetID and password from unauthorized use.
- Access only information that is your own, that is publicly available, or to which you have been given authorized access.
- Use only legal versions of copyrighted software in compliance with vendor license requirements.
- Be considerate in your use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.

Do not:

- Use another person's system, NetID, password, files, or data without permission.
- Use computer programs to decode passwords or access control information.
- Attempt to circumvent or subvert system or network security measures.
- Engage in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files or making unauthorized modifications to University data.
- Use University systems for commercial or partisan political purposes, such as using electronic mail to circulate advertising for products or for political candidates.
- Make or use illegal copies of copyrighted materials or software, store such copies on university systems, or transmit them over university networks.
- Use mail or messaging services to harass or intimidate another person, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted mail, or by using someone else's name or NetID.
- Waste computing resources or network resources, for example, by intentionally placing a program in an endless loop, printing excessive amounts of paper, or by sending chain letters or unsolicited mass mailings.
- Use the University's systems or networks for personal gain; for example, by selling access to your NetID or to university systems or networks, or by performing work for profit with university resources in a manner not authorized by the university.
- Engage in any other activity that does not comply with the principles presented above.

Also see: UW-IT Access and Use Agreement.

12.2 Example System Use Message

You are accessing a University of Washington information system. System usage may be monitored, recorded, and subject to audit. Unauthorized use of this system is prohibited and subject to criminal and civil penalties. Use of this system indicates consent to monitoring and recording.