Published on *University of Colorado* (https://www.cu.edu)

System-wide Baseline Security Standards [1]

Download Document [2]

Table of Contents

        - 1.6.4 CP-8 Telecommunications Services
        - 1.6.5 CP-9 Information System Backup
        - 1.6.6 CP-10 Information System Recovery and Reconstruction
    - 1.7 Identification and Authetication
        - 1.7.1 IA-a Identification and Authentication Policy and Procedure
        - 1.7.2 IA-2 User Identification and Authetication (Organizational Users)
        - 1.7.3 IA-3 Device Identification and Authentication
        - 1.7.4 IA-5 Identifier Management
        - 1.7.5 IA-5 Autheticator Management
        - 1.7.6 IA-6 Authenticator Feedback
        - 1.7.7 IA-7 Cryptographic Module Authentication
        - 1.7.8 IA-8 Identification and Authentication (Non-Organizational Users)
    - 1.8 Incident Response
        - 1.8.1 IR-4 Incident Handling
        - 1.8.2 IR-5 Incident Monitoring
        - 1.8.3 IR-6 Incident Reporting
        - 1.8.4 IR-8 Incident Response Plan
    - 1.9 Maintenance
        - 1.9.1 MA-1 System Maintenance Policy and Procedures
        - 1.9.2 MA-4 Non-Local Maintenance
        - 1.9.3 MA-5 Maintenance Personnel
        - 1.9.4 MA-6 Timely Maintenance
    - 1.10 Media Protection
        - 1.10.1 MP-4 Media Storage
        - 1.10.2 MP-6 Media Sanitization
    - 1.11 Physical and Environmental Protection
        - 1.11.1 PE-2 Physical Access Authorizations
        - 1.11.3 PE-11 Emergency Power
        - 1.11.4 PE-13 Fire Protection
    - 1.12 Planning
        - 1.12.1 PL-2 System Security Plan
        - 1.12.2 PL-4 Rules of Behavio
    - 1.13 Personnel Security
        - 1.13.1 PS-1 Personnel Security Policy and Procedures
        - 1.13.2 PS-2 Position Categorization
        - 1.13.3 PS-3 Personnel Screening
        - 1.13.4 PS-4 Personnel Termination
        - 1.13.5 PS-7 Third-Party Personnel Security
    - 1.14 Risk Assessment
        - 1.14.1 RA-1 Risk Assessment Policy and Procedures
        - 1.14.2 RA-2 Security Categorization
        - 1.14.3 RA-3 Risk Assessment
        - 1.14.4 RA-5 Vulnerability Scanning
    - 1.15 System and Services Acquisition
        - 1.15.1 SA-1 System and Services Acquisition Policy and Procedures
        - 1.15.2 SA-2 Allocation of Resources
        - 1.15.3 SA-3 Life Cycle Support
        - 1.15.4 SA-4 Acquisitions
        - 1.15.5 SA-6 Software Usage Restrictions

1. Baseline Security Controls for Information Systems

1.1 Access Control

1.1.2 AC-3 Access Enforcement

Logical and technical controls are in place to control access. Access controls are implemented based on risk (e.g., additional controls in place for more sensitive information as determined by classification schemes).

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography must meet standards defined by the campus Information Security Principal.

The information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. Explicitly authorized personnel include, for example, security administrators, system and

network administrators, and other privileged users. Privileged users are individuals who have access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

1.1.3 AC-4 Information Flow Enforcement

The flow of sensitive information (as determined by classification schemes) between systems is controlled and/or monitored through technical (network firewalls, intrusion prevention, data loss prevention) means per business requirements.

The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few, of many, generalized examples of possible restrictions that are better expressed as flow control than access control are: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems.

Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability. Network access to campus resources is restricted based on business need. Authentication transactions (e.g., when authenticating system users) and security assertions (e.g., when validating system user identity for System applications) are encrypted in transmission using industry accepted cryptographic modules. Authentication systems employ controls to validate the identity of the authentication source. For example, trusted third party server certificates for SSL/TLS transactions or pre-shared keys of appropriate strength are used to sign security assertions.

1.1.4 AC-7 Unsuccessful Login Attempts

Technical controls implement account lock-out policy.

For the information system, a maximum of 5 invalid authentication attempts shall result in a minimum 5 minute delay before allowing additional authentication attempts.

Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization.

1.1.5 AC-11 Session Lock

The information system prevents further access to the application by initiating a session lock after following minutes of inactivity and retains the session lock until the user reestablishes access using established identification and authentication procedures.

For applications allowing access to private and restricted data – 30 minutes

The above times are the maximum allowable time periods when accessing data through applications such as portals. The campus IT Security Principal working with the necessary department may decide to reduce the time elapsed before the inactivity session lock is enabled.

The campus IT Security Principal working with the necessary department may decide to grant an exception to the lockout times if there are other compensating controls employed.

1.1.6 AC-19 Access Control for Mobile Devices

The organization establishes usage restrictions, configuration requirements, implementation guidance for connection of mobile devices to organizational information systems.

Usage restrictions and specific implementation guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, Bluetooth infrared).

1.2 Awareness and Training

1.2.1 AT-2 Security Awareness

Providing ongoing awareness information for employees.

1.2.2 AT-3 Role Based Security Training

Ensure that employees understand their responsibilities in protecting the organization information.

Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access. In addition, organizations provide enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined.

1.2.3 AT-4 Security Training Records

Mechanism is in place to track training requirements.

1.3 Audit and Accountability

1.3.1 AU-1 Audit and Accountability Policies and Procedures

The organization should develop an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and procedures to review the policy.

1.3.2 AU-3 Content of Audit Records

Ensure that information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results.

1.3.3 AU-4 Audit Storage Capacity

The organization allocates appropriate storage capacity for audit records.

Organizations should consider the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability.

1.3.4 AU-5 Response to Audit Processing Failures

Based on business requirement and risk assessment, the organization ensures that there is a process in place whereby information systems generate alerts to assigned personnel and take appropriate (preferably automated) actions in event of an audit processing failure.

Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

1.3.5 AU-6 Audit Review, Analysis, and Reporting

The organization reviews and analyzes information system audit records for indications of inappropriate, suspicious or unusual activity; and reports findings to defined personnel.

Audit review, analysis, and reporting covers information security-related auditing performed by organizations including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP. Findings can be reported to organizational entities that include, for example, incident response team, help desk, information security group/department.

1.3.6 AU-9 Protection of Audit Information

The organization should ensure that information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Audit information includes all information (e.g. Audit records, audit settings, and audit reports) needed to successfully audit information system activity.

1.4 Security Assessment and Authorization

1.4.1 CA-2 Security Assessments

Process is in place for reviewing system security.

1.4.2 CA-3 Information System Connections

Process in place for reviewing external network connections (ISP connections, VPN tunnels, DSL lines).

1.4.3 CA-6 Security Authorization

Ensure that information systems handling private date have clearly defined management authorizing official.

The organization authorizes the information system for processing before operations and updates the authorization periodically or when there is a significant change to the system. A senior organizational official approves the security review.

The organization assesses the security controls employed within the information system before and in support of the security accreditation. Security assessments conducted in support of security accreditations are called security certifications. The security accreditation of an information system is not a static process. Through the employment of a comprehensive continuous monitoring process (the fourth and final phase of the certification and accreditation process), the critical information contained in the accreditation package (i.e., the system security plan, the security assessment report, and the plan of action and milestones) is updated on an ongoing basis providing the authorizing official and the information system owner with an up-to-date status of the security state of the information system configuration Management.

1.5 Configuration Management

1.5.1 CM-2 Baseline Configuration

Baseline configuration documented, reviewed and regularly updated. The baseline configuration provides information about the components of an information system (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture.

1.5.2 CM-3 Configuration Change Control

Change control process should be in place, configuration repository should be updated and

configuration integrity should be reviewed periodically.

Configuration change controls for organizational information systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of information systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities. Typical processes for managing configuration changes to information systems include, for example, Configuration/Change Control Boards that approve proposed changes to systems. For new development information systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards. Auditing of changes includes activities before and after changes are made to organizational information systems and the auditing activities required to implement such changes.

1.5.3 CM-5 Access Restrictions for Change

Physical and logical access restrictions associated with changes to information systems are enforced.

Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access information systems for purposes of initiating changes, including upgrades and modifications. Organizations should maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls, workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover).

1.5.4 CM-6 Configuration Settings

Security related settings are addressed in baseline configuration; systems are monitored to ensure compliance.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security- related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security-related

parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific settings for information systems. The established settings become part of the systems configuration baseline.

Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements.

1.5.5 CM-7 Least Functionality

Provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services.

1.5.6 CM-8 Information System Component Inventory

Maintain inventory of systems including classification level & individuals with privileged access.

1.5.7 CM-11 User-Installed Software

The organization establishes policies governing the installation of software by users and enforces them. Policy is evaluated at least annually.

If provided the necessary privileges, users have the ability to install software in organizational information systems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved “app stores.” Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems).

1.6 Contingency Planning

1.6.1 CP-2 Contingency Plan

Identify essential missions and business functions and associated contingency requirements.

Ensure that the CP

- Provides recovery objectives, restoration priorities, addresses contingency roles, responsibilities, assigned individuals with contact information
- Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
- Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented.

1.6.2 CP-6 Alternate Storage Site

Based on business requirement and risk assessment, establish an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information for essential mission and business functions.

1.6.3 CP-7 Alternate Processing Site

Based on business requirement and risk assessment establish an alternate physically separate processing site including necessary agreements to permit the resumption of information systems operations for essential mission and business functions.

1.6.4 CP-8 Telecommunications Services

Based on business requirement and risk assessment, establish alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions.

1.6.5 CP-9 Information System Backup

Store offsite and local all critical backup media, documentation and other IT resources necessary for IT recovery and business continuity plans. Determine the content of backup storage in collaboration between business process owners and IT personnel.

1.6.6 CP-10 Information System Recovery and Reconstitution

Provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery and reconstitution procedures are based on organizational priorities, established recovery point/time and reconstitution objectives, and appropriate metrics

1.7 Identification and Authentication

1.7.1 IA-1 Identification and Authentication Policy and Procedure

The IT service providers shall develop, disseminate, and periodically review/update formal, documented procedures to facilitate the implementation of University policies and associated identification and authentication controls. The identification and authentication procedures must be consistent with applicable laws, regulations, directives, University APS, standards, and guidance.

1.7.2 IA-2 User Identification and Authentication (Organizational Users)

Ensure that all the organizational users are uniquely identified and authenticated by the information system.

The information system uniquely identifies and authenticates users (or processes acting on behalf of users).

Validating identity materials (i.e., a government issued photo ID) or information (e.g., legal name, address, date of birth, financial account number in conjunction with a validation process) are required when initially granting access to accounts that are granted access to system applications.

Provisioning and support processes ensure that individual system user account passwords are shared only with the system user.

Authentication systems implement controls to limit or prevent eavesdropper, replay, and on-line guessing attacks.

Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token.

Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

Support processes ensure that credentials are revoked within 72 hours after being notified that an account is no longer valid. In the event that an account is compromised support processes must immediately revoke credentials once notified.

Passwords have at least 24 bits of NIST defined min-entropy. For example, an 8 character password with complexity check would have 24 bits of min-entropy. NOTE: section 1.6.5 requiring 32 bits of min-entropy if periodic password changes are not enforced.

1.7.3 IA-3 Device Identification and Authentication

Ensure that the devices attaching to the campus networks are uniquely identified and logged.

1.7.4 IA-4 Identifier Management

Ensure that unique identifier exists for users that is provisioned appropriately and is not reused without permission.

IT service providers shall manage user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) issuing the user identifier to the intended party; (v) maintain current user affiliation. Identifier management is not applicable to shared information system accounts (e.g., guest and anonymous accounts).

1.7.5 IA-5 Authenticator Management

Ensure that authenticators such as passwords, tokens, etc. are appropriately assigned to users and devices. Ensure that default authenticators are never employed in production.

The IT service providers shall manage information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically or increase password strength to require 10 characters with multiple character classes or some other combination ensuring entropy to a min-entropy value of 32 or higher.

Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions or increase password entropy to a min-entropy value of 32 or higher; and (iv) prohibits password reuse for a specified number of generations.

1.7.6 IA-6 Authenticator Feedback

Ensure that the information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information.

1.7.7 IA-7 Cryptographic Module Authentication

Ensure that the information system implements mechanisms for authentication to a cryptographic module that meet the necessary requirements. Use FIPS 140-2 guidelines with at least security level 3 as described here http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf [3]

The information system authentication methods should use industry accepted cryptographic modules to protect the authentication transaction that meet the requirements of the campus IT Security Principal.

1.7.8 IA-8 Identification and Authentication (Non-Organizational Users)

Ensure that all the non-organizational users are uniquely identified and authenticated by the information system.

1.8 Incident Response

1.8.1 IR-4 Incident Handling

Ensure that the department implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery and coordinate the efforts with contingency plans.

1.8.2 IR-5 Incident Monitoring

Track and document information system security incidents.

1.8.3 IR-6 Incident Reporting

Ensure that suspected Information security incidents are reported to the designated authorities in a timely manner.

1.8.4 IR-8 Incident Response Plan

Ensure development and maintenance of Incident Response Plan that provides a roadmap for implementing the incident response capability and describes the structure and organization of the incident response capability.

1.9 Maintenance

1.9.1 MA-1 System Maintenance Policy and Procedures

The organization develops, disseminates, and reviews a formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.

1.9.2 MA-4 Non-Local Maintenance

Ensure that the organization authorizes monitors, and controls non-local maintenance and diagnostic activities and allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system. Non-local maintenance and diagnostic activities are those activities conducted by individuals communicating through a network; either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection.

1.9.3 MA-5 Maintenance Personnel

Establish a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel and ensure that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.

1.9.4 MA-6 Timely Maintenance

Ensure that mission critical systems and security-critical components including firewalls, guards, gateways, intrusion detection systems, audit repositories, authentication servers, and intrusion prevention systems have requisite maintenance support.

1.10 Media Protection

1.10.1 MP-4 Media Storage

Ensure that the organization protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

1.10.2 MP-6 Media Sanitization

Ensure that the organization sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse; and employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.

1.11 Physical and Environmental Protection

1.11.1 PE-2 Physical Access Authorizations

Ensure that the organization develops and keeps current a list of personnel with authorized access to the facility where the sensitive information system resides, issues authorization credentials, reviews and approves the access list and authorization credentials removing from the access list personnel no longer requiring access.

1.11.2 PE-3 Physical Access Control

Ensure that the organization enforces physical access authorizations for all physical access points to the facility where the sensitive information system resides, verifies individual access authorizations before granting access to the facility, controls entry to the facility containing the information system using physical access devices, secure and maintain keys, combinations, and other physical access devices.

1.11.3 PE-11 Emergency Power

Ensure that the organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

1.11.4 PE-13 Fire Protection

Ensure that the organization employs and maintains fire suppression and detection systems for the information system that are supported by an independent energy source.

1.12 Planning

1.12.1 PL-2 System Security Plan

Ensure that the organization develops a security plan for the information system that (Ensure that organization develops a security plan for the information system that (a) Defines at least logical and network boundaries for the system; (b) Describes the operational context of the information system in terms of missions and business processes; (c) Provides the security categorization of the information system including supporting rationale; (d) Describes the operational environment for the information system and relationships with or connections to other information systems; (e) Provides an overview of the security requirements for the system; (f) Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; (g) Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and (h) Protects the security plan from unauthorized disclosure and modification.

1.12.2 PL-4 Rules of Behavior

Ensure that the organization establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system. Personnel Security.

1.13 Personnel Security

1.13.1 PS-1 Personnel Security Policy and Procedures

Develop a formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

1.13.2 PS-2 Position Categorization

Assign a risk designation to all positions, establish screening criteria for individuals filling those positions and reviews and revise position risk designation.

1.13.3 PS-3 Personnel Screening

Ensure that employees are appropriately screened before getting authorization to information

systems and re-screenings are conducted when necessary.

1.13.4 PS-4 Personnel Termination

The organization upon termination of individual employment disables information system access, terminates/revokes any authenticators/credentials associated with the individual, and retrieves all security-related organizational information system-related property within 72 hours. The organization should retain access to organizational information and information systems formerly controlled by terminated individual.

Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, organizations consider disabling the information system accounts of individuals that are being terminated prior to the individuals being notified.

1.13.5 PS-7 Third-Party Personnel Security

Establish personnel security requirements including security roles and responsibilities for third-party providers and document personnel security requirements.

1.14 Risk Assessment

1.14.1 RA-1 Risk Assessment Policy and Procedures

Develop a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

1.14.2 RA-2 Security Categorization

Ensure that information and information systems are properly categorized according to the University policies and the categorizations are reviewed and approved by the appropriately defined authorities.

1.14.3 RA-3 Risk Assessment

Ensure that there is an assessment of risk including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits. Document results

and review the risk assessment when there is a major change in the environment.

1.14.4 RA-5 Vulnerability Scanning

Scan for vulnerabilities in the information system and hosted applications and when new vulnerabilities potentially affecting the system/applications are identified and reported; the scanning process be as automated as possible and the legitimate vulnerabilities should be mitigated. Review the vulnerabilities to assess for a larger threat to the environment.

1.15 System and Services Aquisition

1.15.1 SA-1 System and Services Acquisition Policy and Procedures

Based on business requirement and risk assessment, develop a formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

1.15.2 SA-2 Allocation of Resources

Include a determination of information security requirements for the information system in business process planning, determine, document, and allocate the resources required to protect the information system as part of the capital planning and investment control process; and establish a discrete line item for information security in organizational programming and budgeting documentation.

1.15.3 SA-3 Life Cycle Support

Manage the information system using a system development life cycle methodology that includes information security considerations. Define, document roles and responsibilities as well as identify individuals involved in system security during the SDLC.

1.15.4 SA-4 Acquisitions

Ensure that the acquisition documents for information systems, information system components, and information system services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation.

1.15.5 SA-6 Software Usage Restrictions

Ensure use of software and associated documentation in accordance with contract agreements and copyright laws.

1.15.6 SA-8 Security Engineering Principles

Based on business requirement and risk assessment, apply information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Apply security engineering principles primarily to new development information systems or systems undergoing major upgrades. For legacy systems, organizations apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. Security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are trained on how to build secure software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions.

1.15.7 SA-9 External Information System Services

Ensure that providers of external information system services comply with organizational information security requirements. Define and document oversight and user roles and responsibilities with regard to external information system services.

1.15.8 SA-10 Developer Configuration Management

Information system developers/integrators shall:

- Perform configuration management during information system design, development, implementation, and operation;
- Manage and control changes to the information system;
- Implement only organization-approved changes;
- Document approved changes to the information system; and
- Track security flaws and flaw resolution.

1.15.9 SA-11 Developer Security Testing

Information system developers/integrators, in consultation with the campus IT security principal shall:

- Create and implement a security test and evaluation plan;
- Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and
- Document the results of the security testing/evaluation and flaw remediation processes.

1.16 System and Communications Protection

1.16.1 SC-1 System and Communications Protection Policy and Procedures

Develop a documented policy for protection of data transfer and handling between systems that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and documented procedures to facilitate the implementation of the policy and associated controls.

SC-2 Application Partitioning

Ensure that information system separates user functionality (including user interface services) from information system management functionality by logical or physical means.

1.16.2 SC-3 Security Function Isolation

Ensure that the information system isolates security functions from non-security functions by means of an isolation boundary (implemented via partitions and domains) that controls access to and protects the integrity of, the hardware, software, and firmware that perform those security functions.

1.16.3 SC-7 Boundary Protection

The information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.

1.16.4 SC-8 Transmission Integrity and Confidentiality

Ensure that the information system protects the integrity and confidentiality of transmitted information.

This control applies to both internal and external networks and all types of information system

components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing physical distribution systems) or by logical means (e.g., employing encryption techniques). Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems.

1.16.5 SC-10 Session Disconnect

It is recommended that the information system terminate the network connection after an appropriate time intervals as decided by the ITSP.

The Campus IT Security Principal can grant exception to the above time restriction if there is a legitimate business need and/or appropriate compensating controls are in place.

1.16.6 SC-12 Cryptographic Key Establishment and Management

Ensure that the organization establishes and manages cryptographic keys for required cryptography employed within the information system.

1.16.7 SC-13 Use of Cryptography

Ensure the appropriate and correct use of cryptography in the organization.

1.16.8 SC-23 Session Authenticity

Based on risk assessment and business requirements, ensure that the information system provides mechanisms to protect the authenticity of communications sessions.

This control addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions. Few examples of approaching this control implementation include generation of unique system generated random session identifiers for each session, invalidation of session identifiers upon user logout or other session termination.

1.17 System and Information Integrity

1.17.1 SI-1 System and Information Integrity Policy and Procedures

Ensure that the organization develops, disseminates, and reviews a formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and documented procedures to facilitate the implementation of the policy and associated integrity controls.

1.17.2 SI-2 Flaw Remediation

Ensure that the organization identifies, reports, and corrects information system flaws. Also, ensure that flaw remediation is a part of the information system configuration management process

Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified.

1.17.3 SI-3 Malicious Code Protection

Ensure that the organization addresses malicious code protection mechanisms at information system entry and/or exit points and at workstations and servers, and when available mobile computing devices on the network to detect and eradicate malicious code. Ensure that the systems are updated with the latest anti-virus signatures.

1.17.4 SI-4 Information System Monitoring

Based on business requirement and risk assessment, ensure that the organization monitors events on the information system and detects information system attacks. Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system (e.g., within internal organizational networks and system components).

1.17.5 SI-5 Security Alerts, Advisories, and Directives

Ensure that the organization: receives information system security alerts, advisories, and directives from designated external and internal sources on an ongoing basis.

1.17.6 SI-7 Software, Firmware and Information Integrity

Groups audience:
Office of Information Security
Sub Title:
Baseline Security Controls for Information Systems

Source URL:https://www.cu.edu/security/system-wide-baseline-security-standards

Links
[1] https://www.cu.edu/security/system-wide-baseline-security-standards
[2] https://www.cu.edu/system/files/pages/243138-system-wide-baseline-security-standards/docs/baseline-security-standard.doc [3] http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf