Highly-Confidential & Highly Critical System Information Security Standard [1]

Update

The University of Colorado is in the process of transitioning from this multicampus standard for high risk IT systems to newer, campus-specific standards. Each campus has a separate process and timeline for this transition, so please contact your campus information security teams for current information on the applicable standards for your work.

Summary

It is the responsibility of IT service providers and IT staff to implement systems in accordance with university security standards. The standards described in this document apply to all IT services which maintain or process highly-confidential data or can be considered as highly critical based on the University of Colorado Process for Data Classification and System Security Categorization. These standards supplement, not supersede, the University Baseline Security Standards.

Download Document [2]

Table of Contents

        - 1.3.6 AU-10 Non Repudiation
        - 1.3.7 AU-12 Audit Generation
    - 1.4 Security Assessment and Authorization
        - 1.4.1 CA-2 Security Assessment
        - 1.4.2 CA-8 Penetration Testing
        - 1.4.3 CA-7 Continuous Monitoring
    - 1.5 Configuration Management
        - 1.5.1 CM-2 Baseline Configuration
        - 1.5.2 CM-3 Configuration Change Control
        - 1.5.3 CM-5 Access Restrictions for Change
        - 1.5.4 CM-6 Configuration Settings
        - 1.5.5 CM-7 Least Functionality
        - 1.5.6 CM-8 Information System Component Inventory
    - 1.6 Contingency Planning
        - 1.6.1 CP-2 Contingency Plan
        - 1.6.2 CP-4 Contingency Plan Testing
        - 1.6.3 CP-6 Alternate Storage Site
        - 1.6.4 CP-7 Alternate Processing Site
        - 1.6.5 CP-8 Telecommunications Services
        - 1.6.6 CP-10 Information System Recovery and Reconstitution
    - 1.7 Identification and Authentication
        - 1.7.1 IA-2 User Identification and Authentication (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
    - 1.9 Maintenance
        - 1.9.1 MA-4 Non-Local Maintenance
    - 1.10 Media Protection
        - 1.10.1 MP-4 Media Transport
        - 1.10.2 MP-7 Media Use
    - 1.11 Physical and Environmental Protection
        - 1.11.1 PE-13 Location of Information System Components
    - 1.12 Planning
        - 1.12.1 PL-2 System Security Plan
    - 1.13 Personnel Security
        - 1.13.1 PS-4 Personnel Termination
    - 1.14 Risk Assessment
        - 1.14.1 RA-5 Vulnerability Scanning
    - 1.15 System and Services Acquisition
        - 1.15.1 SA-4 Acquisitions
        - 1.15.2 SA-15 Development Process, Standards, and Tools
        - 1.15.3 SA-17 Developer Security Architecture and Design
    - 1.16 System and Communications Protection
        - 1.16.1 SC-7 Boundary Protection
        - 1.16.2 SC-8 Transmission Confidentiality
    - 1.17 System and Information Integrity
        - 1.17.1 SI-3 Malicious Code Protection

1. High Impact Baseline Security Controls for Information Systems

It is the responsibility of IT service providers and IT staff to implement systems in accordance with university security standards. The standards described in this document apply to all IT services which maintain or process highly-confidential data or can be considered as highly critical based on the University of Colorado Process for Data Classification and System Security Categorization[1 [3]]. These standards supplement, not supersede, the University Baseline Security Standards[2 [4]].

Highly Confidential Data

Data elements that require protection under laws, regulations, contracts, relevant legal agreements and/or require the institution to provide notification of unauthorized disclosure/security incidents to affected individuals, government agencies or media.

This information that is only for the “eyes of the authorized individuals” in any form including paper or electronic. This information is prohibited from being (1) transmitted or stored without encryption. (2) Handled on networks or systems without appropriate firewall, monitoring, logging, patching, anti-malware and related security controls.

The following are the most common examples of data types under the “Highly Confidential” information category:

- Protected Health Information
- Social Security Numbers
- Payment Card Numbers
- Financial Account Numbers; including University account numbers, student account numbers, and Faculty and Staff Direct Deposit account numbers
- Driver’s License numbers
- Health Insurance Policy ID Numbers
- Level 4 and 5 of Student data (SSN, NID, Financial Aid (except work study), Loan and Bank Account Numbers, Health Information, Disability, Race, Ethnicity, Citizenship, Legal Presence, Visas, Religion)

Highly Critical Service

An IT service or system is considered highly critical when potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (1) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (2) result in major damage to organizational assets; (3) result in major financial loss;

or (4) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

CU uses the following as guides for defining impact:

- Financial – direct or indirect monetary costs to the institution where liability must be transferred to an organization which is external to the campus, as the institution is unable to incur the assessed high end of the cost for the risk; this would include for e.g. Use of an insurance carrier
- Reputation – when the impact results in negative press coverage and/or major political pressure on institutional reputation on a national or international scale
- Safety – when the impact places campus community members at imminent risk for injury
- Legal – when the impact results in significant legal and/or regulatory compliance action against the institution or business.
- Strategic – is in direct support of campus or university leadership strategic plans.

1.1 Access Control

1.1.1 AC-2 Account Management Additional Controls

Employ automated mechanisms to support the management of information system accounts. Examples of automated mechanisms include but are not limited to: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information system to monitor account usage; and using telephonic notification to report atypical system account usage.

The information system automatically disables temporary and emergency accounts after a predefined period of time as specified by the campus information security officer.

The information system automatically disables inactive accounts after predefined period of time as specified by the campus information security officer.

The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and provides notifications as specified by the campus information security officer.

Users posing a significant risk to organizations include individuals for whom reliable evidence or intelligence indicates either the intention to use authorized access to information systems to cause harm or through whom adversaries will cause harm. Harm includes potential adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation. Close coordination between authorizing officials, information system administrators, and human resource managers is essential in order for timely execution of this control enhancement.

1.1.2 AC-6 Least Privilege

The IT Service Provider employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk. Access to privileged accounts must be granted based on a valid business need per guidance from the campus information security officer.

The information system audits the execution of privileged functions to detect misuse. Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT).

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

1.1.3 AC-11 Session Lock

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image. Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey sensitive information.

1.1.4 AC-17 Remote Access

The campus information security officer (ISO) shall establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and authorize remote access to the information system prior to allowing such connections.

The information system monitors and controls remote access methods. Automated monitoring and control of remote access sessions allows organizations to detect cyber attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of information system components (e.g., servers, workstations, notebook computers, smart phones, and tablets).

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. The encryption strength of mechanism is selected based on the security categorization of the information.

The information system routes all remote accesses through managed network access control points as determined by the campus information security officer. Limiting the number of access control points for remote accesses reduces the attack surface for organizations.

Execution of privileged commands and access to security-relevant information from networks not controlled by the university requires additional controls determined by the campus information security officer. Examples include, but not limited to, are: IP based restrictions, VPN, or multi-factor authentication.

1.1.5 AC-19 Access Control for Mobile Devices

The IT Service Provider employs encryption methods approved by the campus information security officer to protect the confidentiality and integrity of information on university owned mobile devices.

1.1.6 AC-20 Use of External Information Systems

The campus ISO establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

1. access the information system from external information systems; and
2. process, store, or transmit organization-controlled information using external information systems.

This control enhancement recognizes that there are circumstances where individuals using external information systems (e.g., contractors, coalition partners) need to access organizational information systems. In those situations, organizations need confidence that the external information systems contain the necessary security safeguards (i.e., security controls), so as not to compromise, damage, or otherwise harm organizational information systems. Verification that the required security controls have been implemented can be achieved, for example, by third-party, independent assessments, attestations, or other means, depending on the confidence level required by organizations.

The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled

information only when the campus information security officer verifies the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan or approves information system connection or processing agreements with the organizational entity hosting the external information system.

1.2 Awareness and Training

1.2.1 AT-2 Security Awareness

Employees of units responsible for processing, managing, or protecting highly confidential data will complete additional security awareness training to recognizing and reporting potential indicators of insider threat. Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of organizational policies, procedures, directives, rules, or practices. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures.

1.3 Audit and Accountability

1.3.1 AU-2 Audit Events

Over time, the events that organizations believe should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient. The IT service provider reviews and updates the audited events per guidance from the campus ISO.

1.3.2 AU-2 Content of Audit Records

The campus ISO shall determine required content generated by information system audit records Examples of detailed information that organizations may consider in audit records includes, but not limited to, full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest.

The IT service provider employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

1.3.3 AU-6 Audit Review, Analysis, and Reporting

The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

The information system provides the capability to process audit records for events of interest based on guidance from the campus ISO. Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed. Organizations may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or subnetwork) or selectable by specific information system component.

1.3.4 AU-8 Time Stamps

The information system synchronizes with an authoritative time source as determined by the campus ISO.

1.3.5 AU-9 Protection of Audit Records

The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Individuals with privileged access to an information system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records. The campus ISO will further defined privileged access between audit-related privileges and other privileges, thus limiting the users with audit-related privileges.

1.3.6 AU-10 Non Repudiation

The campus ISO shall promulgate expectations for specific actions for which an information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed. The campus information security officer shall approve implementation plans for this control.

Examples of Types of individual actions covered by non-repudiation include, for example, creating information, sending and receiving messages, approving information (e.g., indicating concurrence or signing a contract). Non-repudiation protects individuals against later claims

by: (i) authors of not having authored particular documents; (ii) senders of not having transmitted messages; (iii) receivers of not having received messages; or (iv) signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from a particular individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Organizations obtain non-repudiation services by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts).

1.3.7 AU-12 Audit Generation

Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerances.

1.4 Security Assessment and Authorization

1.4.1 CA-2 Security Assessment

The campus ISO assess the security controls in the information system and its environment of operation annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

The campus ISO develops and implements a security assessment plan that describes the scope of the assessment including:

- security controls and control enhancements under assessment;
- assessment procedures to be used to determine security control effectiveness;
- assessment environment, assessment team, and assessment roles and responsibilities;
- requirements for independent or specialized assessors for a given system;
- produces a security assessment report that documents the results of the assessment; and
- provides the results of the security control assessment to the campus CIO/CTO, CISO and appropriate Data Custodian.

Guidance - Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of

independence based on the security categories of information systems and/or the ultimate risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk-based decisions. This includes determining whether contracted security assessment services have sufficient independence, for example, when information system owners are not directly involved in contracting processes or cannot unduly influence the impartiality of assessors conducting assessments. In special situations, for example, when organizations that own the information systems are small or organizational structures require that assessments are conducted by individuals that are in the developmental, operational, or management chain of system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Organizations recognize that assessments performed for purposes other than direct support to authorization decisions are, when performed by assessors with sufficient independence, more likely to be useable for such decisions, thereby reducing the need to repeat assessments.

Specialized assessments may employ information system monitoring, insider threat assessments, malicious user testing, and other forms of testing (e.g., verification and validation) to improve readiness by exercising organizational capabilities and indicating current performance levels as a means of focusing actions to improve security. Assessment activities must be conducted in accordance with applicable federal laws, Colorado revised statutes, policies, regulations, and standards. Authorizing officials approve the assessment methods in coordination with the organizational risk executive function.

1.4.2 CA-8 Penetration Testing

Penetration testing is conducted at minimum every 3 years for high-impact or highly-confidential systems. The campus ISO shall establish expectations for penetration testing.

Guidance: Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills). Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber attacks against organizations and provides a more in-depth analysis of security-related weaknesses/deficiencies. Organizations can also use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the hardware, software, or firmware components of an information system and can exercise both physical and technical security controls. A standard method for penetration testing includes, for example: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before the commencement of penetration testing scenarios. Organizations correlate the penetration testing rules of engagement with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. Organizational risk assessments guide

decisions on the level of independence required for personnel conducting penetration testing.

Testing can also include red team exercises. Red team exercises extend the objectives of penetration testing by examining the security posture of organizations and their ability to implement effective cyber defenses. As such, red team exercises reflect simulated adversarial attempts to compromise organizational mission/business functions and provide a comprehensive assessment of the security state of information systems and organizations. Simulated adversarial attempts to compromise organizational missions/business functions and the information systems that support those missions/functions may include technology-focused attacks (e.g., interactions with hardware, software, or firmware components and/or mission/business processes) and social engineering-based attacks (e.g., interactions via email, telephone, shoulder surfing, or personal conversations). While penetration testing may be largely laboratory-based testing, organizations use red team exercises to provide more comprehensive assessments that reflect real-world conditions. Red team exercises can be used to improve security awareness and training and to assess levels of security control effectiveness.

1.4.3 CA-7 Continuous Monitoring

In collaboration with the campus ISO, IT Service Providers shall create continuous monitoring strategy and implement a continuous monitoring program that includes:

- Establishment of metrics to be monitored;
- Establishment of frequencies for monitoring and assessments supporting such monitoring;
- Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
- Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
- Correlation and analysis of security-related information generated by assessments and monitoring; and
- Response actions to address results of the analysis of security-related information.

1.5 Configuration Management

1.5.2 CM-3 Configuration Change Control

The IT Service Providers test, validate, and document changes to information systems before implementing the changes on the operational system.

IT Service Providers establish dedicated test environments for highly-critical systems to ensure that testing does not interfere with information system operations. Individuals/groups conducting tests understand organizational security policies and procedures, information system security policies and procedures, and the specific health, safety, and environmental risks associated with particular facilities/processes

1.5.3 CM-5 Access Restrictions for Change

IT Service Providers reviews information system changes to determine whether unauthorized changes have occurred based on guidance from the campus ISO.

1.5.4 CM-6 Configuration Settings

IT Service Providers employ automated mechanisms to centrally manage, apply, and verify configuration settings for highly-confidential data systems.

IT Service Providers implement campus ISO approved mechanisms to respond to unauthorized changes. Responses to unauthorized changes to configuration settings can include, for example, alerting designated organizational personnel, restoring established configuration settings, or in extreme cases, halting affected information system processing.

1.5.5 CM-7 Least Functionality

IT Service Providers reviews the information system quarterly to identify and disable unnecessary and/or non-secure functions, ports, protocols, and services. IT Service Providers should seek guidance from the campus ISO regarding the relative security of the function, port, protocol, and/or service. Bluetooth, FTP, and peer-to-peer networking are examples of less than secure protocols.

1.5.6 CM-8 Information System Component Inventory

IT service providers update the inventory of information system components as an integral part of component installations, removals, and information system updates.

IT service providers employ automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

IT service providers maintain information system inventories to the extent feasible. Virtual machines, for example, can be difficult to monitor because such machines are not visible to the network when not in use. In such cases, organizations maintain as up-to-date, complete, and accurate an inventory as is deemed reasonable.

1.6 Contigency Planning

1.6.1 CP-2 Contingency Plan

IT service providers coordinate contingency plan development with organizational elements responsible for related plans. Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.

IT service providers identify and report critical information system assets supporting essential missions and business functions following campus ISO guidance. Critical information system assets include technical and operational aspects. Technical aspects include, for example, information technology services, information system components, information technology products, and mechanisms. Operational aspects include, for example, procedures (manually executed operations) and personnel (individuals operating technical safeguards and/or executing manual procedures).

1.6.2 CP-4 Contingency Plan Testing

IT Service Providers test, review, and adjust the contingency plan for highly critical information systems determine the effectiveness of the plan and the organizational readiness to execute the plan. Plans should be tested annually.

IT service providers coordinate contingency plan testing with organizational elements responsible for related plans. Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. This control enhancement does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. It does require, however, that if such organizational elements are responsible for related plans, organizations should coordinate with those elements.

1.6.3 CP-6 Alternate Storage Site

IT service providers implement an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats as the primary site.

1.6.4 CP-7 Alternate Processing Site

IT service providers implement an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats as the primary site.

1.6.5 CP-8 Telecommunications Services

The campus develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and

The campus considers the potential mission/business impact in situations where telecommunications service providers are servicing other organizations with similar priority-of-service provisions.

The campus alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

1.6.6 CP-10 Information System Recovery and Reconstitution

The information system implements transaction recovery for systems that are transaction-based. Transaction-based information systems include, for example, database management systems and transaction processing systems. Mechanisms supporting transaction recovery include, for example, transaction rollback and transaction journaling.

1.7 Identification and Authentication

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

The information system implements multifactor authentication for network access to privileged accounts.

The information system implements multifactor authentication for network access to non-privileged accounts.

The information system implements multifactor authentication for local access to privileged accounts.

The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.

For remote access to privileged/non-privileged accounts, the purpose of requiring a device that is separate from the information system gaining access for one of the factors during multifactor authentication is to reduce the likelihood of compromising authentication credentials stored on the system. For example, adversaries deploying malicious code on organizational information systems can potentially compromise such credentials resident on the system and subsequently impersonate authorized users.

The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets requirements set by the campus ISO.

1.8 Incident Response

1.8.1 IR-4 Incident Handling

Campus ISO employs automated mechanisms to support the incident handling process. Automated mechanisms supporting incident handling processes include, for example, online incident management systems.

1.8.2 IR-5 Incident Monitoring

The IT Service Provider, in collaboration with the campus ISO, employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

1.8.3 IR-6 Incident Reporting

The IT Service Provider employs automated mechanisms to assist in the reporting of security incidents to the campus ISO.

1.9 Maintenance

1.9.1 MA-4 Non-Local Maintenance

The IT Service Provider documents in the security plan for the information system, the policies

and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

1.10 Media Protection

1.10.1 MP-4 Media Transport

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

1.10.2 MP-7 Media Use

The campus prohibits the use of portable storage devices in organizations maintaining highly confidential data or with highly critical information systems when such devices are not from verified trusted source or cannot be sanitized prior to use. The campus ISO shall include guidance as part of security awareness and training information for appropriate units.

1.11 Physical and Environmental Protection

1.11.1 PE-13 Location of Information System Components

Ensure that the IT service provider conducts a risk assessment to determine appropriate location of information system components to mitigate potential physical and environmental hazards. Examples of physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, acts of terrorism, or vandalism. In addition, organizations consider the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to information systems and therefore increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones).

1.12 Planning

1.12.1 PL-2 System Security Plan

The campus ISO will coordinate security-related activities affecting the information system with IT Service Providers before conducting such activities in order to reduce the impact on other organizational entities. Security-related activities include, for example, security assessments, audits, hardware and software maintenance, patch management, and contingency plan testing. Advance planning and coordination includes emergency and

nonemergency (i.e., planned or non-urgent unplanned) situations. The process defined by organizations to plan and coordinate security-related activities can be included in security plans for information systems or other documents, as appropriate.

1.13 Personnel Security

1.13.1 PS-4 Personnel Termination

The IT Service Provider or human resources staff provides notification to the campus ISO for individuals to privileged access to highly confidential data or highly critical systems. Whenever feasible within a minimum 24 hours in advance of the termination of employees with privileged access.

1.14 Risk Assessment

1.14.1 RA-5 Vulnerability Scanning

The campus ISO employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned. The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible.

The campus ISO updates the vulnerability scanning system weekly or when new high risk vulnerabilities are identified and reported. IT service providers shall provide credentials for authenticated scanning when requested.

By default, the system will implement privileged access vulnerability scanning. In certain situations, the nature of the vulnerability scanning may be more intrusive or the information system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning. The information system implements privileged access authorization to the information system for authenticated scanning.

1.15 System and Services Aquisition

1.15.1 SA-4 Acquisitions

Functional properties of security controls describe the functionality (i.e., security capability,

functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls. The IT Service Provider requires the developer or vendor of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

The IT Service Provider requires the developer or vendor of the information system, system component, or information system service to:

- provide a description of the functional properties of the security controls to be employed
- design and implementation information for the security controls to be employed that includes:
    - security-relevant external system interfaces
    - high-level design
    - low-level design
    - source code
    - hardware schematics
- identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

1.15.2 SA-15 Development Process, Standards, and Tools

Information system developers/integrators, in consultation with the campus information security officer shall:

1. Requires the developer of the information system, system component, or information system service to follow a documented development process that:
    1. Explicitly addresses security requirements;
    2. Identifies the standards and tools used in the development process;
    3. Documents the specific tool options and tool configurations used in the development process; and
    4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and
2. Reviews the development process, standards, tools, and tool options/configurations every two years to determine if the process, standards, tools, and tool options/configurations selected and employed are sufficient to address security throughout the lifecycle of a system.

Development tools include, for example, programming languages and computer-aided design (CAD) systems. Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes enables accurate supply chain risk assessment and mitigation, and requires robust configuration control throughout the life cycle (including design, development, transport, delivery, integration, and maintenance) to track authorized changes and prevent unauthorized changes.

Processes should:

1. The organization requires the developer of the information system, system component, or information system service to implement an explicit process to continuously improve the development process.
2. Define quality metrics at the beginning of the development process and review metrics with the objective of identifying areas of improvement.
3. Business criticality and data sensitivity are used to determine security requirements throughout the system development life cycle.
4. Information system development teams select and deploy security tracking tools, including, for example, vulnerability/work item tracking systems that facilitate assignment, sorting, filtering, and tracking of completed work items or tasks associated with system development processes.
5. Perform threat modeling and a vulnerability analysis for the information system that. Developers should seek guidance from the campus information security officer regarding organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels.
6. Perform automated vulnerability analysis to detect and remediate vulnerabilities.
7. Maintain a knowledge base of threat and vulnerability analysis information for future reuse.
8. The appropriate data owner approves, documents, and controls the use of live data in development and test environments for the information system, system component, or information system service.

1.15.3 SA-17 Developer Security Architecture and Design

The developer of the information system, system component, or information system service to produce a design specification and security architecture that:

1. Is consistent with and supportive of the organization’s security architecture which is established within and is an integrated part of the organization’s enterprise architecture;
2. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and
3. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

1.16 System and Communications Protection

1.16.1 SC-7 Boundary Protection

Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic. The IT Service Provider limits the

number of external network connections to the information system.

The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

The campus:

- Implements a managed interface for each external telecommunication service;
- Establishes a traffic flow policy for each managed interface;
- Protects the confidentiality and integrity of the information being transmitted across each interface;
- Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
- Reviews exceptions to the traffic flow policy annually and removes exceptions that are no longer supported by an explicit mission/business need.

Network traffic to highly-confidential data networks will implement a deny by default, allow by exception, network control. Both inbound and outbound restrictions will be evaluated based on risk. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

VPN systems allowing remote access to highly-confidential data networks will prevent the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks. The control is typically implemented by preventing split-tunneling.

1.16.2 SC-8 Transmission Confidentiality

The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission over untrusted networks. Encrypting information for transmission protects information from unauthorized disclosure and modification.

1.17 System and Information Integrity

1.17.1 SI-3 Malicious Code Protection

Central management is the organization-wide management and implementation of malicious code protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw malicious code protection security controls. The campus IT department centrally manages the malicious code protection mechanisms.

Malicious code protection mechanisms include, for example, signature definitions. Due to

information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates. The information system automatically updates malicious code protection mechanisms.

1.17.2 SI-4 Information System Monitoring

The IT Service Provider employs automated tools to support near real-time analysis of events. Automated tools include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools or Security Information and Event Management (SIEM) technologies that provide real time analysis of alerts and/or notifications generated by organizational information systems.

Unusual/unauthorized activities or conditions related to information system inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code within organizational information systems or propagating among system components, the unauthorized exporting of information, or signaling to external information systems. Evidence of malicious code is used to identify potentially compromised information systems or information system components. The information system monitors inbound and outbound communications traffic for unusual or unauthorized activities or conditions.

The information system alerts the campus ISO, or designee, of indications of compromise or potential compromise occur. The campus ISO will promulgate requirements and processes for alert notification. Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging.

1.17.3 SI-7 Software, Firmware and Information Integrity

The information system will perform an integrity check of high risk software, when security-relevant events occur as determined by the campus ISO. Security-relevant events examples include, but are not limited to, for example, the identification of a new threat to which organizational information systems are susceptible, and the installation of new hardware, software, or firmware.

Following requirements from the campus ISO, the IT Service Provider incorporates the detection of unauthorized events into the organizational incident response capability. Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of information system privileges. Maintaining historical records is important both for being able to identify and discern adversary actions over an extended period of time and for possible legal actions

2. Responsibility Matrix

Attachments:

responsibility-matrx-raci-05042021.pdf [5]
Groups audience:
Office of Information Security
Right Sidebar:
Information Security Campus Contact

Source URL:https://www.cu.edu/security/highly-confidential-highly-critical-system-information-security-standard

Links
[1] https://www.cu.edu/security/highly-confidential-highly-critical-system-information-security-standard
[2] https://www.cu.edu/system/files/pages/243142-highly-confidential-highly-critical-system-information-security-standard/docs/highimpact-security-standardsdoc.doc
[3] https://www.cu.edu/system/files/pages/243142-highly-confidential-highly-critical-system-information-security-standard/docs/cudataclassification.docx [4] https://www.cu.edu/system/files/pages/243142-highly-confidential-highly-critical-system-information-security-standard/docs/baseline-security-standard.doc
[5] https://www.cu.edu/doc/responsibility-matrx-raci-05042021pdf