Commonwealth of Kentucky
Office of the Chief Information Officer
Enterprise Controls

ENT-201:
Enterprise Security Controls and Best Practices

Office of the Chief Information Security Officer
Commonwealth Office of Technology
500 Mero St
Frankfort KY 40601

Version 5.1
3/18/2025

Document Revision History			
Version	**Date**	**Change Description / Notes**	**Author/Editor**
1.0	2/28/2019	Document creation; incorporated AC controls family.	John Barnes
2.0	7/30/2019	Added Security Planning (PL) family.	John Barnes
3.0	9/3/2019	Added CP, MA, PE, PS, SA, SC and SI families.	John Barnes
3.1	9/16/2019	Updated title page to reflect new naming/format conventions.	Tom Walters
3.2	10/18/2019	Added Audit and Accountability (AU) family.	John Barnes
3.2.1	10/25/2019	Added content to AC-17 – Remote Access (lead section), #2.	John Barnes
3.3	11/7/2019	Added AT and CA families.	John Barnes
3.4	2/25/2020	Added Identification and Authentication (IA) family.	John Barnes
3.5	6/25/2020	Added Configuration Management (CM) family.	Tom Walters
4.0	2/17/2022	Added NIST 800-53 Rev 4.0 Security Baselining Moderate Controls	CC Webber
4.1	2/17/2023	Formatting Standardization and Omitted version 4.0 Notes	Tracy Burgess
5.0	3/11/2024	Revised to reflect NIST 800-53 Rev.5 Moderate Controls & added Supply Chain (SR) family	Karen Chrisman
5.1	3/18/2025	Added AC-2 (11) Account Management | Usage Conditions	Tracy Burgess

Contents

Definitions and Acronyms (document-wide)

CISO: Chief Information Security Officer
COT: Commonwealth Office of Technology
DBA: Database Administrator
FIPS: Federal Information Processing Standard Publication, specifically **FIPS 140-2**, the U.S. government computer security standard used to approve cryptographic modules.
NIST: National Institute of Standards and Technology (U.S. Department of Commerce)
NIST Special Publication 800-53 Rev 5: NIST Special Publication 800-53 (Rev 5), *Security and Privacy Controls for Federal Information Systems and Organizations*. This document provides an online cross-reference between Control Families and Security Controls ranked as Low-Impact, Moderate Impact, and High-Impact.
Service Provider: An outsourced or third-party vendor that provides IT services to the organization.

Note: "Outsourced" is relative to COT or the agency. Since we leverage the Information Technology Infrastructure Library (ITIL) framework, there are three types of service providers:

- *Type I = Internal service provider*
- *Type II = Shared service provider*
- *Type III = External service provider.*

SSP: System Security Plan

Note: Other definitions and acronyms specific to individual controls are provided within their sections.

Purpose of this Document

This document details the security controls that COT's Office of the CISO requires for information systems and activities for the Commonwealth of Kentucky. COT aligned the Commonwealth's security program with the framework outlined in the NIST Special Publication 800-53 (Rev 5), *Security and Privacy Controls for Federal Information Systems and Organizations*. COT established the Commonwealth's security framework using the *moderate-level* controls outlined in the NIST publication. Specifically, the Commonwealth's security program addresses the following families in NIST:

AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment and Authentication
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PM	Program Management (no moderate impact controls for this family)
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity
SR	Supply Chain Risk Management

Applicability

The security controls outlined in this document apply to all systems under the authority of the Commonwealth of Kentucky. These controls reference the appropriate policies and require the same compliance as the originating policy. As COT continues to update and develop policies, this document will continue to reflect those changes with the addition and modification of these security controls.

Commonwealth agencies, users, and associated entities such as vendors shall adhere to the most current, published version of the policies and their associated controls in this document. Each version of this document supersedes the previous ones. COT recommends reviewing this document for changes at least annually, or when managing systems for significant changes. Review the most up-to-date official Commonwealth of Kentucky Enterprise IT Policies.

CIO-072 IT Access Control and User Access Management

The security controls outlined in this section support the Commonwealth of Kentucky's **CIO-072 IT Access Control and User Access Management Policy** and require the same compliance as the originating policy. The Office of the CISO may update these controls to ensure the Commonwealth addresses effective security and risk management practices.

These moderate-level controls address the **Access Control (AC) family** as identified in the NIST Special Publication 800-53 Rev 5. They cover all executive and non-executive branch agencies using COT-managed infrastructure or services. Agencies, employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the CISO approves exceptions or mitigating controls.

Information Owners and Service Managers shall follow FedRAMP standards for all cloud services obtained where sensitive or confidential Commonwealth information is transmitted, stored, or processed on non-Commonwealth operated systems. FedRAMP or StateRAMP certification is required when the classification of data ore regulatory compliance requires enhanced security.

For requirements on security training, refer to Information Security - Awareness and Training Procedures. For requirements on personnel matters such as termination or transfer, refer to Personnel procedures.

Account Management Controls

The following section contains COT-directed controls for account management in Commonwealth systems. Where possible and as necessary, system owners, information owners, and service managers should coordinate to ensure that agencies and service providers understand and adhere to these controls.

AC-2 – Account Management

Agencies and service providers shall:

1. Define and document the types of accounts allowed and specifically prohibited for use within the system.
2. Assign account managers according to CIO-085 Authorized Agency Contacts.
3. Require agency-defined prerequisites and criteria for group and role membership.
4. Specify:
    a. Authorized users of the system;
    b. Group and role membership; and
    c. Access authorizations (i.e., privileges) and agency-defined attributes, as required, for each account.
5. Require approvals by authorized agency contacts for requests to create accounts.
6. Create, enable, modify, disable, and delete system accounts in accordance with AC2 controls.
7. Monitor the use of accounts.
8. Notify account managers and COT within 24 hours when:
    a. Accounts are no longer required;

b. Users are terminated or transferred; and
c. Individual system usage or need-to-know changes.

10. Authorize access to the system based on:
    a. A valid access authorization;
    b. Intended system usage; and
    c. Agency-defined attributes (as required).
11. Review accounts for compliance with account management requirements annually for user accounts and semi-annually for privileged accounts.
    a. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group.
12. Align account management processes with personnel termination and transfer processes.

AC-2 (1) – Account Management | Automated System Account Management

Agencies shall ensure service providers employ automated mechanisms to support the management of system accounts. Examples of automated mechanisms include, but are not limited to, email, Active Directory tools, IT identity access management systems, and functions that facilitate these automated mechanisms.

AC-2 (2) – Account Management | Automated Temporary and Emergency Account Management

Agencies shall ensure service providers automatically disable temporary and emergency accounts immediately and delete the disabled accounts after a total of 120 days.

AC-2 (3) – Account Management | Disable Accounts

Agencies shall ensure service providers disable accounts immediately when the accounts:

1. Have expired.
2. Are no longer associated with a user or individual.
3. Are in violation of organization policy.
4. Have been inactive for 90 days.

AC-2 (4) – Account Management | Automated Audit Actions

Agencies shall ensure service providers configure automated system auditing of account creations, modifications, enabling, disabling, and removal actions.

AC-2 (5) – Account Management | Inactivity Logout

Agencies shall ensure service providers require that users log out in accordance with risk tolerance established by the agency.

AC-2 (11) – Account Management | Usage Conditions

Agencies and service providers shall enforce account login restrictions preventing offshore access.

AC-2 (13) – Account Management | Disable Accounts for High-Risk Individuals

Agencies shall ensure service providers disable accounts of individuals immediately upon discovery of indicated or potential account compromise or suspicious activity.

AC-3 – Access Enforcement

Agencies shall ensure service providers:

1. Configure and enforce approved authorizations for logical access to systems.
2. Implement encryption as an access control mechanism if required by federal, state, or other regulatory requirements.
3. Document, audit, and monitor approved explicit overrides of automated access controls in the associated SSP; the SSP shall include a description of the override process to include authorization and termination of the override, and temporary compensating controls for auditing and monitoring.
4. Coordinate with applicable common control providers, for systems or applications that are normally used to support emergency operations such as emergency response for natural or human initiated disasters.
5. Prevent access to security functions or security services in a manner that could result in a failure to enforce system security policies and maintain the isolation of code and data.

AC-4 – Information Flow Enforcement

Agencies shall ensure service providers:

1. For sensitive and confidential data, enforce the following for the system:
    a. Data flow controls within the systems and between interconnected systems *(Note: This will be regulated where information is allowed to travel within a system and between systems)*;
    b. Data flow controls across security domains; and
    c. Separate data flows logically and physically using, for example, agency approved data containers, logical partitions, or physical hard drives.
2. Implement controls and requirements delineated in the Executive Branch Agencies Information Security Architecture or SSP as required.
3. Coordinate with the Agency or Chief Enterprise Architect (CEA, if applicable) and Senior Agency IT Executive Director or Director to develop and maintain the Agency Information Security Architecture.

AC-5 – Separation of Duties

Agencies shall ensure service providers:

1. Establish and maintain separation of duties within and among various IT functions and positions to meet the following minimum requirements:
    a. An individual shall not perform any combination of functions that could result in a conflict of interest, fraud, or abuse related to financial transactions. Examples include but are not limited to the following:
        i. check issuance and input of vendor invoices,
        ii. entering and authorizing a purchase order, and
        iii. funds transfer and accounts payable input.
    b. An individual shall not perform any combination of IT account management and/or data manipulation functions that could jeopardize data confidentiality, integrity, or availability. Examples include but are not limited to the following:
        i. an individual requesting and then creating a user account in the system,

ii. a system administrator conducting audits or reviews of a system he or she is administering,
iii. the Information Security Officer (ISO) acting as a system administrator,
iv. data collection and preparation, and
v. data input, approval, and verification.

c. An individual in a Database Administrator (DBA) capacity shall not exceed the minimum level of privileges necessary to create, edit, and delete rights over the database-specific files in the system directory. Additionally, the DBA shall not have directory level rights to operating system level directories. *(Note: The DBA shall have all rights over the database management system (DBMS) directory and its subdirectories)*;

d. Minimize potential abuse of authorized privileges and the risk of malevolent activity without collusion;

e. Same person may not perform audit functions and administer system access, maintenance, or implementation to include security functions; and

f. Any individual responsible for programming a function, application, etc. may not be the same individual that reviews and approves the programming code for implementation.

2. Document separation of duties of individuals and related business functions and processes.
3. Define and maintain system access authorizations in support of separation of duties.
4. Divide system testing and production functions between different individuals and/or groups.
5. Facilitate independent third-party information security testing of systems.

AC-6 – Least Privilege

Agencies shall ensure service providers:

1. Employ 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 mission, application, and business functions.
2. Explicitly authorize access to specific security functions and relevant security-related information.
3. Configure systems to prevent non-privileged accounts from having access to security settings or logging/auditing settings or controls.
4. Prevent non-privileged users from executing privileged functions to include disabling, circumventing, or otherwise altering established security safeguards and countermeasures.

AC-6 (1) – Least Privilege | Authorize Access to Security Functions

Agencies shall ensure service providers explicitly authorize all security functions to particular individuals or roles. Examples of ***functions*** include but are not limited to:

1. Establishing system accounts.
2. Configuring access authorizations (i.e., permissions, privileges).
3. Setting events to be audited.
4. Establishing intrusion detection parameters.
5. Performing system integrity checks.
6. Administering cryptographic keys.
7. Filtering rules for routers or firewalls, configuration parameters for security services.

Examples of ***roles*** include but are not limited to:

1. Security administrators.
2. System and network administrator.
3. System security officers.
4. System maintenance personnel.
5. System programmers.
6. Other privileged users.

AC-6 (2) – Least Privilege | Non-Privileged Access for Non-Security Functions

Agencies shall ensure service providers require users of system accounts or roles with access to security functions or security relevant information use non-privileged accounts when accessing non-security functions.

AC-6 (5) – Least Privilege | Privileged Accounts

Agencies shall ensure service providers restrict privileged accounts on the system administrators, security administrators, system assurance groups, security groups, or other personnel or roles with approved justification.

AC-6 (7) – Least Privilege | Review of User Privileges

Agencies shall ensure service providers:

1. Review, in accordance with risk tolerance established by the agency, the privileges assigned to agency-defined roles or classes of users to validate the need for such privileges.
2. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

AC-6 (9) – Least Privilege | Auditing Use of Privileged Functions

Agencies shall ensure service providers:

1. Configure the system to audit the execution of privileged functions.
2. Audit the execution of privileged functions and authorized accounts for the following at a minimum:
    a. For the use of privileged or non-privileged functions; and
    b. When adding accounts to a privileged group.

AC-6 (10) – Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions

Agencies shall ensure service providers prevent non-privileged users from executing privileged functions. Privileged functions include:

1. Disabling, circumventing, or altering implemented security or privacy controls.
2. Establishing system accounts.
3. Performing system integrity checks.
4. Administering cryptographic keys.

AC-7 – Unsuccessful Logon Attempts

Note: *This control applies to all accesses other than those explicitly identified and documented in AC-14, and regardless of whether the login occurs via a local or network connection.*

Agencies shall ensure service providers:

1. Configure privileged and non-privileged user accounts such that they will lock after three (3) invalid logon attempts and must remain locked for a period of no less than 120 minutes or until an authorized user requests the account unlocked by contacting appropriate authorized system account administrators.
2. Permit non-privileged account users to unlock their respective account via self-service prior to the 120 minutes lock out period if productivity is hindered.
3. Prohibit privileged account users from unlocking their respective account via self-service prior to the 120 minutes lock out period; activation of these accounts shall require administrator activation.

AC-8 – System Use Notifications

For ***non-public*** systems, agencies shall ensure service providers configure the system to display a system use notification message, before granting access, that outlines the following:

1. Only authorized users may access the system,
2. Users who access the system beyond the warning page represent that they are authorized to do so.
3. Unauthorized system use or abuse is prohibited and subject to criminal prosecution.
4. System use may be monitored and logged and that use of the system indicates consent to such logging and monitoring.
5. Users are using a Kentucky state government system.
6. Any other specific language as required by state or federal regulations.

For ***public*** systems, agencies shall ensure service providers configure the system to display a system use notification message before granting system access that outlines:

1. Unauthorized system use or abuse is prohibited and subject to criminal prosecution.
2. System use may be monitored and logged, and the use of the system indicates consent to such logging and monitoring.
3. Description of the authorized uses of the system.

Agencies shall ensure service providers:

1. Display the system use notification message on the screen until the user takes explicit actions to logon or further access the system.
2. Configure network security, routing, and monitoring devices to display a system use notification banner before granting access for all administrative and maintenance access.
3. Provide appropriate privacy and security notices and disclosures in the system notification message or banner. These notices shall:
    a. Be consistent with applicable state law, federal law, Executive Orders, directives, policies, regulations, standards, and guidelines;
    b. Contain a link to Commonwealth Privacy and Security notices; and
    c. Be compliant with the Children's Online Privacy Protection Act (COPPA); the standard Children's Privacy Policy shall appear on, or be linked from, all Commonwealth publicly accessible systems (i.e., web sites) aimed at children aged 13 and under.

AC-11 – Device Lock

Agencies shall ensure:

1. Service providers configure the system to initiate a device lock after a maximum of 15 minutes of inactivity.
2. Devices will remain locked until the user re-establishes access using established identification and authentication procedures.
3. Users are not to use the device lock control as a substitute for logging out of a system,
4. Staff are responsible for maintaining the security of their assigned workstation and must lock unattended workstations.
5. Workstations automatically lock or invoke a password-protected screensaver after a maximum of ten (10) minutes of inactivity.

AC-11 (1) – Session Lock | Pattern-Hiding Displays

Agencies shall ensure service providers configure the system to conceal information previously visible on the display with a publicly viewable image or blank screen.

AC-12 – Session Termination

Agencies shall ensure service providers configure the system to terminate a user session automatically after defined conditions or trigger events requiring session disconnect. Conditions or trigger events requiring automatic session termination can include, for example:

1. Agency-defined periods of user inactivity.
2. Targeted responses to certain types of incidents.
3. Time-of-day restrictions on system use.

Note: This requirement addresses the termination of user-initiated logical sessions (for local, network, and remote access), which are initiated when a user—or process acting on behalf of a user—accesses a Commonwealth system.

AC-14 – Permitted Actions without Identification or Authentication

This control addresses instances where an agency determines that no identification and authentication is required. It does not, however, mandate that such instances exist in a given system.

For situations where agencies determine not to require identification and authentication, agencies shall ensure service providers:

1. Identify and document specific user actions allowed on the system without identification and authentication.
2. Document the supporting rationale for not requiring identification and authentication.
3. Define conditions for bypassing identification and authentication mechanisms to facilitate operations in emergency situations.

AC-17 – Remote Access

Agencies shall ensure service providers:

1. Document all allowed methods for each type of remote access (e.g., dial-up, broadband, wireless).
2. Establish and document usage restrictions and implementation guidance for each type of remote access method allowed:

a. Personal devices are not permitted on the state network, either directly or via directly connected VPN services such as IPsec VPN. SSL VPN connections are permitted; and
b. Vendor access will be provided through virtual endpoints such as SSL VPN, or Citrix. When direct network IP connectivity is required remotely, it will be provided through approved VPN connections.

3. Authorize remote access to the system prior to connection.
4. Implement adequate security measures (e.g., virus and spam protection, firewall, intrusion detection) on client computers prior to allowing remote or adequately protected VPN access.
5. Configure endpoint protection systems to prohibit "dual-homed" connections (e.g., a laptop shall not be permitted to connect to a Commonwealth system via a wired/VPN connection while using a separate wired or wireless connection to an external, non-Commonwealth system).

AC-17 (1) – Remote Access | Monitoring and Control

Agencies shall ensure service providers:

1. Configure the system to employ automated mechanisms for the monitoring and control of remote access methods.
2. Audit user activity to ensure compliance with established remote access policy.

AC-17 (2) – Remote Access | Protection of Confidentiality/Integrity using Encryption

Agencies shall ensure service providers:

1. Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
2. Base the encryption strength on the security categorization of the information and in compliance with FIPS 140-2.

AC-17 (3) – Remote Access | Managed Access Control Points

Agencies shall ensure service providers:

1. Route connections traversing the Internet through Commonwealth Trust Internet Connection (TIC) technologies.
2. Prohibit remote access utilities such as, but not limited to, Team Viewer or LogMeIn.

AC-17 (4) – Remote Access | Privileged Commands/Access

Agencies shall ensure service providers:

1. Allow the execution of privileged commands and access to security relevant information via remote access only for compelling operational needs and when rationale for such access is documented in the SSP.
2. Document the rationale for remote access in the security plan for the system.

AC-18 – Wireless Access

COT shall:

1. Develop configuration and connection requirements, and implementation guidance for each type of wireless access in Commonwealth executive branch agencies and non-executive branch agencies.

2. Authorize each type of wireless access to Commonwealth systems prior to allowing such connections.

Agencies shall ensure service providers:

1. Obtain authorization from the CISO for non-public wireless use prior to implementation.
2. Implement and enforce COT-developed restrictions and configuration and connection requirements prior to using non-public wireless connections to Commonwealth systems.
3. Monitor Commonwealth systems continuously for unauthorized wireless connections.
4. Configure endpoint protection systems to prohibit "dual-homed" connections (e.g., a laptop shall not be permitted to connect to a Commonwealth system via a wired/VPN connection while using a separate wired or wireless connection to an external, non-Commonwealth system).

AC-18 (1) – Wireless Access | Authentication and Encryption

Agencies shall ensure service providers:

1. Authenticate users and devices on the wireless system.
2. Implement FIPS 140-2 compliant cryptographic protections for the integrity and confidentiality of information transmitted on the non-public wireless system.

AC-18 (3) – Wireless Access | Disable Wireless Networking

Agencies shall ensure service providers disable embedded wireless networking capabilities within system components prior to issuance and deployment when the agency does not intend to use those capabilities.

AC-18 (5) – Wireless Access | Antennas / Transmission Power Levels

Agencies shall ensure service providers deploy wireless antennas in a manner that limits wireless communications outside of Commonwealth-controlled boundaries.

AC-19 – Access Control for Mobile Devices

Agencies shall ensure service providers adhere to the requirements in CIO-071, Wireless Voice and Data Services Policy.

AC-19 (5) – Access Control for Mobile Devices | Full Device/Container-Based Encryption

Agencies shall ensure service providers:

1. Deploy enterprise solutions for mobile device management (MDM) and full-disk encryption on all Commonwealth to include when such devices are outside of controlled areas. Mobile computing devices include laptops, tablets, smart phones, and similar devices.
2. Use FIPS 140-2-compliant encryption mechanisms to protect information storage areas on mobile storage devices such as USB drives, tapes, CDs, and DVD's.

AC-20 – Use of External Systems

Agencies shall ensure service providers establish terms and conditions with organizations owning, operating, and/or maintaining external systems.

1. Agencies and service providers shall allow authorized individuals to:
    a. Access to the system from external systems, and;

b. Process, store, or transmit agency-controlled information using external systems.

2. Prohibit the use of agency-defined types of external systems.

AC-20 (1) – Use of External Systems | Limits On Authorized Use

Agencies shall ensure service providers permit authorized individuals to use an external system to access the Commonwealth system or to process, store, or transmit organization-controlled information, only after:

1. Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plan.
2. Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

AC-20 (2) – Use of External Systems | Portable Storage Devices

Agencies will restrict the use of agency-controlled portable storage devices by authorized individuals on external systems.

AC-21 – Information Sharing

Agencies shall ensure service providers:

1. Determine whether access authorizations assigned to information users (i.e., external partners, employees, contractors, vendors, etc.) match the access and use restrictions on all sensitive but unclassified information (e.g., privileged medical information, contract-sensitive information, and proprietary information).
2. Assist users in making appropriate information sharing decisions with such information by developing mechanisms or processes to assist users in making appropriate sharing decisions and training personnel on the mechanisms or processes.

AC-22 – Publicly Accessible Content

Agencies shall:

1. Designate and authorize individuals to post information in the public domain as outlined in CIO-061 Social Media Policy.
2. Train designated individuals to ensure that publicly accessible information does not contain non-public information.
3. Review proposed content to ensure non-public information is excluded prior to posting the information in the public domain.
4. Review content at a frequency commensurate with the frequency that information is posted and that the personnel conducting these reviews should be different than those posting or conducting the reviews prior to posting (separation of duties).

IT Access Control and User Access Management Best Practices

(This space reserved for best practices)

CIO-090 Incident Response

The security controls outlined in this section support the Commonwealth of Kentucky's **CIO-090 Incident Response Policy** and require the same compliance as the originating policy. The Office of the Chief Information Security Officer (CISO) may update these controls to ensure the Commonwealth addresses effective security and risk management practices.

These moderate-level controls address the Incident Response (IR) family identified in the NIST Special Publication 800-53 Rev 5. They cover all executive and non-executive branch agencies using COT-managed infrastructure or services. Agencies, employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the CISO approves exceptions or mitigating controls.

Incident Response Controls

The following section contains COT-directed controls for incident response for Commonwealth systems. It details the measures agencies shall implement to ensure the applicable incident response controls are in place. Where possible and as necessary, system owners, information owners, and service managers should coordinate to ensure that agencies and service providers understand and adhere to these controls.

IR-2 – Incident Response Training

COT and agencies shall:

1. Provide incident response training to system users consistent with assigned roles and responsibilities:
    a. Annually, assuming an incident response role or responsibility or acquiring system access;
    b. When required by system changes; and
    c. When necessary, thereafter.
2. Review and update incident response training content quarterly and following incident response changes.

IR-3 – Incident Response Testing

COT and agencies shall test the effectiveness of the incident response capability for the system at least annually or when there is a significant change to the system using tests such as disaster recovery or tabletop tests.

IR-3(2) – Incident Response Testing | Coordination with Related Plans

COT and agencies shall coordinate incident response testing with organizational elements responsible for related plans.

IR-4 – Incident Handling

COT and agencies shall:

1. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.
2. Coordinate incident handling activities with contingency planning activities.
3. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting charges accordingly.
   Employ automated mechanisms to support the incident handling process.
4. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

IR-4(1) – Incident Handling | Automated Incident Handling Process

COT and agencies shall support the incident handling process using Incident Response Plan and Procedures.

IR-5 – Incident Monitoring

Agencies shall track and document security incidents.

IR-6 – Incident Reporting

Agencies shall:

1. Require personnel to report suspected incidents to the organizational incident response team immediately.
2. Report incident information in accordance with the Agency Incident Response Manual.

IR-6(1) – Incident Reporting | Automated Reporting

Agencies shall report incidents in accordance with the Agency Incident Response Manual.

IR-6(3) – Incident Reporting | Supply Chain Coordination

Agencies shall report system vulnerabilities associated with reported incidents in accordance with the Agency Incident Response Manual.

IR-7 – Incident Response Assistance

Agencies shall provide an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the system for the handling and reporting of incidents.

IR-7(1) – Incident Response Assistance

Agencies shall increase the availability of incident response information and support using Enterprise Monitoring and Response Solutions.

IR-8 – Incident Response Plan

Agencies shall:

1. Develop an incident response plan that:
   a. Provides the organization with a roadmap for implementing its incident response capability;
   b. Describes the structure and organization of the incident response capability;

c. Provides a high-level approach for how the incident response capability fits into the overall organization;
d. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
e. Defines reportable incidents;
f. Provides metrics for measuring the incident response capability within the organization;
g. Defines the resources and management support needed to effectively maintain and mature an incident response capability;
h. Addresses the sharing of incident information;
i. Is reviewed and approved by executive leadership and other key agency-designated personnel and is reviewed on an agency-defined schedule; and
j. Explicitly designates responsibility for incident response to OCISI.

2. Distribute copies of the incident response plan to key agency-defined stakeholders.
3. Reviews the incident response plan on an agency-defined schedule.
4. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing.
5. Communicate incident response plan changes to key agency-defined personnel.
6. Protect the incident response plan for unauthorized disclosure and modification.

Incident Response Best Practices

(This space reserved for best practices)

CIO-092 Media Protection

The security controls outlined in this section support the Commonwealth of Kentucky's **CIO-092 Media Protection Policy** and require the same compliance as the originating policy. The Office of the Chief Information Security Officer (CISO) may update these controls to ensure the Commonwealth addresses effective security and risk management practices.

These moderate-level controls address the Media Protection (MP) family identified in the NIST Special Publication 800-53 Rev 5. They cover all executive and non-executive branch agencies using COT-managed infrastructure or services. Agencies, employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the CISO approves exceptions or mitigating controls.

Media Protection Controls

The following section contains COT-directed controls for media protection for Commonwealth systems. It details the measures agencies shall implement to ensure the applicable media protection controls are in place. Where possible and as necessary, system owners, information owners, and service managers should coordinate to ensure that agencies and service providers understand and adhere to these controls.

MP-2 – Media Access

COT and agencies shall restrict access to sensitive, confidential, and/or private digital and non-digital media to approved users with a business need to know in order to fulfill the functions of their job.

MP-3 – Media Marking

COT and agencies shall:

1. Mark system media indicating distribution limitations, handling caveats, and applicable security markings of the information in accordance with regulatory requirements.
2. Exempt certain types of system media from marking if said media remains within a physically controlled environment.

MP-4 – Media Storage

COT and agencies shall:

1. Physically control and securely store digital and non-digital media in a manner that ensures that the media cannot be accessed by unauthorized individuals. This may require storing media in locked containers such as cabinets, drawers, rooms, or similar locations if unauthorized individuals have unescorted access to areas where sensitive information/media is stored.
2. Protect system media until said media is destroyed or sanitized using approved equipment, techniques, and procedures.

MP-5 – Media Transport

COT and agencies shall:

1. Protect and control media during transport outside of controlled areas using agency-defined security safeguards.
2. Maintains accountability for system media during transport outside of controlled areas.
3. Document activities associated with transport of system media.
4. Restrict activities associated with transport of such media be fulfilled by authorized personnel.

MP-6 – Media Sanitization

COT and agencies shall:

1. Sanitize agency-defined system media prior to disposal, release out of organizational control, or release for reuse using agency-defined sanitization techniques and procedures.
2. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

MP-7 – Media Use

COT and agencies shall:

1. Restrict or prohibit the use of agency-defined system media on agency-defined systems or system components using agency-defined controls.
2. Prohibit the use of portable media storage devices on systems when such devices have no identifiable owner.

Media Protection Best Practices

(This space reserved for best practices)

CIO-093 Risk Assessment

The security controls outlined in this section support the Commonwealth of Kentucky's **CIO-093 Risk Assessment Policy** and require the same compliance as the originating policy. The Office of the Chief Information Security Officer (CISO) may update these controls to ensure the Commonwealth addresses effective security and risk management practices.

These moderate-level controls address the Risk Assessment (RA) family identified in the NIST Special Publication 800-53 Rev 5. They cover all executive and non-executive branch agencies using COT-managed infrastructure or services. Agencies, employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the CISO approves exceptions or mitigating controls.

Risk Assessment Controls

The following section contains COT-directed controls for risk assessment for Commonwealth systems. It details the measures agencies shall implement to ensure the applicable risk assessment controls are in place. Where possible and as necessary, system owners, information owners, and service managers should coordinate to ensure that agencies and service providers understand and adhere to these controls.

RA-2 – Security Categorization

Agencies shall:

1. Categorize the information and system processes, stores, and transmits in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
2. Document the security categorization results (including supporting rationale) in the security plan for the system.
3. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

RA-3 – Risk Assessment

Agencies shall:

1. Conduct a risk assessment including:

a. Identifying threats to and vulnerabilities in the system;
b. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and
c. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information.

2. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments.
3. Document the risk assessment results in an assessment report of other agency-defined report type.
4. Review risk assessment results at least annually.
5. Disseminate the risk assessment results to the agency-defined personnel.
6. Update the risk assessment at least every three years or whenever there are significant changes to the system or environment of operation. This includes the identification of new threats and vulnerabilities or other conditions that may impact the security or privacy state of the system.

RA-3(1) – Risk Assessment | Supply Chain Risk Assessment

Agencies shall:

1. Assess supply chain risks associated with agency-defined systems, system components, and system services identified as being essential to the mission and business functions of the organization.
2. Update the supply chain risk assessment at least every three years or whenever there are significant changes to the system or environment of operation. This includes the identification of new threats and vulnerabilities or other conditions that may impact the security or privacy state of the system.

RA-5 – Vulnerability Monitoring and Scanning

COT shall:

1. Monitor and scan for vulnerabilities in the system on a monthly basis and hosted applications by request of the agency and when new vulnerabilities potentially affecting the system are identified or reported.
2. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    a. Enumerating platforms, software flaws, and improper configurations;
    b. Formatting checklists and test procedures; and
    c. Measuring vulnerability impact.
3. Analyze vulnerability scan reports from vulnerability monitoring.
4. Remediate legitimate vulnerabilities on a monthly basis in accordance with organization-defined assessment of risk.
5. Share information obtained from the vulnerability monitoring process and control assessments with key agency personnel and COT technical teams to help eliminate similar vulnerabilities in other systems.
6. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

RA-5(2) – Vulnerability Monitoring and Scanning | Update Vulnerabilities to be Scanned

Agencies shall update the system vulnerabilities to be scanned daily and when new vulnerabilities are identified and reported.

RA-5(5) – Vulnerability Monitoring and Scanning | Privileged Access

Agencies shall implement privileged access authorization to all system components for selected vulnerability scanning activities.

RA-5(11) – Vulnerability Monitoring and Scanning | Public Disclosure Program

Agencies shall establish a public reporting channel for receiving reports of vulnerabilities in organizational system components.

RA-7 – Risk Response

Agencies shall respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

RA-9 – Criticality Analysis

Agencies shall identify critical system components and functions by performing a criticality analysis for agency-defined systems, system components, or system services at appropriate decision points within the system development lifecycle as defined by the agency.

Risk Assessment Best Practices

(This space reserved for best practices)

CIO-104 Configuration Management

The security controls outlined in this section support the Commonwealth of Kentucky's **CIO-104 Configuration Management Policy** and require the same compliance as the originating policy. The Office of the Chief Information Security Officer (CISO) may update these controls to ensure the Commonwealth addresses effective security and risk management practices.

These moderate-level controls address the Configuration Management (CM) family identified in the NIST Special Publication 800-53 Rev 5. They cover all executive and non-executive branch agencies using COT-managed infrastructure or services. Agencies, employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the CISO approves exceptions or mitigating controls.

Configuration Management Controls

The following section contains COT-directed controls for configuration management for Commonwealth systems. It details the measures agencies shall implement to ensure the applicable

configuration management controls are in place. Where possible and as necessary, system owners, information owners, and service managers should coordinate to ensure that agencies and service providers understand and adhere to these controls.

CM-2 – Baseline Configuration

COT shall:

1. Develop, document, and maintain a current enterprise-level baseline configuration of each platform (i.e., Windows, UNIX, Linux, Database, etc.) within its environment, using a Configuration Management Database (CMDB) as the master or "golden" record.
2. Review and update the baselines annually and as needed due to system upgrades, patches, or other significant changes.

Agencies shall:

1. Develop, document, and maintain application-specific baseline configurations.
2. Review and update the baselines annually and as needed due to system upgrades, patches, or other significant changes.

CM-2(2) – Baseline Configuration | Automation Support for Accuracy and Currency

COT and agencies shall maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using agency-defined automated mechanisms.

CM-2(3) – Baseline Configuration | Retention of Previous Configurations

COT and agencies shall retain an agency-defined number of previous configurations to support rollback, as determined by the appropriate agency-level procedure.

CM-2(7) – Baseline Configuration | Configure Systems and Components for High-Risk Areas

COT and agencies shall:

1. Issue system components with elevated security controls to individuals traveling to locations that the agency deems to be of significant risk.
2. Apply agency-defined controls to the systems or components when the individuals return from travel.

CM-3 – Configuration Change Control

COT and agencies shall:

1. Determine the types of changes to a system that are configuration-controlled.
2. Review proposed configuration-controlled changes and approve or disapprove such changes, with explicit consideration for security impact analysis, and document change decisions.
3. Document configuration change decisions associated with the system.
4. Implement approved configuration-controlled changes to the system.
5. Retain records of configuration-controlled changes for the life of the system.
6. Monitor and review activities associated with configuration-controlled changes.
7. Coordinate and provide oversight for change control activities through the agency-defined approvers.

CM-3(2) – Configuration Change Control | Testing, Validation, and Documentation Changes

COT and agencies shall test, validate, and document changes to the system before finalizing the implementation of the changes.

CM-3(4) – Configuration Change Control | Security and Privacy Representatives

COT and agencies shall require agency-defined security and privacy representatives to be members of the agency-defined configuration change control element.

CM-4 –Impact Analysis

COT and agencies shall analyze changes to an system to determine potential security and privacy impacts prior to implementation.

CM-4(2) – Impact Analysis | Verification of Controls

COT and agencies shall, after system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

CM-5 – Access Restrictions for Change

COT and agencies shall define, document, approve, and enforce physical and logical access restrictions associated with changes to an system.

CM-6 – Configuration Settings

COT and agencies shall:

1. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using agency-defined common secure configurations.
2. Implement the configuration settings.
3. Identify, document, and approve any deviations from established configuration settings for agency-defined system components based on agency- defined operational requirements.
4. Monitor and control changes to configuration settings in accordance with enterprise and office-level policies and procedures.

CM-7 – Least Functionality

COT and agencies shall:

1. Configure systems to provide only mission essential agency-defined capabilities.
2. Restrict the use of functions, ports, protocols, and services deemed unnecessary or detrimental to the system or business.

CM-7(1) – Least Functionality | Periodic Review

COT and agencies shall:

1. Review the system according to agency-defined frequency to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services.
2. Disable or remove unnecessary or non-secure functions, ports, protocols, software, and services according to agency-defined frequency.

CM-7(2) – Least Functionality | Prevent Program Execution

COT and agencies shall prevent program execution in accordance with agency-defined policies, and/or access agreements, regarding software program usage and restrictions, authorizing the terms, and conditions of software program usage.

CM-7(5) – Least Functionality | Authorized Software – Allow By-Exception

1. Identify agency-defined software programs authorized to execute on the system.
2. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system.
3. Review and update the list of authorized software programs according to agency-defined frequency.

CM-8 –System Component Inventory

Agencies shall:

1. Develop and document an inventory of system components that:
    a. Accurately reflects the current systems for which COT and the agency is responsible;
    b. Includes all components within the authorization boundary of the system;
    c. Does not include duplicate accounting of components or components assigned to any other system;
    d. Is at the level of granularity deemed necessary for tracking and reporting; and
    e. Includes information necessary to achieve effective infrastructure component accountability.
2. Review and update component inventory according to agency-defined frequency.

CM-8(1) –System Component Inventory | Updates During Installation and Removal

Agencies shall review and update the inventory od system components as an integral part of installation, removal, and system updates.

CM-8(3) –System Component Inventory | Automated Unauthorized Component Detection

Agencies shall:

1. Detect presence of unauthorized hardware, software, and firmware components within the system using agency-defined automated mechanism according to agency-defined frequency.
2. Act when unauthorized components are detected by notifying authorized agency-defined points of contact.

CM-9 – Configuration Management Plan

Agencies shall develop, document, and implement a configuration management plan for systems that:

1. Addresses roles, responsibilities, and configuration management processes and procedures.
2. Establishes a process for identifying configuration items throughout the system development life cycle (SDLC).
3. Defines configuration items for the system and ensure they align with established processes and procedures.
4. Is reviewed and approved by authorized agency-defined points of contact.
5. Protects the configuration management plan from unauthorized disclosure and modification.

CM-10 – Software Usage Restrictions

Agencies shall:

1. Use software and associated documentation in accordance with contractual agreements and copyright laws and track the use of software protected for quantity licenses.
2. Strictly prohibit the use of peer-to-peer file sharing technology.
3. Establish restrictions on the use of open-source software (OSS), which must be approved and listed in the Kentucky Information Technology Standards (KITS) and adhere to a secure configuration baseline.

CM-11 – User-Installed Software

Agencies shall establish, monitor, and enforce guidelines, policies, and compliance governing the installation of software by users.

CM-12 – Information Location

Agencies shall:

1. Identify and document the location of agency-defined information and the specific system components on which the information is processed and stored.
2. Identify and document the users who have access to the system and system components where the information is processed and stored.
3. Document changes to the location (i.e., system or system components) where the information is processed and stored.

CM-12(1) – Information Location | Automated Tools to Support Information Location

Agencies shall use automated tools to identify agency-defined information by information type on agency-defined system components to ensure controls are in place to protect organizational information and individual privacy.

Configuration Management Best Practices

(This space reserved for best practices)

CIO-105 System and Information Integrity

The security controls outlined in this section support the Commonwealth of Kentucky's **CIO-105 System and Information Integrity Policy** and require the same compliance as the originating policy. The Office of the Chief Information Security Officer (CISO) may update these controls to ensure the Commonwealth addresses effective security and risk management practices.

These moderate-level controls address **System and Information Integrity (SI)** as identified in the NIST Special Publication 800-53 Rev 5. They cover all executive and non-executive branch agencies

using COT-managed infrastructure or services. Agencies, employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the CISO approves exceptions or mitigating controls.

Definitions

Data Integrity: The maintenance and assurance of the accuracy and consistency of data over its entire life cycle and is a critical aspect to the design, implementation and usage of any systems that store, process, or retrieve data.

Information Integrity: The assurance that the data being accessed or read has neither been tampered with nor altered or damaged through system error since the time of the last authorized access.

System Integrity: The state of a system when performing its intended functions without being degraded or impaired by changes or disruptions in its internal or external environments.

System and Information Integrity Controls

The following section contains COT-directed controls for system and information integrity of Commonwealth systems. Where possible, system owners, information owners, and service managers should coordinate as necessary to ensure that agencies and service providers understand and adhere to these controls.

SI-2 – Flaw Remediation

Agencies shall:

1. Identify, report, and correct system flaws.
2. Test all software, firmware, and system changes, updates, upgrades, and new systems implementations.
3. Install security-relevant software and firmware updates within established timelines following the release of the update.
4. Incorporate flaw remediation into configuration management process.
5. Employ automated mechanisms to determine the state of infrastructure components with regard to flaw remediation.

SI-2(2) – Flaw Remediation | Automated Flaw Remediation Status

Agencies shall determine if system components have applicable security-relevant software and firmware updates installed using enterprise-defined automated mechanisms in accordance with risk tolerance established by the agency.

SI-3 – Malicious Code Protection

Note: This includes antivirus software, antimalware, and intrusion detection systems.

Agencies shall:

1. Employ signature based and non-signature based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.
2. Automatically update malicious code protection mechanisms whenever new releases are available in accordance with established procedures.
3. Configure malicious code protection mechanisms to:

a. Perform periodic scans of the system weekly and real-time scans of files from external sources at endpoint and network entry/exit points as the files are downloaded, opened, or executed in accordance with agency security policy; and
b. Either block or quarantine malicious code and send an alert to the administrator in response to malicious code detection

4. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.
5. Centrally manage malicious code protection mechanisms.
6. Ensure the systems automatically update malicious code protection mechanisms.

SI-4 –System Monitoring

Agencies shall:

1. Monitor the system to detect:
    a. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and
    b. Unauthorized local, network, and remote connections.
2. Identify unauthorized use of the system and deploy monitoring devices strategically within the system to collect organization-determined essential information and at ad hoc locations within the system to track specific types of transactions of interest to the organization.
3. Invoke internal monitoring capabilities or deploy monitoring devices:
    a. Strategically within the system to collect organization-determined essential information; and
    b. At ad hoc locations within the system to track specific types of transactions of interest to the organization.
4. Analyze detected events and anomalies.
5. Adjust the level of system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the nation, based on law enforcement information, intelligence information, or other credible sources of information.
6. Obtain a legal opinion with regard to system monitoring activities in accordance with applicable federal laws, executive orders, directives, policies, or regulations.
7. Provide system monitoring information to designated agency officials as needed.
8. Employ automated mechanisms to alert security personnel of inappropriate or unusual activities with negative security implications.
9. Implement host-based monitoring mechanisms (e.g., host intrusion prevention system (HIPS) on systems that receive, process, store, or transmit data.

SI-4(2) – System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis

Agencies shall employ automated tools to support near real-time analysis of events.

SI-4(4) – System Monitoring | Inbound and Outbound Communications Traffic

The system shall:

1. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic.

2. Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conductions.

SI-4(5) – System Monitoring | System-Generated Alerts

The system shall alert key personnel, such as system administrators, business/process owners, system owners, or information security officers when indications of a compromise or a threat of a compromise occurs.

SI-5 – Security Alerts, Advisories, and Directives

Agencies shall:

1. Receive system security alerts, advisories, and directives from reliable industry sources, such as the US Computer Emergency Readiness Team (US-CERT), Cybersecurity & Infrastructure Security Agency and MS-ISAC (CISA), Homeland Security Cyber Security, or other relevant organizations or vendors.
2. Generate internal security alerts, advisories, and directives as deemed necessary.
3. Disseminate security alerts, advisories, and directives to appropriate personnel, such as management, system administrators, business/process owners, system security officers, etc.
4. Implement security directives in accordance with established periods or notify the issuing organization of the degree of noncompliance.

SI-7 – Software, Firmware, and Information Integrity

Agencies shall:

1. Employ integrity verification tools to detect unauthorized changes to software, firmware, and information.
2. Take the following actions when unauthorized changes to the software, firmware, and information are detected in accordance with agency-defined actions.

SI-7(1) – Software, Firmware, and Information Integrity | Integrity Checks

Agencies shall perform integrity checks of organization hardware, software, firmware, and services at startup, shutdown, and restart and on demand by the system administrator.

SI-7(7) – Software, Firmware, and Information Integrity

Agencies shall incorporate the detection of unauthorized changes to the system into the organizational incident response capability.

SI-8 – Spam Protection

Agencies shall:

1. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages.
2. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

SI-8(2) – Spam Protection | Automatic Updates
Agencies shall update spam protection mechanisms automatically.

SI-10 – Information Input Validation
The system shall check the integrity and validity of system inputs such as character set, length, numerical range, and other acceptable values.

SI-11 – Error Handling
The system shall:

1. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.
2. Reveal error messages only to designated organization personnel.

SI-12 – Information Management and Retention
Agencies shall manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, policies, regulations, standards, guidelines, and operational requirements.

SI-16 – Memory Protection
Agencies shall implement security safeguards to protect its memory from unauthorized code execution.

Note: Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can be either hardware-enforced or software-enforced, with hardware providing the greater strength of mechanism.

System and Information Integrity Best Practices

(This space reserved for best practices)

CIO-112 Security Planning

The security controls outlined in this section support the Commonwealth of Kentucky's **CIO-112 Security Planning Policy** and require the same compliance as the originating policy. The Office of the Chief Information Security Officer (CISO) may update these controls to ensure the Commonwealth addresses effective security and risk management practices.

These moderate-level controls address the **Security Planning (PL) family** as identified in NIST Special Publication 800-53 Rev 5. They cover all executive branch and non-executive branch agencies using COT-managed infrastructure or services. Agencies, employees, contractors, vendors,

consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the CISO approves exceptions or mitigating controls.

Security Planning Controls

The following section contains COT-directed controls for security planning for Commonwealth systems. Where possible, system owners, information owners, and service managers should coordinate as necessary to ensure that agencies and service providers understand and adhere to these controls.

PL-2 – System Security Plan

Agencies shall:

1. Develop security and privacy plans for the system that:
    a. Are consistent with the organization enterprise architecture;
    b. Explicitly define the constituent system components;
    c. Describe the operational context of the system in terms of mission and business processes;
    d. Identify the individuals that fulfill system roles and responsibilities;
    e. Identify the information types processed, stored, and transmitted by the system;
    f. Provide the security categorization of the system, including supporting rationale;
    g. Describe any specific threats to the system that are of concern to the organization;
    h. Provide the results of a privacy risk assessment for systems processing personally identifiable information;
    i. Describe the operational environment for the system and any dependencies on, or connections to, other systems or system components;
    j. Provide an overview of the security and privacy requirements for the system;
    k. Identify any relevant control baselines or overlays, if applicable;
    l. Describe the controls in place or planned for meeting the security and privacy requirements including a rationale for the tailoring decisions;
    m. Include risk determinations for security and privacy architecture and design decisions;
    n. Include security and privacy-related activities affecting the system that require planning and coordination with agency-defined individuals or groups; and
    o. Are reviewed and approved by the authorizing official or designated representatives prior to plan implementation.
2. Distribute copies of the plans and communicate subsequent changes to the plan implementation.
3. Review the security plans for the system in accordance with risk tolerance established by the agency.
4. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or security control assessments.
5. Protects the security plan from unauthorized disclosure and modification.
6. Organize and coordinate security-related activities and testing affecting the system with COT Change Management before conducting such activities in order to reduce the impact on other organizational entities. Ensure that all changes and/or security exceptions are properly completed, reviewed, and approved prior to plan implementation.

PL-4 – Rules of Behavior

Agencies shall:

1. Establish and make readily available to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior with regard to information system usage.
2. Receive a signed acknowledgement from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system.
3. Review and update the rules of behavior in accordance with risk tolerance established by the agency.
4. Require individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

PL-4(1) – Rules of Behavior | Social Media and External Site/Application Usage Restrictions

Agencies shall include the rules of behavior, restriction on:

1. Use of social media, social networking sites, and external sites/applications.
2. Posting organizational information on public websites.
3. Use of organization-provided identifiers (e.g., email addresses) and authentication credentials for creating accounts on external sites/applications.

PL-8 –Security and Privacy Architecture

Agencies shall:

1. Develop security and privacy architecture for the system that:
    a. Describe the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
    b. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;
    c. Describe how the architectures are integrated into and support the enterprise architecture; and
    d. Describe any assumptions about, and dependencies on external systems and services.
2. Review and update the architectures in accordance with risk tolerance established by the agency to reflect changes in the enterprise architecture.
3. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

PL-10 – Baseline Selection

Agencies shall select a control baseline for the system that is in alignment with enterprise standards, commensurate with the system classification, and applicable regulatory guidance.

PL-11 – Baseline Tailoring

Agencies shall tailor the selected control baseline by applying specified tailoring actions. Deviations must be documented as a policy exemption.

Security Planning Best Practices

(This space reserved for best practices)

CIO-113 Contingency Planning

The security controls outlined in this section support the Commonwealth of Kentucky's **CIO-113 Contingency Planning Policy** and require the same compliance as the originating policy. The Office of the Chief Information Security Officer (CISO) may update these controls to ensure the Commonwealth addresses effective security and risk management practices.

These moderate-level controls address the **Contingency Planning (CP) family** identified in NIST Special Publication 800-53 Rev 5. They cover all executive and non-executive branch agencies using COT-managed infrastructure or services. Agencies, employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the CISO approves exceptions or mitigating controls.

Contingency Planning Controls

The following section contains COT-directed controls for contingency planning for Commonwealth systems. It details the measures agencies shall implement to ensure the applicable contingency planning controls are in place for compliance. Where possible and as necessary, system owners, information owners, and service managers should coordinate to ensure that agencies and service providers understand and adhere to these controls.

CP-2 – Contingency Plan

Agencies shall:

1. Develop a contingency plan for their systems that:
    a. Identifies essential mission and business functions and associated contingency requirements;
    b. Provides Recovery Time Objectives (RTOs), Restoration Point Objectives (RPOs), and other metrics;
    c. Addresses contingency roles and responsibilities and assigns individuals with contact information;
    d. Addresses the maintenance of essential mission and business functions despite a system disruption, compromise, or failure;

e. Addresses eventual full restoration of system functionality without deterioration of security safeguards originally implemented; and
f. Is reviewed and approved by key contingency personnel.

2. Distribute copies of the contingency plan to key contingency personnel.
3. Coordinate contingency planning activities with incident handling activities.
4. Review the contingency plan for their systems at least annually.
5. Update the contingency plan to address changes to the organization, system, or environment of operation, and problems encountered during contingency plan implementation, execution, or testing.
6. Communicate contingency plan changes to key agency contingency personnel.
7. Protect the contingency plan from unauthorized disclosure or modification.
8. Coordinate contingency plan development with organizational elements responsible for related plans such as Business Continuity Plans and Disaster Recovery Plans.

CP-2(1) – Contingency Plan | Coordinate with Related Plans

Agencies shall coordinate contingency plan development with organizational elements responsible for related plans.

CP-2(3) – Contingency Plan | Resume Mission and Business Functions

Agencies shall plan for the resumption of essential mission and business functions within 24 hours of contingency plan activation.

CP-2(8) – Contingency Plan | Identify Critical Assets

Agencies shall identify critical system assets supporting essential mission and business functions.

CP-3 – Contingency Training

Agencies shall:

1. Provide contingency training to system users consistent with assigned roles and responsibilities:
    a. Within 30 days of assuming a contingency role or responsibility;
    b. When required by system changes; and
    c. And annually, thereafter.
2. Review and update contingency training content annually and following a significant change.

CP-4 – Contingency Plan Testing

Agencies shall:

1. Test their contingency plan for each system at least annually to determine the effectiveness of the plan and the organizational readiness to execute the plan.
2. Review the contingency plan test results.
3. Initiate corrective action, if needed.

CP-4(1) – Contingency Plan Testing – Coordinate with Related Plans

1. Coordinate contingency plans for systems, including Incident Response Plans and other emergency plans, with elements related to these plans.

CP-6 – Alternate Storage Site

Agencies shall:

1. Establish an alternate storage site including necessary agreements to permit the storage and retrieval of system backup information.
2. Ensure that the alternate storage site provides information security safeguards equivalent to that of the primary site.

CP-6(1) – Alternate Storage Site – Separation from Primary Site

Agencies shall identify an alternate storage site that is physically separated from the primary site to reduce the susceptibility of the alternate site being exposed to the same threats as the primary site (i.e., natural disasters, structural failures, major utility disruptions, etc.).

CP-6(3) – Alternate Storage Site – Accessibility

Agencies shall identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

CP-7 – Alternate Processing Site

Agencies shall:

1. Establish an alternate processing site including the necessary agreements to permit the transfer and resumption of organizational system operations for essential missions/business functions within defined time periods when the primary processing capabilities are unavailable.
2. Ensure that equipment and supplies required to transfer, and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within organization-defined time periods for transfer/resumption of service.
3. Ensure that the alternate processing site provides controls equivalent to those at the primary site.

CP-7(1) – Alternate Processing Site | Separation from Primary Site

Agencies shall identify an alternate processing site that is separated from the primary site to reduce exposure and susceptibility to the same threats as the primary site.

CP-7(2) – Alternate Processing Site | Accessibility

Agencies shall identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

CP-7(3) – Alternate Processing Site | Priority of Service

Agencies shall develop alternate agreements with the alternate site that contain priority-of-service provisions in accordance with organizational availability requirements.

CP-8 – Telecommunication Services

Agencies shall establish alternate telecommunication services including necessary agreements to permit the resumption of organization's system operations, in accordance with the RTOs defined in the organization's contingency plan when the primary telecommunications capabilities are unavailable at either the primary or alternate storage sites.

CP-8(1) - Telecommunication Services | Priority of Service Provisions

Agencies shall:

1. Develop primary and alternative telecommunication service agreements that include priority-of-service provisions that match organization availability requirements, including RTOs.
2. Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

CP-8(2) - Telecommunication Services | Single Points of Failure

Agencies shall procure alternate (redundant) telecommunication services to reduce the likelihood of a single point of failure.

CP-9 –System Backup

Agencies shall:

1. Coordinate and arrange backups for user-level information consistent with the defined frequency in the organization's contingency plan.
2. Coordinate and arrange backups for system-level information consistent with the defined frequency in the organization's contingency plan.
3. Coordinate and arrange backups for system documentation consistent with the defined frequency in the organization's contingency plan.
4. Protect the confidentiality, integrity, and availability of backup information.

CP-9(1) – System Backup | Testing for Reliability and Integrity

Agencies shall test backup media and equipment annually to ensure and verify media reliability and information integrity.

CP-9(8) – System Backup | Cryptographic Protection

Agencies shall implement cryptographic mechanisms to prevent unauthorized disclosure and modification of agency-defined backup information.

CP-10 –System Recovery and Reconstitution

Agencies shall provide for the recovery and reconstitution of systems to a known state within 24 hours of a disruption, compromise, or failure.

CP-10(2) - System Recovery and Reconstitution | Transaction Recovery

Agencies shall include systems that are transaction-based.

Contingency Planning Best Practices

(This space reserved for best practices)

CIO-114 System Maintenance

The security controls outlined in this section support the Commonwealth of Kentucky's **CIO-114 System Maintenance Policy** and require the same compliance as the originating policy. The Office of the Chief Information Security Officer (CISO) may update these controls to ensure the Commonwealth addresses effective security and risk management practices.

These moderate-level controls address the **Maintenance (MA) family** identified in NIST Special Publication 800-53 Rev 5. They cover all executive and non-executive branch agencies using COT-managed infrastructure or services. Agencies, employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the CISO approves exceptions or mitigating controls.

System Maintenance Controls

The following section contains COT-directed controls for maintenance of Commonwealth systems. It details the measures agencies shall implement to ensure the applicable maintenance provisions are in place for compliance. Where possible and as necessary, system owners, information owners, and service managers should coordinate to ensure that agencies and service providers understand and adhere to these controls.

Definitions

Controlled Maintenance: Tasks performed on an system or components (software or hardware) that are scheduled and performed in accordance with manufacturer, vendor, or agency specifications.

Nonlocal Maintenance: System maintenance activities that agency personnel with approved authorization, access, and technical competence conduct on an system through a network, whether external (e.g., the internet) or internal (e.g., LAN).

MA-2 – Controlled Maintenance

Agencies shall:

1. Schedule, document, and review records of maintenance, repairs, and replacement on system components in accordance with manufacturer or vendor specifications and COT requirements.
2. Approve and monitor all maintenance activities, whether performed on-site or remotely and whether servicing the equipment on-site or moved to another location.
3. Explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement.
4. Sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement.

5. Check all security controls potentially affected by maintenance to verify that the controls are still functioning properly following maintenance, repair, or replacement.
6. Maintain system records, and include the following in the organizational maintenance records at a minimum:
    a. Date and time of maintenance;
    b. Name of the individual(s) performing maintenance; and
    c. The maintenance description to include details of what equipment was replaced, serial numbers, tracking numbers, and other similar information.

MA-3 – Maintenance Tools

Agencies shall:

1. Approve, control, and monitor system maintenance tools.
2. Review previously approved system maintenance tools annually.

MA-3(1) – Maintenance Tools | Inspect Tools

Agencies shall inspect maintenance tools used by maintenance personnel for improper use and unauthorized modifications.

MA-3(2) – Maintenance Tools | Inspect Media

Agencies shall check media containing diagnostic and test programs for malicious code before the media are used in the system.

MA-3(3) – Maintenance Tools | Prevent Unauthorized Removal

Agencies shall prevent the removal of maintenance equipment containing organizational information by ensuring one or more of the following:

1. Verify that there is no organization information contained on the equipment.
2. Sanitize or destroy the equipment.
3. Retain the equipment within the facility.
4. Authorize removal of the equipment from the facility, in accordance with CIO-059 Equipment Installation and Removal at Commonwealth Data Centers.

MA-4 – Nonlocal Maintenance

Agencies shall:

1. Approve and monitor nonlocal maintenance and diagnostic activities.
2. Allow the use of nonlocal maintenance and diagnostic tools only according to agency policy and as documented in the security plan for the system.
3. Employ strong authentication and/or encryption methods in the establishment of nonlocal maintenance and diagnostic sessions, such as biometrics, tokens, and passphrases.
4. Include the following, at a minimum, in the agency's maintenance records for nonlocal maintenance and diagnostic activities:
    a. Date and time of maintenance;
    b. Name of individual(s) performing the maintenance; and
    c. The maintenance description to include details of what data was transferred (if any), what software tools were used for diagnostics, and the manner in which the remote connection was facilitated.
5. Terminate session and network connections after completing nonlocal maintenance.

MA-5 – Maintenance Personnel

Agencies shall:

1. Establish a process for authorizing maintenance personnel.
2. Maintain a list of authorized maintenance organizations or personnel.
3. Ensure that non-escorted personnel performing maintenance on the system have required access authorization.
4. Designate COT personnel with required access authorization and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.
5. Ensure that non-escorted personnel performing maintenance activities not directly associated with the system—but in the physical proximity of the system—have the required access authorizations.

MA-6 – Timely Maintenance

Agencies shall obtain maintenance support and spare parts for systems and their components within an agency-defined period as outlined in the system security plan.

System Maintenance Best Practices

(This space reserved for best practices)

CIO-115 Physical and Environmental Protection

The security controls outlined in this section support the Commonwealth of Kentucky's **CIO-115 Physical and Environmental Protection Policy** and require the same compliance as the originating policy. The Office of the Chief Information Security Officer (CISO) may update these controls to ensure the Commonwealth addresses effective security and risk management practices.

These moderate-level controls address the **Physical and Environmental Protection (PE) family** as identified in the NIST Special Publication 800-53 Rev 5 and cover all executive and non-executive branch agencies using COT-managed infrastructure or services. Agencies, employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the CISO approves exceptions or mitigating controls.

Physical and Environmental Protection Controls

The following section contains COT-directed controls for physical and environmental protection for Commonwealth systems. Where possible, system owners, information owners, and service managers should coordinate as necessary to ensure that agencies and service providers understand and adhere to these controls.

PE-2 – Physical Access Authorizations

Agencies shall:

1. Develop, approve, and maintain a list of individuals with authorized access to the facility where the information system resides.
2. Issue authorization credentials for facility access.
3. Review the access list detailing authorized facility access by individuals.
4. Remove individuals from the facility access list when access is no longer required.

PE-3 – Physical Access Control

Agencies shall:

1. Enforce physical access authorizations at entry/exit points to the facility where the system resides by:
    a. Verifying individual access authorizations before granting access to the facility; and
    b. Controlling ingress/egress to the facility using physical access control systems, devices, or security guards.
2. Maintain physical access audit logs for every entry and exit points.
3. Control access to areas within the facility officially designated as publicly accessible in accordance with policy document CIO-058 Commonwealth Data Center IT Equipment Room Physical Access.
4. Escort visitors and monitor visitor activity.
5. Secure keys, combinations, and other physical access devices,
6. Take inventories of physical access devices every two years.
7. Change combinations and keys whenever keys are declared missing, combinations are compromised, or individuals are transferred or terminated.

PE-4 – Access Control for Transmission

Agencies shall control physical access to system distribution and transmission lines within organizational facilities using agency-defined security controls.

PE-5 – Access Control for Output Devices

Agencies shall control physical access to output devices to prevent unauthorized individuals from obtaining the output.

PE-6 – Monitoring Physical Access

Agencies shall:

1. Monitor physical access to the facility where the system resides to detect and respond to physical incidents.
2. Review physical access logs monthly.
3. Coordinate results of reviews and investigations with the organizational incident response capability.
4. Monitor physical intrusion alarms and surveillance equipment where applicable.

PE-8 – Visitor Access Records

Agencies shall:

1. Maintain visitor access records to the facility where the system resides for agency-defined time period in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.
2. Review visitor access records monthly.
3. Report anomalies in visitor access records to agency-defined personnel.

PE-9 – Power Equipment and Cabling

Agencies shall protect power equipment and power cabling for the system from damage and destruction.

PE-10 – Emergency Shutoff

Agencies shall:

1. Provide the capability of shutting off power to the agency-defined system or individual system components in emergency situations.
2. Place emergency shutoff switches or devices in agency-defined location to facilitate safe and easy access for personnel.
3. Protect emergency power shutoff capability from unauthorized activation.

PE-11 – Emergency Power

Agencies shall provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the system or transition of the systems to long-term alternate power in the event of a primary power source loss.

PE-12 – Emergency Lighting

Agencies shall employ and maintain automatic emergency lighting for the lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

PE-13 – Fire Protection

Agencies shall:

1. Employ and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.
2. Employs automatic fire suppression capability for the system when the facility is not staffed on a continuous basis.

PE-14 –Environmental Controls

Agencies shall:

1. Maintain temperature and humidity levels within the facility where the system resides at agency-defined acceptable levels.
2. Monitor temperature and humidity levels continuously.

PE-15 – Water Damage Protection

Agencies shall protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

PE-16 – Delivery and Removal

Agencies shall:

1. Authorize and control all system components entering and exiting the facility in accordance with policy document CIO-059 Equipment Installation and Removal at Commonwealth Data Centers.
2. Maintain records of those components.

PE-17 – Alternate Work Site

Agencies shall:

1. Determine and document the agency-defined alternate work sites allowed for use by employees.
2. Employ appropriate management, operational, and technical system security controls at alternate work sites.
3. Assess, as feasible, the effectiveness of security controls at alternate work site.
4. Provide a means for employees to communicate with information security personnel in case of security incidents or problems.

Physical and Environmental Protection Best Practices

(This space reserved for best practices)

CIO-116 Personnel Security

The security controls outlined in this section support the Commonwealth of Kentucky's **CIO-116 Personnel Security Policy** and require the same compliance as the originating policy. The Office of the Chief Information Security Officer (CISO) may update these controls to ensure the Commonwealth addresses effective security and risk management practices.

These moderate-level controls address the **Personnel Security (PS) family** as identified in the NIST Special Publication 800-53 Rev 5. They cover all executive and non-executive branch agencies using COT-managed infrastructure or services. Agencies, employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere, at a minimum, to these controls unless the CISO approves exceptions or mitigating controls.

Personnel Security Controls

The following section contains COT-directed controls for personnel security for Commonwealth systems. Where possible, system owners, information owners, and service managers should coordinate as necessary to ensure that agencies and service providers understand and adhere to these controls.

PS-2 – Position Risk Designation

Agencies shall:

1. Assign a risk designation to all organizational positions.
2. Establish screening criteria for individuals filling those positions.
3. Review and update position risk designations at an agency-defined frequency.

PS-3 – Personnel Screening

Agencies shall:

1. Screen individuals prior to authorizing access to the system.
2. Rescreen individuals according to organization-defined conditions requiring rescreening and frequency.

PS-4 – Personnel Termination

Upon termination of individual employment, agencies shall:

1. Disable system access within organization-defined time period.
2. Terminate/revoke any authenticators/credentials associated with the individual.
3. Conduct exit interviews that include organization-defined information security topics.
4. Retrieve all security-related agency system-related property.
5. Retain access to organizational information and systems formerly controlled by terminated individual.

PS-5 – Personnel Transfer

Agencies shall:

1. Review and confirm ongoing operational need for current logical and physical access authorizations to systems/facilities when individuals are reassigned or transferred to other positions within the organization.
2. Initiate deadline transfer or reassignment actions within organization-defined time period following the formal transfer action.
3. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.
4. Notify agency personnel within an agency-defined period.

PS-6 – Access Agreements

Agencies shall:

1. Develop and document access agreements for organizational systems.
2. Review and update the access agreements.
3. Ensure that individuals requiring access to organizational information and systems:
    a. Sign appropriate access agreements prior to being granted access; and
    b. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated.

PS-7 – Third-Party Personnel Security

Agencies shall:

1. Establish personnel security requirements including security roles and responsibilities for third party providers.
2. Require third-party providers to comply with personnel security policies and procedures established by the organization.
3. Document personnel security requirements.
4. Require third-party providers to notify agency personnel of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have system privileges within a defined time period.
5. Monitor provider compliance with personnel security requirements.

PS-8 – Personnel Sanctions

Agencies shall:

1. Employ a formal sanction process for individuals failing to comply with established information security and privacy policies and procedures.
2. Notify agency-defined personnel an agency-defined time period when a formal employee sanction process is initiated, identifying the individual sanctioned, and the reason for the sanction.

PS-9 – Position Descriptions

Agencies shall incorporate security and privacy roles and responsibilities into position descriptions.

Personnel Security Best Practices

(This space reserved for best practices)

CIO-117 System and Services Acquisition

The security controls outlined in this section support the Commonwealth of Kentucky's **CIO-117 System and Services Acquisition Policy** and require the same compliance as the originating policy. The Office of the Chief Information Security Officer (CISO) may update these controls to ensure the Commonwealth addresses effective security and risk management practices.

These moderate-level controls address the **System and Services Acquisition (SA) family** as identified in the NIST Special Publication 800-53 Rev 5. They cover all executive and non-executive branch agencies using COT-managed infrastructure or services. Agencies, employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the CISO approves exceptions or mitigating controls.

System and Services Acquisition Controls

The following section contains COT-directed controls for system and services acquisition for Commonwealth systems. Where possible, system owners, information owners, and service managers should coordinate as necessary to ensure that agencies and service providers understand and adhere to these controls.

SA-2 – Allocation of Resources

Agencies shall:

1. Determine information security and privacy requirements for the system or system service in mission and business process planning.
2. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process.
3. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

SA-3 – System Development Life Cycle

Agencies shall:

1. Acquire, develop, and manage the system using organization-defined system development life cycle (SDLC) that incorporates information security and privacy considerations.
2. Define and document information security and privacy roles and responsibilities throughout the SDLC.
3. Identify individuals having information security and privacy roles and responsibilities.
4. Integrate the organizational information security and privacy risk management process into system development life cycle activities.

SA-4 – Acquisition Process

The agency shall include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the system, system component, or system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

1. Security and privacy functional requirements.
2. Strength of mechanism requirements.
3. Security and privacy assurance requirements.
4. Controls needed to satisfy the security and privacy requirements.
5. Security and privacy documentation requirements.
6. Requirements for protecting security and privacy documentation.
7. Description of the system development environment and environment in which the system is intended to operate.
8. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management.
9. Acceptance criteria.

SA-4(1) – Acquisition Process | Functional Properties of Controls

The agency shall require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

SA-4(2) – Acquisition Process | Design and Implementation Information for Controls

The agency shall require the developer of system, system component, or system service to provide a description of the functional properties of the security controls to be employed that includes, but not limited to, security-relevant external system interfaces, high-level design, low-level design, source code or hardware schematics at a level of detail that addresses mid-level NIST controls outlined in this document.

SA-4(9) – Acquisition Process | Functions, Ports, Protocols, and Services in Use

The agency shall require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.

SA-4(10) – Acquisition Process | Use of Approved PIV Products

The agency shall employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.

SA-5 –System Documentation

Agencies shall:

1. Obtain, or develop, administrator documentation for the system, system component, or system service that describes:
    a. Secure configuration, installation, and operation of the system, component, or service;
    b. Effective use and maintenance of security and privacy functions and mechanisms; and
    c. Known vulnerabilities regarding configuration and use of administrative or privileged functions.
2. Obtain, or develop, user documentation for the system, system component, or system service that describes:
    a. User-accessible security and privacy functions and mechanisms and how to effectively use those security functions and mechanisms;
    b. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
    c. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals.
3. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent.
4. Protect documentation as required, in accordance with the risk management strategy.
5. Distribute documentation to organization personnel.

SA-8 – Security and Privacy Engineering Principles

Agencies shall apply system security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components.

SA-9 – External System Services

Agencies shall:

1. Require that providers of external system services comply with organizational security and privacy requirements and employ security and privacy controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

2. Define and document government oversight and user roles and responsibilities regarding external system services.
3. Employ Service Level Agreements (SLAs) to monitor security control compliance by external service providers on an ongoing basis.

SA-9(2) – External System Services | Identification of Functions, Ports, Protocols, and Services

Agencies shall require providers of external system services to identify the functions, ports, protocols, and other services required for the use of such services.

SA-10 – Developer Configuration Management

Agencies shall require the developers of the system, system component, or system service to:

1. Perform configuration management during system, component, or service (development, implementation, disposal, and operation).
2. Document, manage, and control the integrity of changes to configuration items under configuration management.
3. Implement only COT-approved changes to the system, component, or service.
4. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes.
5. Track security flaws and flaw resolution within the system, component, or service and report findings to the system owner.

SA-11 – Developer Testing and Evaluation

Agencies shall require the developer of the system, system component, or system service to:

1. Develop and implement a plan for ongoing security and privacy assessments.
2. Perform integration, system, regression testing, and evaluation at a frequency required by the agency.
3. Produce evidence of the execution of the assessment plan and the results of the security testing and evaluation.
4. Implement a verifiable flaw remediation process.
5. Correct flaws identified during security testing and evaluation.

SA-15 – Development Process, Standards and Tools

Agencies shall:

1. Require the developer of the system, system component, or system service to follow a documented development process that:
    a. Explicitly addresses security and privacy requirements;
    b. Identifies the standards and tools used in the development process;
    c. Documents the specific tool options and tool configurations used in the development process; and
    d. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development.
2. Review the development process, standards, tools, tool options, and tool configurations no less than annually to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy enterprise and agency security and privacy standards, and any applicable regulatory requirements.

SA-15(3) – Development Process, Standards and Tools | Criticality Analysis

Require the developer of the system, system component, or system service to perform criticality analysis:

1. At project planned decision points in the system development lifecycle.
2. At an appropriate level of rigor based on the system classification.

SA-22 – Unsupported System Components

Agencies shall:

1. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer.
2. Include provisions for alternative sources for continued support of unsupported components.

System and Services Acquisition Best Practices

(This space reserved for best practices)

CIO-118 System and Communications Protection

The security controls outlined in this section support the Commonwealth of Kentucky's **CIO-118 System and Communications Protection Policy** and require the same compliance as the originating policy. The Office of the Chief Information Security Officer (CISO) may update these controls to ensure the Commonwealth addresses effective security and risk management practices.

These moderate-level controls address the **System and Communications Protection (SC) family** as identified in the NIST Special Publication 800-53 Rev 5. They cover all executive and non-executive branch agencies using COT-managed infrastructure or services. Agencies, employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the CISO approves exceptions or mitigating controls.

System and Communications Protection Controls

The following section contains COT-directed controls for system and communications protection for Commonwealth systems. Where possible, system owners, information owners, and service managers should coordinate as necessary to ensure that agencies and service providers understand and adhere to these controls.

SC-2 – Application Partitioning

Agencies shall ensure the system separates user functionality, including user interface services, from system management functionality.

SC-4 – Information in Shared Resources

Agencies shall ensure the system prevents unauthorized and unintended information transfer via shared system resources such as registers, main memory, and hard disks after those resources have been released back to systems.

SC-5 – Denial of Service Protection

Agencies shall:

1. Ensure the system protects against, or limits, the effects of enterprise-defined types of denial-of-service events.
2. Employ the enterprise-defined controls to achieve the denial-of-service objective.

SC-7 – Boundary Protection

Agencies shall:

1. Monitor and control communications at the external managed interfaces to the system and at key internal managed within the system.
2. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks.
3. Connect to external networks or systems through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
4. Adopt a deny all, allow by exception policy regarding network communications.
5. Prevent split tunneling for remote devices from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks. Any exceptions require approval.

SC-7(3) – Boundary Protection | Access Points

Agencies shall limit the number of external network connections to the system.

SC-7(4) – Boundary Protection | External Communications Services

Agencies shall:

1. Implement a managed interface for each external telecommunication server.
2. Establish traffic flow policies for each managed interface.
3. Protect the confidentiality and integrity of the information being transmitted across each interface.
4. Document each exception to the traffic flow policy with a supporting business need and duration of the need.
5. Review exceptions to the traffic flow policy annually and remove exceptions that are no longer supported by a business need.
6. Prevent unauthorized exchange of control plane traffic with external networks.
7. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks.
8. Filter unauthorized control plane traffic from external networks.

SC-7(5) – Boundary Protection | Deny by Exception

Agencies shall deny network communications traffic by default and allow network communications traffic by exception at managed interfaces for inbound and outbound traffic.

SC-7(7) – Boundary Protection | Split Tunneling for Remote Devices

Agencies shall prevent split tunneling for remote devices from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

SC-7(8) – Boundary Protection | Route Traffic to Authenticated Proxy Servers

Agencies shall route agency-defined internal communications traffic through managed firewalls.

SC-8 – Transmission Confidentiality and Integrity

Agencies shall ensure the system protects the confidentiality and integrity of transmitted information.

SC-8(1) – Transmission Confidentiality and Integrity | Cryptographic Protection

Agencies shall implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission.

SC-10 – Network Disconnect

Agencies shall ensure the system terminates the network connection associated with a communications session at the end of the session, or after 15 minutes of inactivity.

SC-12 – Cryptographic Key Establishment and Management

Agencies shall establish and manage applicable cryptographic keys for required cryptography employed within the system.

SC-13 – Cryptographic Protection

Agencies shall:

1. Determine enterprise-defined cryptographic uses.
2. Implement applicable cryptographic uses and types of cryptography as required in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

SC-15 – Collaborative Computing Devices and Applications

The agency shall ensure the system:

1. Prohibits remote activation of collaborative computing devices.
2. Provides an explicit indication of use to users physically present at the devices and applications with agency-defined exceptions.

SC-17 – Public Key Infrastructure Certificates

Agencies shall:

1. Obtain or issue public key certificates from an approved service provider.
2. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

SC-18 – Mobile Code

Agencies shall:

1. Define acceptable and unacceptable mobile code and mobile code technologies.
2. Authorize, monitor, and control the use of mobile code within the system.

SC-20 – Secure Name / Address Resolution Service (Authoritative Source)

Agencies shall ensure the system:

1. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.
2. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

SC-21 – Secure Name / Address Resolution Service (Recursive or Caching Resolver)

Agencies shall ensure the system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

SC-22 – Architecture and Provisioning for Name / Address Resolution Service

Agencies shall ensure the systems that collectively provide name/address resolution service for an agency are fault-tolerant and implement internal/external (split-horizon, split-view) role separation.

SC-23 – Session Authenticity

Agencies shall ensure the system protects the authenticity of communication sessions.

SC-28 – Protection of Information at Rest

Agencies shall ensure systems protect the confidentiality and integrity of agency-defined information at rest.

SC-28(1) – Protection of Information at Rest | Cryptographic Protection

Agencies shall implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the internal and confidential classified information at rest on agency-defined system components or media, and agency-defined information.

SC-39 – Process Isolation

The agency shall ensure system maintains a separate execution domain for each executing process.

System and Communications Protection Best Practices

(This space reserved for best practices)

CIO-119 Audit and Accountability

The security controls outlined in this section support the Commonwealth of Kentucky's **CIO-119 Audit and Accountability Policy** and require the same compliance as the originating policy. The Office of the Chief Information Security Officer (CISO) may update these controls to ensure the Commonwealth addresses effective security and risk management practices.

These moderate-level controls address the **Audit and Accountability (AU)** family as identified in the NIST Special Publication 800-53 Rev 5. They cover all executive and non-executive branch agencies using COT-managed infrastructure or services. Agencies, employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the CISO approves exceptions or mitigating controls.

Audit and Accountability Controls

The following section contains COT-directed controls for Audit and Accountability for Commonwealth systems. Where possible, system owners, information owners, and service managers should coordinate as necessary to ensure that agencies and service providers understand and adhere to these controls.

AU-2 –Event Logging

The system owner shall:

1. Identify the types of events that the system is capable of logging in support of the audit function agency-defined event types that the system is capable of logging.
2. Coordinate the event logging function with other organization entities requiring audit-related information, to enhance mutual support and to help guide the selection of events to be logged.
3. Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.
4. Specify the events, their frequency, and as applicable, the situation requiring the auditing for each defined event.
5. Review and update the event types selected for logging and review on an agency-defined frequency.

AU-3 – Content of Audit Records

The system shall ensure that audit records contain information that established the following:

1. What type of event occurred.
2. When the event occurred.
3. Where the event occurred.
4. Source of the event.
5. Outcome of the event.
6. Identity of any individuals, subjects, or objects/entities associated with the event.

AU-3(1) – Content of Audit Records | Additional Audit Information

The system shall generate audit records containing agency-defined information.

AU-4 – Audit Log Storage Capacity

Agencies shall determine and allocate audit log storage capacity in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.

AU-5 – Response to Audit Logging Process Failures

The system shall:

1. Alert agency-defined personnel, within an agency-defined timeframe, in the event of an audit logging process failure.
2. Take the following additional actions: determine why audit logging process failed and remediate.

AU-6 – Audit Review, Analysis, and Reporting

COT and agencies shall:

1. Review and analyze system audit records in accordance with risk tolerance established by the agency for indications of agency-defined inappropriate activity or unusual activity, and the potential impact of the inappropriate or unusual activity.
2. Report the findings to agency-defined personnel.
3. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

AU-6(1) – Audit Review, Analysis, and Reporting | Automated Process Integration

Agencies shall integrate audit record review, analysis, and reporting processes of agency-defined mechanisms.

AU-6(3) – Audit Review, Analysis, and Reporting | Correlate Audit Record Repositories

Agencies shall analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

AU-7 – Audit Reduction and Report Generation

Agencies shall provide and implement an audit record reduction and report generation capability that:

1. Supports on-demand audit record review, analysis, and reporting requirements after-the-fact investigations of incidents.
2. Does not alter the original content or time-ordering of audit records.

AU-7(1) – Audit Record Reduction and Report Generation | Automatic Processing

Agencies shall provide and implement the capability to process, sort, and search audit records for events of interest based on agency-defined fields within audit records.

AU-8 – Time Stamps

The system shall:

1. Use internal system clocks to generate time stamps for audit records.
2. Record time stamps for audit records that map to UTC or GMT.

AU-9 – Protection of Audit Information

The system shall:

1. Protect audit information and audit logging tools from unauthorized access, modification, or deletion.
2. Alert agency-defined personnel upon detection of unauthorized access, modification, or deletion of audit information.

AU-9(4) – Protection of Audit Information | Access by Subset of Privileged Users

The system shall authorize access to management of audit logging functionality only to agency-defined personnel or roles.

AU-11 – Audit Record Retention

COT shall retain audit records, in accordance with risk tolerance established by the agency, or as required by regulatory and records retention requirements.

AU-12 – Audit Generation

The system shall provide audit record generation capability for events defined above in AU-2 and AU-3 and allow events to be selected by COT as well as agency requests.

Audit and Accountability Best Practices

(This space reserved for best practices)

CIO-120 Security Assessment and Authorization

The security controls outlined in this section support the Commonwealth of Kentucky's **CIO-120 Security Assessment and Authorization Policy** and require the same compliance as the originating policy. The Office of the CISO may update these controls to ensure the Commonwealth addresses effective security and risk management practices.

These moderate-level controls address the **Security Assessment and Authorization (CA) family** as identified in the NIST Special Publication 800-53 Rev 5. They cover all executive and non-executive branch agencies using COT-managed infrastructure or services. Agencies, employees, contractors,

vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the CISO approves exceptions or mitigating controls.

Security Assessment and Authorization Controls

The following section contains COT-directed controls for Security Assessment and Authorization for Commonwealth systems. Where possible and as necessary, system owners, information owners, and service managers should coordinate to ensure that agencies and service providers understand and adhere to these controls.

CA-2 – Control Assessments

Agencies shall:

1. Select the appropriate assessor or assessment team for the type of assessment to be conducted.
2. Develop a security assessment plan that describes the scope of the assessment including:
    a. Controls and control enhancements under assessment;
    b. Assessment procedures to be used to determine control effectiveness; and
    c. Assessment environment, assessment team, and assessment roles and responsibilities.
3. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment.
4. Assess the controls in the system and its environment of operation annually, upon major system upgrade/replacement, or as required by law, 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.
5. Produce a control assessment report that documents the results of the assessment.
6. Provide the results of the control assessments.

CA-2(1) – Control Assessments | Independent Accessors

Agencies shall employ independent assessors or assessment teams to conduct control assessments.

CA-3 – Information Exchange

Agencies shall:

1. Authorize connection from the system to other systems through the use of interconnection security agreements (ISA), information exchange agreements (IEA), memoranda of understanding or agreement, service level agreements (SLA), user agreements, nondisclosure agreements, as well as any agency-defined agreements.
2. Document, for each exchange, the interface characteristics, security and privacy requirements, controls, responsibilities for each system, and the impact level of the information communicated.
3. Review and update the agreements annually.

CA-5 – Plan of Action and Milestones

Agencies shall:

1. Develop a plan of action and milestones for the system to document the agency's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls, and to reduce or eliminate known vulnerabilities in the system.
2. Update existing plan of action and milestones based on the findings from controls assessments, security impact analyses, continuous monitoring activities, and based on risk.

CA-6 –Authorization

Agencies shall:

1. Assign a senior-level executive or manager as the authorizing official for the system.
2. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems.
3. Ensure that the authorizing official for the system before commencing operations:
    a. Accepts the use of common controls inherited by the system; and
    b. Authorizes the system to operate.
4. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems.
5. Update the security authorization when the senior authorizing official changes.

CA-7 – Continuous Monitoring

Agencies shall develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

1. Establish agency-defined system-level metrics to be monitored.
2. Establishment of continuous monitoring and assessment of control effectiveness based on Risk.
3. Ongoing control assessments in accordance with the organizational continuous monitoring strategy.
4. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy.
5. Correlation and analysis of information generated by assessments and monitoring.
6. Response actions to address the results of the control assessment and monitoring information analysis.
7. Reporting the security and privacy status of the agency and the system in accordance with the continuous monitoring strategy.

CA-7(1) – Continuous Monitoring | Independent Assessment

Agencies shall employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.

CA-7(4) – Continuous Monitoring | Risk Monitoring

Agencies shall ensure risk monitoring is an integral part of the continuous monitoring strategy that include effectiveness, compliance and change monitoring.

CA-9 – Internal System Connections

Agencies shall:

1. Authorize internal connections of agency-defined components to the system.
2. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated.
3. Terminate internal system connections according to agency-defined conditions.
4. Review in accordance with the continuous monitoring strategy the continued need for each internal connection.

Security Assessment and Authorization Best Practices

(This space reserved for best practices)

CIO-121 Security Awareness and Training

The security controls outlined in this section support the Commonwealth of Kentucky's **CIO-121 Security Awareness and Training Policy** and require the same compliance as the originating policy. The Office of the Chief Information Security Officer (CISO) may update these controls to ensure the Commonwealth addresses effective security awareness and training practices.

These moderate-level controls address the **Security Awareness and Training (AT) family** as identified in the NIST Special Publication 800-53 Rev 5 and cover all executive branch agencies and non-executive branch agencies using COT-managed infrastructure or services. Agencies, employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls.

Awareness and Training Controls

The following section contains COT-directed controls for Security Awareness and Training for Commonwealth systems. Where possible and as necessary, system owners, information owners, and service managers should coordinate to ensure that agencies and service providers understand and adhere to these controls.

AT-2 –Literacy Training and Awareness

COT shall:

1. Provide basic privacy and security literacy training to system users including managers, senior executives, and contractors.
    a. As a part of initial training for new users and on an agency-defined schedule thereafter; and
    b. When required by a system change or another agency-defined event.

2. Employ techniques to increase the security and privacy awareness of system users.
3. Review or update literacy training and awareness content annually and following agency-defined events.
4. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.

AT-2(2) – Literacy Training and Awareness | Insider Threat

Agencies and service providers shall provide literacy training on recognizing and reporting potential indicators of insider threat.

AT-2(3) – Literacy Training and Awareness | Social Engineering and Mining

Agencies and service providers shall provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

AT-3 – Role-Based Training

Agencies and service providers shall:

1. Provide role-based security and privacy training to agency-defined personnel: and annually thereafter and when required by system changes.
    a. Before access is given to the system, information, or performing assigned duties; and
    b. Annually thereafter and when required by system changes.
2. Review or update role-based training content annually and following agency-defined events.
3. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.

AT-4 –Training Records

Agencies and service providers shall document, and monitor security training activities including basic security awareness training and specific system security training and retain those records for a period of at least one year.

Security Awareness and Training Best Practices

(This space reserved for best practices)

CIO-123 Identification and Authentication

The security controls outlined in this section support the Commonwealth of Kentucky's **CIO-123 Identification and Authentication Policy** and require the same compliance as the originating policy. The Office of the CISO may update these controls to ensure the Commonwealth addresses effective security and risk management practices.

These moderate-level controls address the **Identification and Authentication (IA) family** as identified in the NIST Special Publication 800-53 Rev 5. They cover all executive and non-executive

branch agencies using COT-managed infrastructure or services. Agencies, employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the CISO approves exceptions or mitigating controls.

Identification and Authentication Controls

The following section contains COT-directed controls for Identification and Authentication in Commonwealth systems. Where possible and as necessary, system owners, information owners, and service managers should coordinate to ensure that agencies and service providers understand and adhere to these controls.

IA-2 – Identification and Authentication (Organizational Users)

COT, agencies, and service providers shall ensure that systems uniquely identify and authenticate agency users or processes acting on behalf of users. Unique identifier and authentication requirements are outlined in the IA controls below. In providing access to Commonwealth systems, COT, agencies, and service providers shall:

1. Assign User IDs individually so that a single individual shall be responsible for every action initiated by that ID.
2. Prohibit users from using their User IDs to sign up for or access non-government websites unless utilized for official business.
3. Ensure that the system displays the last use of the individual's account, where possible, to detect unauthorized use.

IA-2 (1) – Identification and Authentication (Organizational Users) | Multi-factor Authentication to Privileged Accounts

Agencies and service providers shall ensure that systems and users implement multi-factor authentication (MFA) to privileged accounts.

IA-2 (2) – Identification and Authentication (Organizational Users) | Multi-factor Authentication to Non-Privileged Accounts

Agencies and service providers shall ensure that systems and users implement multi-factor authentication (MFA) to non-privileged accounts.

IA-2 (8) – Identification and Authentication (Organizational Users) | Access to Accounts - Replay Resistant

Agencies and service providers shall implement replay-resistant authentication mechanisms for access to all accounts on Commonwealth systems.

IA-2 (12) – Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials

Agencies and service providers may allow systems to accept and use Personal Identity Verification (PIV) credentials, provided the PIV credentials adhere to the Commonwealth's Kentucky Information Technology Standards (KITS).

IA-3 – Device Identification and Authentication

Systems for the Commonwealth shall uniquely identify and authenticate any device before establishing any local, remote, or network connection. Systems may use Media Access Control (MAC), Transmission Control Protocol/Internet Protocol (TCP/IP addresses), IEEE 802.1x and Extensible Authentication Protocol (EAP), Radius server with EAP-Transport Layer Security (TLS), or Kerberos protocols.

IA-4 – Identifier Management

Agencies and service providers shall ensure Commonwealth systems manage identifiers such as MAC addresses, TCP/IP addresses, usernames, and computer names such that:

1. Only COT authorizes assigning individual, group, role, or device identifiers.
2. Identifiers uniquely distinguish an individual, group, role, or device.
3. Identifiers are assigned to the correct, intended individual, group, role, or device.
4. Systems and agencies shall prevent reuse of identifiers for a minimum of 24 hours.

IA-4(4) – Identifier Management | Identify User Status

Agencies and service providers shall manage individual identifiers by uniquely identifying each individual employee type (i.e. state, contact, temporary, interns and vendors).

IA-5 – Authenticator Management

Agencies and service providers shall adhere to authenticator management controls and processes as outlined in the COT-156 Password Management Process

IA-5 (1) – Authenticator Management | Password-Based Authentication

Agencies and service providers shall adhere to authenticator management controls and processes as outlined in the COT-156 Password Management Process.

IA-5 (2) – Authenticator Management | PKI-Based Authentication

Agencies and service providers shall ensure that the systems, for PKI-based authentication:

IA-5 (2) (a) – Validate certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information,
IA-5 (2) (b) – Enforce authorized access to the corresponding private key,
IA-5 (2) (c) – Map the authenticated identity to the account of the individual or group, and
IA-5 (2) (d) – Implement a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

IA-5 (6) – Authenticator Management | Protection of Authenticators

Agencies and service providers shall protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

IA-6 – Authenticator Feedback

Agencies and service providers shall ensure that systems obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

IA-7 – Cryptographic Module Authentication

Agencies and service providers shall ensure that the systems implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidance for such authentication.

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

Agencies and service providers shall ensure that systems uniquely identify and authenticate non-organizational users (or processes that act on behalf of non-organizational users).

> *Note: The following controls for Federal Identity, Credential, and Access Management (FICAM) and Personal Identity Verification (PIV) credentials are not a requirement; but agencies that use these credentialing platforms should use the controls as a framework for FICAM and PIV use.*

IA-8 (1) – Identification and Authentication (Non-Organizational Users) | Acceptance of PIV Credentials from Other Agencies

Agencies and service providers shall accept and electronically verify PIV-compliant credentials from other federal agencies, where applicable.

IA-8 (2) – Identification and Authentication (Non-Organizational Users) | Acceptance of External Authenticators

Agencies and service providers shall:

1. Ensure that systems only accept external authenticators that are NIST compliant.
2. Document and maintain a list of accepted external authenticators.

IA-8 (4) – Identification and Authentication (Non-Organizational Users) | Use of Defined Profiles

Agencies and service providers shall define profiles for identity management based on open identity management standards.

IA-11 – Identification and Authentication | Re-Authentication

Agencies and service providers shall require users to re-authenticate when required to maintain the level of identity assurance required by the agency or regulatory guidance.

IA-12 – Identity Proofing

Agencies and service providers shall:

1. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines.
2. Resolve user identities to a unique individual.
3. Collect, validate, and verify identity evidence.

IA-12(2) – Identity Proofing | Identity Evidence

Agencies and service providers shall require evidence of individual identification be presented to the registration authority.

IA-12(3) – Identity Proofing | Identity Evidence Validation and Verification

Agencies and service providers shall require that the presented identity evidence be validated and verified through appropriate mechanisms to provide the level of identity assurance as required by the agency or applicable regulatory guidance.

IA-12(5) – Identity Proofing | Address Confirmation

Require that an appropriate notice of proofing be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

Identification and Authentication Best Practices

(This space reserved for best practices)

CIO-125 Supply Chain Risk Management

The security controls outlined in this section support the Commonwealth of Kentucky's **CIO-000 Supply Chain Risk Management** and require the same compliance as the originating policy. The Office of the Chief Information Security Officer (CISO) may update these controls to ensure the Commonwealth addresses effective security and risk management practices.

These moderate-level controls address the Incident Response (SR) family identified in the NIST Special Publication 800-53 Rev 5. They cover all executive and non-executive branch agencies using COT-managed infrastructure or services. Agencies, employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the CISO approves exceptions or mitigating controls.

Supply Chain Risk Management Controls

The following section contains COT-directed controls for supply chain risk management for Commonwealth systems. Where possible and as necessary, system owners, information owners, and service managers should coordinate to ensure that agencies and service providers understand and adhere to these controls.

SR-2 – Supply Chain Risk Management Plan

Agencies shall:

1. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of disposal and data storing components.

2. Review and update the supply chain risk management plan annual or as required, to address threat, organizational or environmental changes.
3. Protect the supply chain risk management plan from unauthorized disclosure and modification.

SR-2(1) – Supply Chain Risk Management Plan | Establish SCRM Team

Agencies shall establish a supply chain risk management team consisting of appropriate personnel with roles sufficient to lead and support SCRM functions.

SR-3 – Supply Chain Controls and Processes

Agencies shall:

1. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes in coordination with personnel with agency defined SCRM roles.
2. Employ organization-defined controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events.
3. Document the selected and implemented supply chain processes and controls in security and privacy plans.

SR-5 – Acquisition Strategies, Tools, and Methods

Agencies shall employ organization-defined acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks.

SR-6 – Supplier Assessments and Reviews

Agencies shall access and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide annually.

SR-8 – Notification Agreements

Agencies shall establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the notification of supply chain compromises and results of assessments or audits in response to reported weaknesses.

SR-10 – Inspection of System Components

Agencies shall inspect systems or system components at random, no less than annually, and upon a major system change to detect tampering.

SR-11 – Component Authenticity

Agencies shall:

1. Develop and implement anti-counterfeit policies and procedures that include the means to detect and prevent counterfeit components from entering the system.
2. Report counterfeit system components internally to COT Office of the CISO.

SR-11(1) – Component Authenticity | Anti-Counterfeit Training

Agencies shall train technical staff to detect counterfeit system components (including hardware, software, and firmware).

SR-11(2) – Component Authenticity | Configuration Control for Component Service and Repair

Agencies shall maintain configuration control over organization-defined system components awaiting service or repair and serviced or repaired components awaiting return to service, as outlined in the CIO-092 Media Protection policy.

SR-12 – Component Disposal

Agencies shall dispose of organization-defined data, documentation, tools, or system components using organization-defined techniques and methods, as outlined in the CIO-092 Media Protection policy.

Supply Chain Risk Management Best Practices

(This space reserved for best practices)

****** END OF DOCUMENT******