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 2020-2
6/25/2020

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

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.4: NIST Special Publication 800-53 (Rev.4), *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 4), *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
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity

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 information 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 4. 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 requirements for all cloud services obtained where Commonwealth information is transmitted, stored, or processed on non-Commonwealth operated systems. More information is available at FedRAMP Authorization.

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. Identify and select types of information system accounts and or roles to support organizational missions or business functions and assign managers for accounts.
2. Establish conditions for authorized users of the system, group and role membership, and access authorizations and other attributes for each account.
3. Require approvals by information owners for requests to create information system accounts;
4. Create, enable, modify, disable, and delete system accounts in accordance with CIO-072 IT Access Control and User Access Management Policy.
5. Review and monitor system accounts according to System Security Plan (SSPs);
6. Require guest users of enterprise wireless networks to read and acknowledge the rules of behavior before receiving access to the system.
7. Notify account managers when:
    a. accounts are no longer required,
    b. users are terminated or transferred,
    c. individual information system usage or need-to-know changes, and
    d. users will not be accessing their respective account for greater than 30 days.

8. Establish processes and procedures for users to obtain access to required information systems on an emergency basis. These emergency procedures shall:
    a. allow access to live systems and associated data only to identified and authorized personnel,
    b. document all emergency actions in detail,
    c. report emergency action to management and review action in a timely manner, and
    d. disable emergency accounts within 24 hours of returning to normal business operations.

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

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

AC-2 (2) – Account Management | Removal of Temporary/Emergency Accounts

Agencies shall ensure service providers:

1. Require and obtain appropriate approvals and authorizations for the creation and use of special accounts (e.g., guest, training, anonymous, maintenance, or temporary emergency accounts) when such accounts are needed.
2. Audit and monitor special account usage.
3. Remove, disable, or otherwise secure special accounts when they are no longer necessary.
4. Render maintenance accounts inactive immediately after the maintenance task(s) has/have been completed.
5. Disable training accounts immediately after the training has been completed. If training accounts are used for multiple classes during a given day, administrators may keep the accounts and their passwords active without modification until the end of the workday rather than disabling the accounts between training sessions.
6. Adhere to the following requirements for guest, temporary, and emergency accounts:
    a. Require acknowledgement of the agency rules of behavior before authorizing access.
    b. Disable these types of accounts automatically within five (5) days after the need is fulfilled.
    c. Lock accounts that cannot be disabled.

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

Agencies shall ensure service providers:

1. Configure the information system to disable accounts automatically after a maximum of 90 days of inactivity, and delete the disabled account after a total of 120 days of inactivity. The system should alert the necessary personnel of such an event.
2. Prohibit users from self-activating accounts that have been disabled after 90 days. Systems will require administrator restoration and/or activation after an account has been disabled or deleted for non-use or inactivity.

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

Agencies shall ensure service providers configure the information system automated auditing of account creations, modifications, disabling, and termination and notify appropriate individuals of these actions.

AC-3 – Access Enforcement

Agencies shall ensure service providers:

1. Configure and enforce approved authorizations for logical access to information 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 information system:
    a. data flow controls within the systems and between interconnected systems; *(Note: This will be regulated where information is allowed to travel within an information system and between information 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,
        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,
    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 also administer information system access, maintenance, or implementation to include security functions.

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 information system access authorizations in support of separation of duties.
4. Divide information system testing and production functions between different individuals and/or groups.
5. Facilitate independent third-party information security testing of information 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 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, and
6. administering cryptographic keys.

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

1. security administrators,
2. system and network administrators,
3. system security officers,
4. system maintenance personnel,
5. system programmers, and
6. other privileged users.

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

Agencies shall ensure service providers require users of information 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 information system to system administrators, security administrators, system assurance groups, security groups, or other personnel or roles with approved justification.

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

Agencies shall ensure service providers:

1. Configure the information 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 to include disabling, circumventing, or otherwise altering established security safeguards and countermeasures.

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*** information systems, agencies shall ensure service providers configure the information 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, and
6. Any other specific language as required by state or federal regulations.

For ***public*** information systems, agencies shall ensure service providers configure the information 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 information 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 (https://Kentucky.gov/policies/Pages/default.aspx);
    c. be in compliance 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 age 13 and under.

AC-11 – Session Lock

Agencies shall ensure:

1. service providers configure the information system to initiate a session lock after a maximum of 15 minutes of inactivity,
2. that sessions will remain locked until the user re-establishes access using established identification and authentication procedures,
3. that users not use the session lock control as a substitute for logging out of a system,
4. that staff are responsible for maintaining the security of their assigned workstation and must lock unattended workstations, and
5. that 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 information 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 information 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, or
3. time-of-day restrictions on information 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 information 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 information 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 information system without identification and authentication,
2. document the supporting rationale for not requiring identification and authentication, and
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 of remote access (e.g., dial-up, broadband, wireless),
2. establish and document use restrictions and implementation guidance for each remote access method allowed,
    - 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.

- 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 information 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, and
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 | Automated Monitoring/Control

Agencies shall ensure service providers:

1. configure the information system to employ automated mechanisms for the monitoring and control of remote access methods, and
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, and
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 all connections traversing the Internet through Commonwealth Trust Internet Connection (TIC) technologies, and
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 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.

AC-17 (6) – Remote Access | Protection of Information

Agencies shall ensure service providers protect information about remote access mechanisms and capabilities from unauthorized use and disclosure.

AC-17 (9) – Remote Access | Disconnect / Disable Access

Agencies shall ensure service providers provide the capability to disconnect or disable remote access to information systems expeditiously, within a period no greater than 15 minutes.

AC-18 – Wireless Access

COT shall:

1. develop use restrictions, configuration and connection requirements, and implementation guidance for wireless access in Commonwealth executive branch agencies and non-executive branch agencies, and
2. authorize non-public 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, and
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, and
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 information 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:

1. deploy enterprise solutions for mobile device management (MDM) and full-disk encryption on all Commonwealth mobile computing devices such as laptops, tablets, smart phones, and similar devices, and
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.

Agencies shall ensure service providers:

1. deploy enterprise solutions for mobile device management (MDM) and full-disk encryption on all Commonwealth mobile computing devices such as laptops, tablets, smart phones, and similar devices, and
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 Information Systems

Agencies shall ensure service providers establish terms and conditions with organizations owning, operating, or maintaining external systems. Agencies shall apply terms and conditions consistently to organizations and agencies, and the terms and conditions at a minimum shall address:

1. Access to the system from external systems, and
2. Processing, storage, or transmission of agency-controlled information using external systems.

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

Agencies shall ensure service providers implement protections for external information systems according to Commonwealth directives before storing, processing, or transmitting Commonwealth information transmitted on those systems.

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

Agencies ***may*** allow the use of portable storage devices on external systems when not transferring information for storage to an external system. For example, a user may transfer a brief at a conference to the host's projection system, where the brief during the presentation is accessed through the projection system from the portable storage device. *Users shall contact help desk support to scan rewriteable devices for malware prior to accessing Commonwealth systems after such use*.

AC-20 (3) – Use of External Information Systems | Non-organizationally Owned Systems Components / Devices

Agencies shall prohibit the processing, storage, or transmission of organizational information on information systems, system components, or devices that the agencies do not own.

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 restrictions on all sensitive but unclassified information (e.g., privileged medical information, contract-sensitive information, and proprietary information), and
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, and
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-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 National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev 4. 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,
3. Retain a number of previous configurations to support rollback, as determined by the appropriate office level procedure, and
4. Issue information system components with elevated security controls to individuals traveling to locations that the agency deems to be of significant risk and apply predefined security safeguards to the devices when the individual returns.

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,
3. Retain a number of previous configurations to support rollback, as determined by the appropriate office-level procedure, and
4. Issue information system components with elevated security controls to individuals traveling to locations that the agency deems to be of significant risk, and apply predefined security safeguards to the devices when the individual returns.

CM-3 – Configuration Change Control

COT and agencies shall:

1. Determine the types of changes to an information system that are configuration-controlled,
2. Review proposed configuration changes, approve or disapprove changes—with explicit consideration for security impact analysis, and document change decisions.
3. Test, validate, and document changes prior to implementation,
4. Retain records of changes for the life of the system.
5. Audit and review activities associated with changes.
6. Coordinate and provide oversight for change control activities through the Change Advisory Board (CAB).

CM-4 – Security Impact Analysis

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

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 information system.

CM-6 – Configuration Settings

COT and agencies shall:

1. Establish, document, and implement configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements,
2. Identify, document, and approve any deviations from established configuration settings, and
3. 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 information systems to provide essential capabilities only.
2. Restrict (or prohibit) and regularly review the use of functions, ports, protocols, and services deemed unnecessary or detrimental to the system or business.
3. Disable unnecessary or non-secure ports, protocols, or services on a periodic basis.
4. Identify and document software programs that are prohibited or restricted from execution on the information system.
5. Employ an allow-all, deny-by-exception policy to prohibit unauthorized software execution, and periodically review and update the list.

CM-8 – Information System Component Inventory

Agencies shall:

1. Develop and document an inventory of information system components that:
    a. Accurately reflects the current systems for which COT and the agency is responsible, and

b. Includes all components within the authorization boundary of the system; is at the level of granularity deemed necessary for tracking and reporting; and includes information necessary to achieve effective infrastructure component accountability.
2. Review and update component inventory as an integral part of installation, removal, and updates;
3. Employ automated mechanisms to detect the presence of unauthorized hardware, software, and firmware;
4. Take action when unauthorized components are detected, such as disabling network access for such components, isolating the components, or notifying authorized points of contact; and
5. Verify that no components within the authorized boundary are duplicated in other inventories.

CM-9 – Configuration Management Plan

Agencies shall develop, document, and implement a configuration management plan for information 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 information system and ensures they align with established processes and procedures, and
4. 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, and
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.

References

- NIST Special Publication 800-12 Rev.1, *An Introduction to Information Security*
- NIST Special Publication 800-53 Rev 4, Configuration Management Control Family
- NIST Special Publication 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST Special Publication 800-100, *Information Security Handbook: A Guide for Managers*

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 National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev 4 Security and Privacy Controls for Federal Information Systems and Organizations. 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 information 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, and
5. Employ automated mechanisms to determine the state of infrastructure components with regard to flaw remediation.

Note: Security-relevant software updates include, for example: firmware, patches, service packs, hot fixes, and antivirus signatures.

SI-3 – Malicious Code Protection

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

Agencies shall:

1. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code,
2. 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 information 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
    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 information system,
5. Centrally manage malicious code protection mechanisms.
6. Ensure the information systems automatically update malicious code protection mechanisms.

SI-4 – Information System Monitoring

Agencies shall:

1. Monitor the information system to detect attacks, indicators of potential attacks and unauthorized local, network, and remote connections;
2. Identify unauthorized use of the information system and deploy monitoring devices strategically within the information 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. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
4. Heighten the level of information 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;
5. Obtain a legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, executive orders, directives, policies, or regulations,
6. Provide information system monitoring information to designated agency officials as needed,
7. Employ automated mechanisms to alert security personnel of inappropriate or unusual activities with negative security implications,
8. Implement host-based monitoring mechanisms (e.g., host intrusion prevention system (HIPS)) on information systems that receive, process, store, or transmit data; and
9. Employ automated tools to support near real-time analysis of events.

The information system shall:

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

2. 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 information system security alerts, advisories, and directives from reliable industry sources, such as the US Computer Emergency Readiness Team (US-CERT), Microsoft Safety and Security Center, 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, information system security officers, etc.; and
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. Incorporate the detection of unauthorized changes to the information system into the organizational incident response capability, and
3. Perform integrity checks of organization hardware, software, firmware, and services at startup, shutdown, and restart and on demand by the system administrator.

SI-8 – Spam Protection

Agencies shall:

1. Employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages;
2. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures;
3. Manage spam protection mechanisms centrally; and
4. Update spam protection mechanisms automatically.

SI-10 – Information Input Validation

The information 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 information system shall:

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

SI-12 – Information Handling and Retention

Agencies shall handle and retain information within the information system and information output from the system in accordance with applicable federal laws, executive Orders, directives, policies, regulations, standards, 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 4. 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 a security plan for the information system that:
    a. Is consistent with the organization enterprise architecture;
    b. Explicitly defines the authority boundary for the system;
    c. Describe the operational context of the information system in terms of missions and business processes;
    d. Provide the security categorization of the information system including supporting rationale;
    e. Describes the operational environment for the information system and relationships with or connections to other information systems;
    f. Provides an overview of the security requirements for the system;
    g. Identifies any relevant overlays, if applicable;
    h. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
    i. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.
2. Distribute copies of the security plan and communicates subsequent changes to the plan;
3. Review the security plan for the information system;
4. Update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
5. Protects the security plan from unauthorized disclosure and modification.

PL-4 – Rules of Behavior

Agencies shall:

1. Establish and make readily available to individuals requiring access to the information 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 information system;
3. Review and update the rules of behavior; and
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-8 – Information Security Architecture

Agencies shall:

1. Develop an information security architecture for the information 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 how the information security architecture is integrated; and
    c. Describe any information security assumptions about, and dependencies on external services;
2. Review and update the information security architecture changes are reflected in the security plan, the security concept of operations (CONOPS), and organizational procurements/acquisitions.

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 4. 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 information 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 an information system disruption, compromise or failure
    e. Addresses eventual full restoration of information system functionality without deterioration of security safeguards originally implemented
    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 information systems at least annually.
5. Update the contingency plan to address changes to the organization, information 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.

9. Plan for resumption of essential missions and business functions within a defined time period of contingency plan activation.
10. Identify critical information systems assets supporting essential missions and business functions.

CP-3 – Contingency Training

Agencies shall provide contingency training to information system users consistent with assigned roles and responsibilities upon users assuming a contingency role or responsibility or when required by information system changes, and annually thereafter

CP-4 – Contingency Plan Testing

Agencies shall:

1. Test their contingency plan for each information 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.
4. Coordinate contingency plans for information 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 information system backup information.
2. Ensure that the alternate storage site provides information security safeguards equivalent to that of the primary site.
3. 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.).
4. 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 information 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 information security safeguards equivalent to those at the primary site.
4. 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.

5. Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster, and outline explicit mitigation actions.
6. 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:

1. Establish alternate telecommunication services including necessary agreements to permit the resumption of organization's information 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.
2. Develop primary and alternative telecommunication service agreements that include priority-of-service provisions that match organization availability requirements, including RTOs.
3. Procure alternate (redundant) telecommunication services to reduce the likelihood of a single point of failure.

CP-9 – Information 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 security-related documentation consistent with the defined frequency in the organization's contingency plan.
4. Protect the confidentiality, integrity, and availability of backup information at storage locations.
5. Test backup media and equipment at an organization-defined interval to ensure and verify media reliability and information integrity.

CP-10 – Information System Recovery and Reconstitution

Agencies shall:

1. Provide for the recovery and reconstitution of critical information systems to a known state after a disruption, compromise, or failure.
2. Include systems that are transaction-based such as database management systems and transaction processing systems, and activities such as transaction journaling and rollback.

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 4. 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 information 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 information system through a network, whether external (e.g., the internet) or internal (e.g., LAN).

MA-2 – Controlled Maintenance

For Commonwealth information systems, agencies shall:

1. schedule, perform, document, and review records of maintenance and repairs on information 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 information system or system components from organizational facilities for off-site maintenance or repairs,
4. sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs,
5. check all security controls potentially affected by maintenance to verify that the controls are still functioning properly following maintenance, and
6. maintain information 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

For Commonwealth information systems, agencies shall approve, control, and monitor information system maintenance tools.

MA-4 – Nonlocal Maintenance

For Commonwealth information systems, 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 information 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,
    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, and
5. terminate session and network connections after completing nonlocal maintenance.

MA-5 – Maintenance Personnel

For Commonwealth information systems, 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 information 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, and
5. ensure that non-escorted personnel performing maintenance activities not directly associated with the information system—but in the physical proximity of the system—have the required access authorizations.

MA-6 – Timely Maintenance

For Commonwealth information systems, agencies shall obtain maintenance support and spare parts for information systems and their components within an agency-defined period as outlined in the information 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 4 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, and
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 information 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. Provide security safeguards to control access to areas within the facility officially designated as publicly accessible,
4. Escort visitors and monitor visitors 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 Medium

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

PE-5 – Access Control for Output Devices

Agencies shall control physical access to an information system's 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 information 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, and
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 information system resides, and
2. Review visitor access records monthly.

PE-9 – Power Equipment and Cabling

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

PE-10 – Emergency Shutoff

Agencies shall:

1. Provide the capability of shutting off power to the information 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, and
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 information system or transition of the information 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 information 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 employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

PE-14 – Temperature and Humidity Controls

Agencies shall:

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

PE-15 – Water Damage Protection

Agencies shall protect the information 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 authorize, monitor, and control all information system entering and exiting the facility and maintains records of those items.

PE-17 – Alternate Work Site

Agencies shall:

1. Employ appropriate management , operational, and technical information system security controls at alternate work sites,
2. Assess, as feasible, the effectiveness of security controls at alternate work site, and
3. 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 4, Security and Privacy Controls for Federal Information Systems and Organizations. 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, and
3. Review and update position risk designations.

PS-3 – Personnel Screening

Agencies shall:

1. Screen individuals prior to authorizing access to the information system, and
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 information system access within organization-defined period of time,
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 information system-related property,
5. Retain access to organizational information and information systems formerly controlled by terminated individual,
6. Notify the agency personnel in charge within a certain period, and
7. Notify the terminated individual of applicable requirements addressing the protection of confidential information.

PS-5 – Personnel Transfer

Agencies shall:

1. Review and confirm ongoing operational need for current logical and physical access authorizations to information 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, and
4. Notify agency personnel within an agency-defined period.

PS-6 – Access Agreements

Agencies shall:

1. Develop and document access agreements for organizational information systems,
2. Review and update the access agreements, and
3. Ensure that individuals requiring access to organizational information and information systems:
    a. Sign appropriate access agreements prior to being granted access; and
    b. Re-sign access agreements to maintain access to organizational information 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 information system privileges within a period of time, and
5. Monitor provider compliance.

PS-8 – Personnel Sanctions

Agencies shall:

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

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 National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations. 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 requirements for the information system or information system service in mission/business process planning,
2. Determine, document, and allocate the resources required to protect the information system or information system service as part of its capital planning and investment control process, and
3. Establish a discrete line item for information security in organizational programming and budgeting documentation.

SA-3 – System Development Life Cycle

Agencies shall:

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

SA-4 – Acquisition Process

The agency shall:

1. Include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system

service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

- Security functional requirements,
- Security strength requirements,
- Security assurance requirements,
- Security-related documentation requirements,
- Requirements for protecting security-related documentation,
- Description of the information system development environment and environment in which the system is intended to operate, and
- Acceptance criteria.

2. Require the developer of information system, system component, or information 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.
3. Require the developer of information system, system component, or information system service to identify early in the SDLS the functions, ports, protocols, and services.

SA-5 – Information System Documentation

Agencies shall:

1. Obtain administrator documentation for the information system, system component, or information system service that describes:
    a. Secure configuration, installation, and operation of the system, component, or service,
    b. Effective use and maintenance of security functions/mechanism, and
    c. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.
2. Obtain user documentation for the information system, system component, or information system service that describes:
    a. User-accessible security functions/mechanisms and how to effectively use those security functions/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.
3. Document attempts to obtain information system, system component, or information 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 Engineering Principles

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

SA-9 – External Information System Services

Agencies shall:

1. Require that providers of external information system services comply with organizational information security requirements and employ security 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 with regard to external information system services; and
3. Employ Service Level Agreements (SLAs) to monitor security control compliance by external service providers on an ongoing basis.
4. Require providers of external information 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 information system, system component, or information system service to:

1. Perform configuration management during system, component, or service (development, implementation, 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 impacts of such changes, and
5. Track security flaws and flaw resolution within the system, component, or service and report findings.

SA-11 – Developer Security Testing and Evaluation

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

1. Create and implement a security assessment plan,
2. Perform integration, system, regression testing, and evaluation,
3. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation,
4. Implement a verifiable flaw remediation process, and
5. Correct flaws identified during security testing/evaluation.

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 National Institute of Standards and Technology (NIST) NIST Special Publication 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations. 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 information system separates user functionality, including user interface services, from information system management functionality.

SC-4 – Information in Shared Resources

Agencies shall ensure the information 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 information systems.

SC-5 – Denial of Service Protection

Agencies shall ensure the information system protects against, or limits the effects of denial of service attacks.

SC-7 – Boundary Protection

Agencies shall ensure the information system must:

1. Monitor and control communications at the external boundary of the system and at key internal boundaries 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 information systems through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture,

4. Implement a managed interface for each external telecommunication server,
5. Establish traffic flow policies for each managed interface,
6. Document each exception to the traffic flow policy with a supporting business need and duration of the need,
7. Review exceptions to the traffic flow policy annually and remove exceptions that are no longer supported by a business need, and
8. 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-8 – Transmission Confidentiality and Integrity

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

SC-10 – Network Disconnect

Agencies shall ensure the information 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 information system.

SC-13 – Cryptographic Protection

Agencies shall ensure information systems 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

The agency shall ensure the information system:

1. Prohibits remote activation of collaborative computing devices, and
2. Provides an explicit indication of use to users physically present at the devices.

SC-17 – Public Key Infrastructure Certificates

Agencies shall obtain or issue public key certificates from an approved service provider.

SC-18 – Mobile Code

Agencies shall:

1. Define acceptable and unacceptable mobile code and mobile code technologies,
2. Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies, and
3. Authorize, monitor, and control the use of mobile code within the information system.

SC-19 – Voice over Internet Protocol

Agencies shall:

1. Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
2. Authorize, monitor, and control the use of VoIP within the information system.

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

Agencies shall ensure the information 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, and
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 information 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 information 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 information system protects the authenticity of communication sessions.

SC-28 – Protection of Information at Rest

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

SC-39 – Process Isolation

The agency shall ensure information 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 National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev 4. 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-1 – Audit and Accountability Policy and Procedures

COT shall develop, document, and disseminate to agencies:

1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
2. Procedures to facilitate the implementation of the audit and accountability policy as well as associated controls.

COT shall review and update the policy and procedures at a frequency defined within those documents.

AU-2 – Audit Events

COT and agencies shall:

1. Determine that the information system is capable of auditing defined events.
2. Coordinate the security audit function with other organization entities requiring audit-related information, to enhance mutual support and to help guide the selection of auditable events.
3. Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.
4. Determine the events, their frequency, and as applicable, the situation requiring the auditing for each defined event.

AU-3 – Content of Audit Records

The information system shall generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of the users or system associated with the event.

AU-4 – Audit Storage Capacity

COT shall work with the agency to determine and allocate audit storage capacity.

AU-5 – Response to Audit Processing Failures

The information system shall:

1. Provide alerts in the event of audit processing failure.
2. Take any other appropriate actions that may be defined.

AU-6 – Audit Review, Analysis, and Reporting

COT along with the agency shall review and analyze information system audit records and report the findings to appropriate personnel.

AU-7 – Audit Reduction and Report Generation

The information system shall provide an audit reduction and report generation capability that:

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

AU-8 – Time Stamps

The information 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 information system shall protect audit information and audit tools from unauthorized access, modification, or deletion. Audit information shall include all information needed to audit information system activity successfully.

AU-11 – Audit Record Retention

COT shall retain audit records as agreed upon with the agency or as required by regulatory and records retention requirements.

AU-12 – Audit Generation

The information 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.

AU-13 – Monitoring for Information Disclosure

COT along with the agency shall monitor the audit records for evidence of unauthorized disclosure of organization information.

AU-14 – Session Audit

The information system shall provide the capability, where appropriate and possible, for authorized users to select a user session to capture and record.

AU-15 – Alternate Audit Capability

COT shall provide an alternate audit capability in the event of a failure in primary audit capability.

AU-16 – Cross-Organization Auditing

COT and agencies shall capture audit record requests to external organizations. COT and agencies shall make sure that auditable events can be coordinated across internal and external COT and vendor assets.

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 4. 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 – Security Assessments

Agencies shall:

1. Develop a security assessment plan that describes the scope of the assessment including:
    a. Security controls and control enhancements under assessment;
    b. Assessment procedures to be used to determine security control effectiveness; and
    c. Assessment environment, assessment team, and assessment roles and responsibilities;
2. Assess the security controls in the information system and its environment of operation annually, upon major information 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;
3. Produce a security assessment report that documents the results of the assessment; and
4. Provide the result of the security control assessments.

CA-3 – System Interconnections

Agencies shall:

1. Authorize connection from the information system to other information systems through the use of Interconnection Security Agreements (ISA);
2. Document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
3. Review and update Interconnection Security Agreements on an ongoing basis.
4. Employ a permit-by-exception policy for allowing information systems to connect to external information systems.

CA-5 – Plan of Action and Milestones

Agencies shall:

1. Develop a plan of action and milestones for the information 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; and
2. Update existing plan of action and milestones based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

CA-6 – Security Authorization

Agencies shall:

1. Assign a senior-level executive or manager as the authorizing official for the information system;
2. Ensure that the authorizing official authorizes the information system for processing before commencing operations; and
3. Update the security authorization on annual basis.

CA-7 – Continuous Monitoring

Agencies shall develop a continuous monitoring program that includes:

1. A configuration management process for the information asset and its constituent components;
2. Establishment of ongoing monitoring for assessments;
3. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
4. Ongoing security status monitoring;
5. Correlation and analysis of security-related information generated by assessments and monitoring;
6. Response actions to address results of the analysis of security-related information; and
7. Reporting the security status of the agency and the information system on regular basis.

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 National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev 4 *Security and Privacy Controls for Federal Information Systems and Organizations* 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.

Security 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 – Security Awareness Training

COT shall provide basic security awareness training content for all users within the enterprise. This training will be provided as part of the initial training for new users, as required by system changes, and at least once annually.

Specifically, COT shall develop, document, and communicate a security awareness and training program that addresses purpose, scope, roles, responsibilities, management commitment, and compliance, as well as communicating procedures to facilitate the implementation of the CIO-121 Security Awareness and Training Policy and associated training controls.

AT-3 – Role-Based Security Training

All executive branch agencies and non-executive branch agencies using COT-managed infrastructure or services shall provide role-based security training to personnel with assigned security roles and responsibilities before access is given to information systems and as required by system changes.

AT-4 – Security Training Records

All executive branch agencies and non-executive branch agencies using COT-managed infrastructure or services shall document and monitor security training activities including basic security awareness training and specific information 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 4. 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 information 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:

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

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

Agencies and service providers shall ensure that information systems and users implement multifactor authentication (MFA) for network access to privileged accounts. Agencies and providers shall require use of separate accounts for elevated privileges, and shall prohibit distribution of system ID credentials (unique identifiers) to non-privileged users. A system ID is an account used by applications, systems, or automated processes with no direct user access or login.

- Systems that contain CONFIDENTIAL information as outlined in the Commonwealth's ENT-101: Enterprise Data Classification Standard shall require ***physical*** MFA devices. CONFIDENTIAL data is that which must be kept private under federal, local, or state laws, or contractual agreements, or to protect its proprietary value, or must be kept private for any combination of these reasons.

- Multifactor authentication solutions shall be placed as close as possible to the protected data or asset.
- System ID credentials shall meet all complexity requirements of elevated privilege accounts as outlined in the COT-156 Password Management Process. For more information about these requirements, please contact the Office of the CISO.
- Users shall not store or remember privileged account credentials or allow for automatic login.

Agencies and providers shall prohibit non-expiring system ID passwords unless expiration would cause a demonstrated negative impact on system functionality. When used, non-expiring passwords may only be used for system, application, or service accounts with no direct user access. The non-expiring passwords shall meet or exceed complexity requirements for elevated privilege accounts.

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

Agencies and service providers shall ensure that information systems and users implement multifactor authentication (MFA) for network access to privileged accounts. Agencies and providers shall require use of separate accounts for elevated privileges and shall prohibit distribution of system ID credentials to non-privileged users.

- Systems that contain CONFIDENTIAL information as outlined in the Commonwealth's ENT-101: Enterprise Data Classification Standard shall require at least ***software*** MFA devices. CONFIDENTIAL data is that which must be kept private under federal, local, or state laws, or contractual agreements, or to protect its proprietary value, or must be kept private for any combination of these reasons.
- Multifactor authentication solutions shall be placed as close as possible to the protected data or asset.
- System ID credentials shall meet all complexity requirements of elevated privilege accounts as outlined in COT-156 Password Management Process. For more information about these requirements, please contact the Office of the CISO.
- Users shall not store or remember privileged account credentials or otherwise allow for automatic login.

Agencies and providers shall prohibit non-expiring system ID passwords unless expiration would cause a demonstrated negative impact on system functionality. When used, non-expiring passwords may only be used for system, application, or service accounts with no direct user access. The non-expiring passwords shall meet or exceed complexity requirements for elevated privilege accounts.

IA-2 (3) – Identification and Authentication (Organizational Users) | Local Access to Privileged Accounts

Agencies and service providers shall ensure that information systems and users implement multifactor authentication for local access to privileged accounts.

- Administrators shall use physical or virtual MFA to access privileged accounts.
- COT prohibits non-administrators from local access to privileged accounts.

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

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

IA-2 (11) – Identification and Authentication (Organizational Users) | Remote Access - Separate Device

Agencies and service providers shall implement multifactor authentication for remote access to privileged and non-privileged accounts, such that one of the factors is provided by an authorized device separate from the system gaining access. This device must adhere to encryption standards in the Commonwealth's Kentucky Information Technology Standards (KITS).

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

Agencies and service providers may allow information systems to accept and use Personal Identity Verification (PIV) credentials, provided the PIV credentials adhere to KITS.

IA-3 – Device Identification and Authentication

Information 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 information systems manage identifiers such as MAC addresses, TCP/IP addresses, usernames, and computer names such that:

- only COT authorizes assigning individual, group, role, or device identifiers,
- identifiers uniquely distinguish an individual, group, role, or device,
- identifiers are assigned to the correct, intended individual, group, role, or device,
- systems and agencies shall prevent reuse of identifiers for a minimum of 24 hours, and
- systems shall disable the identifier after 90 days of inactivity.

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. For more information about these requirements, please contact the Office of the CISO.

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. For more information about these requirements, please contact the Office of the CISO.

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

Agencies and service providers shall ensure that the information 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 (3) – Authenticator Management | In-Person or Trusted Third-Party Registration

Agencies and service providers shall require that only authorized Agency Contacts can request unique identifiers (credentials), and that authorized Agency Contacts shall confirm the user or system identity prior to releasing identifier information to that user.

IA-5 (11) – Authenticator Management | Hardware Token-Based Authentication

Agencies and service providers shall ensure that information systems, for hardware token-based authentication, employ mechanisms that adhere to KITS.

IA-6 – Authenticator Feedback

Agencies and service providers shall ensure that information 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 information 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 information 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 ensure that information systems accept and electronically verify PIV credentials from other federal agencies.

IA-8 (2) – Identification and Authentication (Non-Organizational Users) | Acceptance of Third-Party Credentials

Agencies and service providers shall ensure that information systems only accept third-party credentials that meet FICAM-approved standards.

IA-8 (3) – Identification and Authentication (Non-Organizational Users) | Use of FICAM-Approved Products

When agencies and providers use FICAM-approved credentials, they shall also use FICAM-approved products and shall employ only FICAM-approved system components to accept the third-party credentials.

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

The information systems shall conform to FICAM-issued profiles.

Identification and Authentication Best Practices

(This space reserved for best practices)

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