Shared Administrative Services | Office of State Technology

State Cybersecurity Office

Standard Title: Access Control Standard
Standard Version: 1.1
Effective Date: 12/19/2022
Review Date: 7/15/2025

---

1. Purpose

The purpose of this standard is to establish the rules and processes for creating, maintaining, and controlling the access of a digital identity to an entity's applications and resources for means of protecting their systems and information.

This standard covers all systems developed by, or on behalf of the Arkansas Office of State Technology (OST), that require authenticated access. This includes all development, test, quality assurance, production and other ad hoc systems.

2. Applicability

This standard applies to all systems managed by the Arkansas OST Data Centers that store, process, or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

Notations of specific control items (e.g., CMS, CJIS, FTI, PCI) only pertain to the systems that are required to comply with such regulations.

3. Definitions

Refer to the State Cybersecurity Office (SCSO) Regulatory Definitions document.

4. Standard

Account management and access control includes the process of requesting, creating, issuing, modifying and disabling user accounts; enabling and disabling access to resources and applications; establishing conditions for group and role membership; tracking accounts and their respective access authorizations; and managing these functions.

4.1 Account Management AC-2 (NIST Moderate Control)

As defined in the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet:

a. Remove or disable default user accounts.
b. Rename active default accounts.
c. Implement centralized control of user access to administrator functions, where possible.
d. Regulate the access provided to contractors and define security requirements for contractors.
e. Notify account managers according to the posted SCSO Regulatory Settings spreadsheet timeframe when temporary accounts are no longer required or when information system users are terminated or transferred or information system usage or need-to-know/need-to-share changes.
f. Prohibit use of guest, anonymous, and shared accounts for providing access to sensitive data (see SS-70-001).
g. Prior to granting access to PII, users demonstrate a need for the PII in the performance of the user's duties.
h. Implement access controls within the information system based on users' or user group's need for access to PII in the performance of their duties.
i. Organizations should provide access only to the minimum amount of PII necessary for users to perform their duties.
j. Create, enable, modify, disable, and remove information system accounts in accordance with the requirement for each user to complete according to the SCSO Regulatory Settings spreadsheet training required by the State Cybersecurity Office (SCSO) and external regulators.

4.2 Automated System Account Management AC-2(1) (NIST Moderate Control)

a. Automated mechanisms must be employed to monitor the use and management of accounts. These mechanisms must allow for usage monitoring and notification of atypical account usage. Thresholds for alerting should be set based on the criticality of the system or assurance level of the account.
b. Staff in the appropriate account management/access control role(s) must be notified, as defined in the SCSO Regulatory Settings spreadsheet when account management activities occur, such as, accounts are no longer

required, users are terminated or transferred, or system usage or need-to-know changes. This should be automated where technically possible.

c. Automated access control policies that enforce approved authorizations for information and system resources must be in place within systems. These access control polices could be identity, role or attribute based.
d. By default, no one has access unless authorized.

4.3 Automated Temporary and Emergency Account Management AC-2(2) (NIST Moderate Control)

a. Temporary accounts are intended for short-term use and include restrictions on creation, point of origin, usage (i.e., time of day, day of week), and must have start and stop dates. An entity may establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation, such as for vendors, manufacturers, etc. These accounts must have strictly limited permissions and access only to the systems required. Temporary accounts must be automatically disabled as defined in the SCSO Regulatory Settings spreadsheet.
b. Emergency Accounts are intended for short-term use and include restrictions on creation, point of origin, and usage (i.e., time of day, day of week). SEs may establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency accounts must be automatically disabled as defined in the SCSO Regulatory Settings spreadsheet.

4.4 Disable Accounts AC-2(3) (NIST Moderate Control)

a. De-provisioning Upon Separation: All user accounts (including privileged) must be disabled as defined in the SCSO Regulatory Settings spreadsheet. In addition, credentials must be revoked in accordance with organizational requirements, and access attributes must be removed. Self-service mechanisms may not be used to re-enable the account.
b. Inactivity Disable: When an account is disabled due to inactivity, access attributes may remain unchanged if deemed appropriate by the information owner.

4.5 Automated Audit Actions AC-2(4) (NIST Moderate Control)

a. All account activity must be logged and audited in accordance with the Standard Audit and Logging document.
b. The ability to modify or delete audit records shall only be allowed with CISO review and approval.
c. Any modification to access attributes must be recorded and traceable to a single individual.

4.6 Inactivity Logout AC-2(5) (NIST Moderate Control)

a. Sessions must be locked after a maximum inactivity period according to the posted SCSO Regulatory Settings spreadsheet timeframe. Session inactivity locks are temporary actions taken when users stop work and move away from their immediate vicinity but do not want to log out because of the temporary nature of their absences. Users must re-authenticate to unlock the session.

4.7 Privileged User Accounts AC-2(7) (CJIS Specific Control)

a. A privileged account is an account which provides increased access and requires additional authorization. Examples include a network, system or security administrator account. A privileged account may only be provided to members of the workforce who require it to accomplish their job duties. The use of privileged accounts must be compliant with the principle of least privilege. Access will be restricted to only those programs or processes specifically needed to perform authorized business tasks and no more. There are two privileged account types - Administrative Accounts and Default Accounts.
b. Administrative Accounts: Accounts given to a user that allow the right to modify the operating system or platform settings, or those which allow modifications to other accounts. These accounts must:
    1. be at an Identity Assurance Level commensurate with the protected resources to which they access.
    2. not have user-IDs that give any indication of the user's privilege level, e.g., supervisor, manager, administrator, or any flavor thereof.
    3. be internally identifiable as an administrative account per a standardized naming convention.
    4. be revoked in accordance with organizational requirements

c. Default Privileged Accounts: Default privileged accounts (e.g., root, Administrator) are provided with a particular system and cannot be removed without affecting the functionality of the system. Default privileged accounts must:
    1. be disabled if not in use or renamed if technically possible.
    2. only be used for the initial system installation or as a service account. When technically feasible, alerts must be issued to the appropriate personnel when there is an attempt to log-in with the account for access.
d. Service Accounts: A special type of privileged account, specifically used for non-human interaction, to execute applications and run automated services, virtual machine instances, and other types of processes.
e. not use the initial default password provided with the system.
f. have password known or accessible by at least two individuals within OST Support, if password is known by anyone. As such, restrictions for shared accounts, outlined below, must be followed.

4.8 Disable Accounts for High-Risk Individuals AC-2(13) (NIST Moderate Control)

a. Event/Risk Based (Administrative Disable): When an account poses or has the potential to pose a significant risk, either the account is disabled and/or access attributes are removed upon discovery of the risk.
b. An account identifier is required to distinguish these accounts and prevent inappropriate re-enabling of the account/access.
c. Re-enabling requires explicit approval from OST management.
d. Self-service mechanisms may not be used to re-enable disabled account.

4.9 Access Enforcement AC-3 (NIST Moderate Control)

a. The information systems shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.
b. Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration

functions (system administrators, information system security officers, maintainers, system programmers).

c. Access control policies (identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information systems.

4.10 Discretionary Access Control AC-3(4) (CJIS Specific Control)

a. Agencies shall control access to CJI based on one or more of the following criteria:
    1. Job assignment or function (i.e., the role) of the user seeking access
    2. Physical location
    3. Logical location
    4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
    5. Time-of-day and day-of-week/month restrictions

4.11 Security-relevant Information AC-3(5) (CJIS Specific Control)

a. The information system shall enforce assigned authorizations for controlling access to the system and contained information as defined in the SCSO Regulatory Settings spreadsheet.
b. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

4.12 Information Flow Enforcement AC-4 (NIST Moderate Control)

a. OST shall deploy mechanisms to control access to the State's network backbone and/or routed infrastructure.
b. The State Network must be configured to monitor and control communications at the external boundary of the network and internal boundaries at strategic locations.
c. The State Network must connect to external networks or information systems only through managed interfaces approved by OST management. These managed interfaces must consist of boundary protection devices

(e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels, web content filters, data loss prevention) arranged in accordance with an effective security architecture.

d. Protective controls shall at a minimum include the following:
    1. Source and destination address checking to restrict rogue networks from manipulating the State's routing tables.
    2. Authentication to ensure that routing tables do not become corrupted with false entries.
    3. Use network address translation (NAT) to obfuscate internal network addresses.
    4. Encryption when sensitive or confidential data is passed across the public network.

4.13 Separation of Duties AC-5 (NIST Moderate Control)

a. Audit functions must not be performed by security personnel responsible for administering access control.
b. Maintain a limited group of administrators with access based upon roles and responsibilities.
c. The critical mission functions and information system support functions are divided among separate individuals.
d. The information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions must be divided among separate individuals.
e. An independent entity, not the Business Owner, System Developer(s)/Maintainer(s), or System Administrator(s) responsible for the information system, conducts information security testing of the information system.
f. Assign accounts and authenticators in accordance with user roles and responsibilities.
g. Configure the system to request user ID and authenticator prior to system access.

4.14 Least Privilege AC-6 (NIST Moderate Control)

a. Disable all file system access not explicitly required for system, application, and administrator functionality.

b. Contractors must be provided with minimal system and physical access and must agree to and support the organizational security requirements. The contractor selection process must assess the contractor's ability to adhere to and support the organization's security policy.
c. Restrict the use of database management utilities to only authorized database administrators. Prevent users from accessing database data files at the logical data view, field, or field-value level. Implement table-level access control.
d. Ensure that only authorized users are permitted to access those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of job duties.
e. Disable all system and removable media boot access unless it is explicitly authorized by the OST CISO for compelling operational needs. If system and removable media boot access is authorized, boot access is password protected.

4.15 Authorize Access to Security Functions AC-6(1) (NIST Moderate Control)

a. Account administrators are an optional subset of the account manager role. They do not determine procedures. System rights and/or responsibilities are assigned to them by the account manager. All account administrator responsibilities are contained within the role of account manager should an account administrator not exist. A subset of account administrator duties may be assigned as appropriate. For example, a role for password reset only may exist for service desk employees. Additionally, some of these responsibilities may remain with the account manager should that manager determine it is necessary. For account management, the administrator may:
    1. Maintain any necessary information supporting account administration activities, including account management requests and approvals.
    2. Enroll new users.
    3. Enable/disable user accounts.
    4. Create and maintain user roles and groups.
    5. Assign rights and privileges to a user or group.
    6. Collect data to periodically review user accounts and their associated rights.

7. Assign new authentication tokens (e.g., password resets).

4.16 Non-privileged Access for Non-security functions AC-6(2) (NIST Moderate Control)

a. The default non-privileged account (guest or anonymous user) is an account for people who do not have individual accounts. An example of where this might be necessary is on a public Wi-Fi network. This account type must:
    1. be disabled until necessary
    2. have limited rights and permissions.
    3. only be allowed after a risk assessment
    4. have compensatory controls that include restricted network access.
    5. be assigned a password that the user cannot change but that is according to the SCSO Regulatory Settings spreadsheet, by an administrator
    6. not allow the account to be assigned for delegation by another account.
    7. have a log maintained of users to whom the password is given.

4.17 Privileged Accounts AC-6(5) (NIST Moderate Control)

a. Default privileged accounts (e.g., root, Administrator) are provided with a particular system and cannot be removed without affecting the functionality of the system. Default privileged accounts must:
    1. be disabled if not in use or renamed if technically possible.
    2. only be used for the initial system installation or as a service account. When technically feasible, alerts must be issued to the appropriate personnel when there is an attempt to log-in with the account for access.
    3. not use the initial default password provided with the system.
    4. have password known or accessible by at least two individuals within OST, if password is known by anyone. As such, restrictions for shared accounts, outlined below, must be followed.

4.18 Review of User Privileges AC-6(7) (NIST Moderate Control)

a. Information owners must review all accounts as defined in the SCSO Regulatory Settings spreadsheet to determine if they are still needed.

b. Access to privileged accounts must be reviewed according to the SCSO Regulatory Settings spreadsheet to determine whether or not they are still needed.
c. Information owners must review account authorizations and/or user access assignments according to the SCSO Regulatory Settings spreadsheet to determine if all access is still needed.
d. Accounts or records of the account must be archived after inactivity defined by the according to the posted SCSO Regulatory Settings spreadsheet timeframe or after specific audit purposes are met.
e. Reviewers must ensure that any needed changes to address incorrect account rights are made in a timely manner.

4.19 Log Use of Privileged Functions AC-6(9) (NIST Moderate Control)

a. All account activity must be logged and audited in accordance with the Audit and Logging Standard.
b. The ability to modify or delete audit records must be limited to a subset of privileged accounts.
c. Any modification to access attributes must be recorded and traceable to a single individual

4.20 Prohibit Non-privileged Users from Executing Privileged Functions AC-6(10) (NIST Moderate Control)

a. Prohibit non-privileged users from executing privileged functions Privileged functions include disabling, circumventing or altering security or privacy controls, establishing system accounts, performing integrity checks and administering cryptographic keys.

4.21 Unsuccessful Logon Attempts AC-7 (NIST Moderate Control)

a. Configure the information system to lock out the user account automatically according to the posted SCSO Regulatory Settings spreadsheet; and
b. Automatically locks the account/node until released by an administrator or delays next logon prompt. The control applies whether the login occurs via a local or network connection.

4.22 System Use Notification AC-8 (NIST Moderate Control)

a. The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules.
b. The system use notification message shall, at a minimum, provide the following information:
    1. The user is accessing a restricted information system.
    2. System usage may be monitored, recorded, and subject to audit.
    3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
    4. Use of the system indicates consent to monitoring and recording
c. The System Owner determines elements of the environment that require the System Use Notification control.
d. The System Owner determines how System Use Notification will be verified and provides appropriate periodicity of the check.
e. In a cloud environment, if not performed as part of a Configuration Baseline check, the organization has a documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider.

4.23 Previous Logon Notification AC-9 (CJIS Specific Control)

a. Notify user upon initial login of date and time of last successful login

4.24 Concurrent Session Control AC-10 (NIST High Control – CJIS, PCI)

a. Multiple active sessions for all account types are prohibited for those accessing confidential CJI or PCI data. Also see SCSO Regulatory Settings spreadsheet.

4.25 Device Lock AC-11 (NIST Moderate Control)

a. A session lock will be initiated according to the posted SCSO Regulatory Settings spreadsheet timeframe of inactivity.
b. The session lock will require the user to re-establish access using standard identification and authentication.

4.26 Pattern-Hiding Displays AC-11(1) (NIST Moderate Control)

a. Conceal via device lock all information previously viewable on the screen.

b. The pattern-hiding display can include static or dynamic images, such as patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen with the caveat that controlled unclassified information is not displayed.

4.27 Session Termination AC-12 (NIST Moderate Control)

a. The information system will automatically terminate a user-initiated session, when communicating through an external, non-OST network, according to the posted SCSO Regulatory Settings spreadsheet timeframe.

4.28 Session Termination AC-12(1) (CJIS Specific Control)

a. The information system will provide a logout capability for user-initiated communications sessions (local or remote) whenever authentication is used to gain access to systems accessing CJI data.

4.29 Session Termination AC-14(NIST Moderate Control)

a. The data owner may determine that no identification and authentication is required for specific information systems. (This control does not apply to situations where identification and authentication have already occurred and are not being repeated).
b. Sensitive or confidential data (FTI, CJI, PCI, CMS, FERPA, SSA) may not be disclosed without identification and authentication.
c. Users may access public websites or publicly available information on accessible State information systems without identification and authentication.
d. The data owner must identify, provide justification, and develop supporting documentation for user actions that can be performed on systems not requiring identification and authentication.
e. Justification must specify the following:
    1. Actions that can be performed on the information system without identification and authentication may be permitted only to the extent necessary to accomplish Mission/Business Objectives.
    2. Identification of responsible person for ensuring access control and monitoring is conducted.
    3. Supporting rationale for not requiring identification and authentication

f. Implement compensating security controls at the directory and file level for all application specific and system accounts which do not require passwords.
g. Implement only using least privilege, with access given only to necessary directories and files.

4.30 Security and Privacy Attributes AC-16 (PCI Specific Control)

a. PCI Data Owners will provide the means to associate defined types of security and privacy attributes with defined security and privacy attribute values for information in storage, in process, and/or in transmission; (Establish, implement, and maintain a record classification scheme)
b. Ensure that the attribute associations are made and retained with the information
c. Audit changes to attributes; and
d. PCI Data Owner shall review attributes for applicability annually

4.31 Remote Access AC-17 (NIST Moderate Control)

a. Require callback capability with re-authentication to verify connections from authorized locations when the Multi-Protocol Label Switching (MPLS) service network cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor will be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems will be authorized and logged. User IDs assigned to vendors will be recertified according to the posted SCSO Regulatory Settings spreadsheet timeframe.
b. If re-authentication is implemented as a remote access solution or associated with remote access, refer to the most recent NIST SP 800-63.
c. All computers and devices, whether organization-furnished equipment or contractor-furnished equipment, that require any network access to a network or system are securely configured and meet at a minimum, the following security requirements:
    1. Up-to-date system patches.
    2. Current anti-virus software.
    3. Host-based intrusion detection system.
    4. Functionality that provides the capability for automatic execution of code disabled; and

5. Employs required encryption (FIPS 140-2 validated module).

d. When utilizing remote access (including teleworking), ensure NIST SP 800-46 guidelines are followed by defining policies and procedures that define:
    1. Forms of permitted remote access.
    2. Types of devices permissible for remote access.
    3. Type of access remote users are granted; and
    4. How remote user account provisioning is handled.
e. Remote connection for privileged functions must be performed using multi-factor authentication.

4.32 Monitoring and Control AC-17(1)

a. Any method of remote access must use a centrally managed authentication system for administration and user access.
b. Devices and software used for remote access must be approved after review by the State Cybersecurity Office. Blanket approvals may be provided based on this review.
c. The authentication token used for remote access must conform to the requirements of the appropriate assurance level.
d. Remote access sessions must require re-authentication according to the posted SCSO Regulatory Settings spreadsheet timeframe of inactivity.
e. Remote access sessions will be configured according to the posted SCSO Regulatory Settings spreadsheet timeframe.
f. The entity must monitor for unauthorized remote connections and other anomalous activity and take appropriate incident response action as per the *Cyber Incident Response Standard*.

4.33 Protection of Confidentiality and Integrity Using Encryption AC-17(2) (NIST Moderate Control)

a. All remote systems and connections must implement current encryption standards for in transit traffic.

4.34 Managed Access Control Points AC-17(3) (NIST Moderate Control)

a. All remote connections will be routed through an organization defined number of remote access control points

4.35 Privileged Commands and Access AC-17(4) (NIST Moderate Control)

a. OST shall authorize the execution of privileged commands and access to security-relevant information (e. g. logging into a firewall device for administrative functions).
    1. Remote access under these conditions shall be authorized only for compelling operational needs and the agency shall document the rationale for such access.
    2. All activity shall be logged and audited as defined in the SCSO Regulatory Settings spreadsheet.

4.36 Protection of Mechanism Information AC-17(6) (CJIS Specific Control)

a. OST shall control all remote accesses through managed access control points. OST may permit remote access for privileged functions only for compelling operational needs but shall document the technical and administrative process for enabling remote access for privileged functions in the security plan for the information system.
b. Virtual escorting of privileged functions is permitted only when all the following conditions are met:
    1. The session shall be monitored at all times by an authorized escort
    2. The escort shall be familiar with the system/area in which the work is being performed.
    3. The escort shall have the ability to end the session at any time.
    4. The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.
    5. The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session

4.37 Wireless Access AC-18 (NIST Moderate Control)

a. If wireless access is explicitly authorized, wireless device service set identifier broadcasting is disabled and the following wireless restrictions and access controls are implemented:
    1. Encryption protection is enabled;
    2. Access points are placed in secure areas;

3. Access points are shut down when not in use (i.e., nights, weekends);
4. A stateful inspection firewall is implemented between the wireless network and the wired infrastructure;
5. MAC address authentication is utilized;
6. Static IP addresses, not Dynamic Host Configuration Protocol (DHCP), is utilized
7. Personal firewalls are utilized on all wireless clients;
8. File sharing is disabled on all wireless clients;
9. Intrusion detection agents are deployed on the wireless side of the firewall;
10. Wireless activity is monitored and recorded, and the records are reviewed on a regular basis;

b. Adheres to the IEEE 802.11 Wireless Local Area Network (WLAN). Wireless printers and all Bluetooth devices such as keyboards are not allowed.

4.38 Authentication and Encryption AC-18(1) (NIST Moderate Control)

a. Users and systems must be authenticated
b. Implement FIPS 140-2 compliant cryptographic protections for the integrity and confidentiality of information transmitted through a wireless connection.

4.39 Disable Wireless Networking AC-18(3) (NIST Moderate Control)

a. OST will disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

4.40 Antennas and Transmission Power Levels AC-18(5) (NIST Moderate Control)

a. OST will ensure that all devices transmitting a wireless signal will be set to a level that does not exceed the agencies physical boundaries.

4.41 Access Control for Mobile Devices AC-19 (NIST Moderate Control)

a. The organization defines inspection and preventative measures
b. Purge/wipe information from mobile devices based the SCSO Regulatory Settings spreadsheet, unsuccessful device logon attempts (e.g., personal

digital assistants, smartphones, and tablets). Laptop computers are excluded from this requirement

c. Only organization-owned encrypted mobile devices and software can be used to process, access, and store sensitive and/or confidential data.

4.42 Full Device or Container-based Encryption AC-19(5) (NIST Moderate Control)

a. Full-disk encryption shall be used to protect the confidentiality and integrity of information on all mobile computing devices such as laptops, netbooks, and similar devices.
b. Mobile storage devices must use approved encryption methods.
c. Handheld mobile computing devices (e.g., smartphones, tablets) will utilize state defined mobile device management and encryption solutions.
d. Encryption must be FIPS 140-2-compliant.

4.43 Use of External Systems AC-20 (NIST Moderate Control)

a. Instruct all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Limit remote access only to information resources required by home users to complete job duties. Require that any OST-owned equipment be used only for business purposes by authorized employees.
b. Only OST owned computers and software can be used to process, access, and store sensitive and confidential data.
c. Privacy requirements must be addressed in agreements that cover relationships in which external information systems are used to access, process, store, or transmit and manage sensitive and confidential data.
d. Access to sensitive and confidential data from external information systems, including but not limited to personally owned information systems/devices, is limited to those organizations and individuals with a binding agreement to terms and conditions of privacy requirements that protect the sensitive and confidential data.

4.44 Limits of Authorized Use AC-20 (1) (NIST Moderate Control)

a. OST may permit authorized individuals to use an external information system to access the information system or to process, store, or transmit State data only when OST does one of the following:

1. Verifies the implementation of required security controls on the external system as specified in the agency's information security policy and security plan; or
2. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

4.45 Portable Storage Devices – Restricted Use AC-20(2) (NIST Moderate Control)

a. Limit the usage of OST-controlled portable storage devices in external systems.
b. Document restrictions as to how and when the portable storage devices may be used and under what conditions.

4.46 Information Sharing AC-21 (NIST Moderate Control)

a. OST shall protect the State's sensitive and confidential data while utilizing software or information systems under the following conditions:
    1. A written agreement that addresses the business, security and technical requirements regarding the use and custodial responsibilities of the data and systems. These agreements can take the form of a Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU), Service Level Agreement (SLA), or equivalent contractual agreement, and an Interconnection Security Agreement (ISA) or a combined agreement.
    2. If the sharing of data or systems is between two state agencies as part of a service, and not otherwise governed by legal requirements, the agencies may choose to use a Service Level Agreement (SLA) that clearly defines the responsibilities, services, priorities and performance metrics of the services to be provided.
    3. Agency software or information systems that allow the sharing of files and data containing sensitive or confidential information shall be used to share data only if the appropriate security controls are properly configured and implemented.
    4. Appropriate security controls shall include the following:
        a. Authentication controls to ensure that authorized users are identified.

b. Access controls to limit an individual's access to only the restricted and/or highly restricted data necessary for that person to perform his/her role.
c. Authorization controls to enforce version control and record retention requirements as defined in the SCSO Regulatory Settings spreadsheet such that only designated individuals are able to modify or delete sensitive or critical records.
d. Audit controls that record individual actions on files and records, such as file modification.
e. Audit logs shall be retained in accordance with the posted SCSO Regulatory Settings spreadsheet.
f. These controls may be supplemented by operating-system-level controls (file and directory access control lists and system audit logs).

4.47 Publicly Accessible Content AC-22 (NIST Moderate Control)

a. The data owners shall:
    1. Designate individuals as authorized to post information onto publicly accessible information systems;
    2. Train designated individuals to ensure that publicly accessible information does not contain non-public information;
    3. Review the proposed content of publicly accessible information to ensure non-public information is not included prior to posting onto the information system as defined in the SCSO Regulatory Settings spreadsheet; and
    4. Review content on the publicly accessible information systems for non-public information and remove such information if discovered.
    5. Content shall be reviewed at a frequency commensurate with the frequency information is posted.
    6. Personnel conducting these reviews should be different than those posting or conducting the reviews prior to posting.

4.48 Data Mining Protection AC-23 (CJIS Specific Control)

a. Utilize data mining prevention and detection techniques to detect and protect against unauthorized data mining.

4.49 Access Control Decisions AC-24 (PCI Specific Control)

a. Establish procedures implementing mechanisms to ensure that appropriate access is applied to each access request prior to access enforcement.

4.50 Reference Monitor AC-25 (PCI Specific Control)

a. Implement a reference validation mechanism that:
    1. enforces an access control policy over all subjects and objects,
    2. is continuously monitored; and
    3. is small enough to be subject to analysis and tests so that completeness can be verified (assured).

5. Authority

Refer to the State Cybersecurity Office (SCSO) Regulatory Definitions document.

6. Related Controls

NIST: AC-02, AC-03, AC-04, AC-05, AC-06, AC-07, AC-08, AC-09, AC-11, AC-14, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AC-24, AC-25, AT-02, AT-03, AU-02, AU-03, AU-06, AU-09, AU-10, AU-12, AU-13, AU-14, CA-02, CA-03, CA-07, CA-09, CM-02, CM-05, CM-06, CM-07, CM-10, CM-11, CP-09, IA-01, IA-02, IA-03, IA-04, IA-05, IA-06, IA-07, IA-08, IA-11, IA-12, MA-03, MA-04, MA-05, MP-02, MP-04, MP-05, MP-07, PE-02, PE-17, PL-02, PL-04, PL-09, PM-02, PM-09, PM-12, PM-24, PS-02, PS-03, PS-04, PS-05, PS-07, PS-08, PT-02, PT-03, PT-07, RA-03, SA-08, SA-09, SA-15, SA-17, SC-02, SC-03, SC-04, SC-07, SC-08, SC-10, SC-12, SC-13, SC-15, SC-16, SC-23, SC-28, SC-31, SC-34, SC-37, SC-38, SC-40, SC-41, SC-43, SI-03, SI-04, SI-08, SI-12

7. Roles & Responsibilities

The roles and responsibilities are from the data owner perspective. RACI is an acronym derived from the four key components: Responsible (R), Accountable (A), Consulted (C), and Informed (I).

Activities	**Roles**			
	CISO	Security Admin	Dept Heads/Process Owners	Employees
Identify Accounts (Temp Accounts, Privileged, User, etc.)	A	R	C	I
Access Enforcement / Account Management	A	R	C	I
Separation of Duties	I	A	R	C
Remote Management	A	R	I	I
Wireless Access	A	R	I	I
Authentication / encryption	A	R	C	I

8. Compliance

This control shall take effect upon publication. Compliance is expected with all OST controls. Employees not following this OST control are subject to the standard disciplinary procedures.

If compliance with this control is not feasible or technically possible, or if deviation from this control is necessary to support a business function, applicable entities shall request an exception through the State Cybersecurity Office (SCSO) Exception Request Procedure.

9. Related Documentation

Access Control Procedures
Policy_AC_Access Control
SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings

10. Revision History

This standard shall be subject to review according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet to ensure relevancy.

Date	Description of Change	Reviewer
12/16/2022	Moved from Draft to Final	Greggari Tucker, Deputy Chief Information Security
06/04/2024	Updated AC-6(7)	Ray Girdler, State IT Security Specialist
12/18/2024	Annual Review. Update of "Related Controls" and "Related Documentation".	Ray Girdler, State IT Security Specialist
07/15/2025	Replaced DIS with OST	Ray Girdler, IT Infrastructure Architect