	<h1>Access Control Policy</h1>		Document No. SCIO-SEC-301-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 1 of 20


Scope

The Statewide Information Security Policies are the foundation for information technology security in North Carolina. The policies set out the statewide information security standards required by N.C.G.S. §143B-1376, which directs the State Chief Information Officer (State CIO) to establish a statewide set of standards for information technology security to maximize the functionality, security, and interoperability of the State's distributed information technology assets, including, but not limited to, data classification and management, communications, and encryption technologies. These standards apply to all executive branch agencies, their agents or designees subject to Article 15 of N.C.G.S. §143B. Use by local governments, local education agencies (LEAs), community colleges, constituent institutions of the University of North Carolina (UNC) and other executive branch agencies is encouraged to the extent allowed by law.

Responsibilities

All covered personnel that utilize IT resources are responsible for adhering to this policy and any local Access Control requirements.

Role	Definition
Agency Management	The Agency Head, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or other designated organizational officials at the senior leadership level are assigned the responsibility for ensuring that the goals and requirements of the Access Control Policy are met. Responsible for ensuring that the approved administrative and technical privacy controls are in place and effective. Responsible for educating employees about their access control responsibilities.
Information Security	The Information Security function is responsible for the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability
Agency Security Liaison	The Agency Security liaison is responsible for ensuring that security risks are managed in compliance with the State's requirements by collaborating with organizational entities. Liaisons are responsible for ensuring that the appropriate access controls are in effect for agency information systems.
Covered Personnel	Covered personnel are required to understand their security responsibilities and have the requisite skills and knowledge to ensure the effective execution of the roles they are assigned to reduce the risk of unauthorized access, use or modification of IT Resources (theft, fraud or misuse of facilities).
Third Parties	Third party service providers must ensure that all IT systems and applications developed for the State conform to this and other applicable Enterprise Information Technology Policies, Standards and Procedures. Non-conforming IT systems cannot be deployed unless the purchasing entity and their contractor have jointly applied for and received, in writing from the CIO or designee, notice that a specified exception will be permitted.

	<h1 style="margin: 0;">Access Control Policy</h1>		Document No. SCIO-SEC-301-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 2 of 20

AC-1 - Policy


All users of State and agency systems with access to non-public data must identify themselves and provide a means to authenticate their claimed identities appropriately for the risk level of the system and/or transaction. The policy statements in this document address the considerations that will help to ensure that the State's IT resources and information assets are properly protected against unauthorized access, while meeting the access requirements for all authorized users. Critical to achieving this objective is the implementation of controls that address each of the requirements stated in this policy. This policy shall be reviewed annually, at a minimum.

The State and agencies are required to implement necessary controls for providing authorized access and preventing unauthorized access to IT resources and information assets on the basis of business and security requirements.

The State utilizes the Access Control principles established in the NIST SP800-53 Rev 4 Access Control family guidelines as the official policy for this domain. The "AC" designator identified in each procedure represents the NIST-specified identifier for the Access Control family. The following subsections in this document outline the Access Control requirements that the State and each agency must develop, or adhere to in order to be compliant with this policy and to ensure that logical and physical access to information systems is sufficiently controlled. Each State business system is then bound to this policy, and must develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented.

Access to State information technology assets shall be controlled and managed to ensure that only authorized devices/persons have appropriate access in accordance with an agency's business needs. All computers that are permanently or intermittently connected to an agency's network shall have an approved credentials-based access control system. Regardless of the network connections, all systems handling the State's restricted and/or highly restricted data shall employ approved authentication credentials-based access control systems and encryption for data in transit. Access to State and Agency systems shall be controlled by the following:


- a. User profiles that define roles and access.
- b. Documented review of standard users' rights, at least annually.
- c. Documented review of administrator user accounts every 6 months.
- d. Revocation of access upon termination of employment.
- e. Only authorized users shall be granted access to the State's information systems, and the principle of least privilege shall be used and enforced.
- f. Assignment of privileges shall be based on an individual's job classification, job function, and the person's authority to access information. Job duties shall be separated as appropriate to prevent any single person or user from having any access not required by their job function.
- g. Default access for systems containing restricted or highly restricted data shall be deny-all.

	<h1 style="margin: 0;">Access Control Policy</h1>		Document No. SCIO-SEC-301-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 3 of 20


AC-2 - Account Management

Agencies shall establish policies and procedures for managing access rights for use of their networks and systems throughout the life cycle of the user's credentials, such as user IDs, ID cards, tokens, or biometrics. Access authorization includes the following appropriate requirements:

- a. There shall be a documented approval process whereby authorized parties create user accounts and specify required privileges for user access to systems and data. Agencies shall require approval for requests to create information system accounts.
- b. Agencies shall assign account managers for their information systems. Agencies shall also identify a backup system administrator to assist with user account management when the primary system administrator is unavailable.
- c. Agencies shall create, enable, modify, disable, and remove information system accounts in accordance with documented agency account management procedures.
- d. Agencies shall communicate user account policies and procedures including authentication procedures and requirements to all users of an information system.
- e. User credentials shall be individually assigned and unique in order to maintain accountability. User credentials shall not be shared but only used by the individual assigned to the account, who is responsible for every action initiated by the account linked to that credential.
- f. Default/generic credentials, such as "root" or "admin", shall be disabled or changed prior to a system being put into production.
- g. User credentials shall be disabled immediately upon the account owner's termination from work for the State or when the account owner no longer needs access to the system or application.
- h. Agencies shall establish conditions for group and role membership. Agencies shall specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.
- i. All systems must be assigned a system owner responsible for authorizing access.
- j. The default access method for files and documents is role-based access control (RBAC), however, other methods to securely access files and documents may be used (e.g. attribute-based access control (ABAC), lattice-based access control (LBAC), etc.).
- k. Access rights of users in the form of read, write and execute shall be controlled appropriately and the outputs of those rights shall be seen only by authorized individuals.
- l. Access to restricted and/or highly restricted data shall be restricted to authorized individuals who require access to the information as part of their job responsibilities.
- m. Agencies shall modify an individual's access to a State information technology asset upon a change of employment or change in authorization, such as termination, a leave of absence or temporary/permanent reassignment. An agency may change, restrict or eliminate user access privileges *at any time*.

	<h1>Access Control Policy</h1>	Document No. SCIO-SEC-301-00	
Status Final	Effective Date 01/29/2018	Version 1	Page No. 4 of 20

- n. Only authorized system or security administrators or an authorized service desk staff shall be allowed to enable or re-enable a user credential except in situations where a user can do so automatically through challenge/response questions or other user self-service mechanisms.
- o. All user credential creation, deletion and change activity performed by system administrators and others with privileged access shall be securely logged and reviewed on a regular basis.
- p. User credentials established for a non-employee/contractor must have a specified expiration date unless a user credential without a specified expiration date is approved in writing by the agency security liaison. If an expiration date is not provided, a default of thirty (30) days must be used.
- q. Access control may need to be modified in response to the confidentiality, integrity or availability of information stored on the system, if existing access controls pose a risk to that information.
- r. In order to facilitate intrusion detection, information shall be retained on all logon attempts until the agency determines the information is no longer valuable, or as required by law or the standards of this policy.
- s. All authorized users of administrative-access accounts shall receive appropriate training on the use of those accounts.
- t. There shall be a process for notifying account managers when system accounts are no longer required, when users are terminated or transferred, or when individual information system usage or need- to-know permission changes.
- u. Agencies shall authorize access to information systems that receive, process, store, or transmit Federal Tax Information (FTI) based on a valid access authorization, need-to-know permission, and under the authority to re-disclosed FTI under the provisions of IRC 6103.
- v. Agencies shall monitor the use of information system accounts. Agencies shall review accounts for compliance with account management requirements at a minimum of annually for user accounts and semi-annually for privileged accounts/roles. Privileged accounts are those accounts which can perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, account management, network and system administration, database administration, and web administration.
- w. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group, for example, RACF accounts that are reissued to different individuals.
- x. All accounts are processed for records management, litigation hold and other similar information disposition purposes prior to deleting, disabling or transferring.
- y. Appropriate background checks shall be completed and adjudicated for unprivileged and privileged access and accounts according to Federal and/or State designation procedures for those systems that require it, for example, systems with FTI and Criminal Justice Information (CJI).

	<h1 style="color: white; background-color: #4F81BD; padding: 10px; margin: 0;">Access Control Policy</h1>		Document No. SCIO-SEC-301-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 5 of 20

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

Where feasible, agencies shall employ automated mechanisms to support the management of information system accounts. The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information system to monitor account usage; and using system notification to report atypical system account usage.

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

Temporary and emergency accounts shall be immediately disabled or removed from a system once they are no longer needed. When temporary accounts are needed for internal or external audit, software development, software installation, training, guest access, or other defined need, the following conditions shall apply:

- a. Authorized in advance by agency management;
- b. Have a specific expiration date;
- c. Be monitored while in use,
- d. Be removed when the work is completed.


Training accounts shall be rendered inactive (e.g., by resetting the password) at the end of the training event. If multiple classes are held during a given day, the account may remain active until the end of the day, rather than resetting the accounts between classes held on the same day.

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

User credentials that are inactive for a maximum of ninety (90) days must be disabled, except as specifically exempted by a security administrator. All accounts that have been disabled for greater than 365 days shall be deleted. Where feasible, the system shall automatically disable accounts per the conditions of this control.

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

Information systems shall automatically audit account creation, modification, enabling, disabling, and removal actions, and notify the appropriate agency-defined personnel of these events.

	<h1 style="color: white; background-color: #4F81BD; padding: 10px;">Access Control Policy</h1>		Document No. SCIO-SEC-301-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 6 of 20

AC-3 - Access Enforcement

The information system must enforce a role-based access control policy over defined subjects and objects and control access to the data based upon a valid access authorization, intended system usage, and the authority to disclose FTI under the provisions of IRC 6103. Password management requirements are described in the Identification and Authentication Policy, SCIO-SEC-307, Section IA-5.


AC-4 – Information Flow Enforcement

Agencies shall deploy mechanisms to control access to the State’s network backbone and/or routed infrastructure. The State Network must be configured to monitor and control communications at the external boundary of the network and internal boundaries at strategic locations. The State Network must connect to external networks or information systems only through managed interfaces approved by agency 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. Protective controls shall at a minimum include the following:

- a. Positive source and destination address checking to restrict rogue networks from manipulating the State’s routing tables.
- b. Authentication to ensure that routing tables do not become corrupted with false entries.
- c. Use network address translation (NAT) to obfuscate internal network addresses.
- d. Email data leak prevention (DLP) to maintain compliance, identify and monitor the safe handling of specific categories of restricted or highly restricted data as defined by N.C.G.S. 132-1.2, e.g. credit card numbers and U.S. social security numbers (SSNs).
- e. Firewalls shall control inbound and outbound network traffic by limiting that traffic to only that which is necessary to accomplish the mission of the agencies. Firewall configuration, installation, monitoring and filtering requirements are found in the System and Communications Protection Policy SCIO-SEC-316, Section SC-7.
- f. The information system shall enforce approved authorizations for controlling the flow of FTI within the system and between interconnected systems based on the technical safeguards in place to protect the FTI.

AC-5 - Separation of Duties

Separation of duties is an integral part of a successful information security program that reduces the risk of accidental or deliberate system misuse. Separation of duties reduces opportunities for unauthorized modification or misuse of information by segregating the management and execution of certain duties or areas of responsibility. Although smaller agencies without the manpower to staff separate sections or groups will find this method of control more challenging to implement, the


	<h1 style="margin: 0;">Access Control Policy</h1>		Document No. SCIO-SEC-301-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 7 of 20

principle should be applied to the extent possible. Agency management must ensure that there is proper segregation of duties to reduce the risk of agency system misuse and fraud.

- a. Agencies shall conduct information system support functions (e.g., system management, programming, configuration management, quality assurance and testing, and network security) with different individuals; and ensure security personnel administering access control functions do not also administer audit functions.
- b. Agencies shall monitor and review system usage for activities that may lead to business risks by personnel who are able to quantify and qualify potential threats and business risks. Appropriate controls and separation of duties shall be employed to provide review and monitoring of system usage of personnel normally assigned to this task. Some events that should be monitored include over utilization of bandwidth, un- authorized login attempts, and un-authorized attempts to make changes to system settings.
- c. System administration and system auditing shall be performed by different personnel.
- e. System development and system change management shall be performed by different personnel.
- f. System operations and system security administration shall be performed by different personnel.
- g. If possible, security administration and security audit shall be performed by different personnel.
- h. Agencies shall keep the responsibility for security audit separate from other audit duties.
- i. Agencies shall identify, document, and segregate activities that require collusion to defraud (e.g., exercising a purchase order and verifying receipt of goods).
- j. Separation of duties is mandatory for all financial applications where misuse could cause a direct financial loss. Examples include, but are not limited to the following:
 - i. Check issuance
 - ii. Funds transfer
 - iii. Input of vendor invoices
 - iv. Other purchasing information
 - v. Receiving information

Some additional examples of this principle include the following:

- i. The same individual shall not enter and authorize a purchase order.
- ii. The same individual shall not request a user account and also create the account in the system.
- iii. A system administrator shall not be the one to conduct the audits/reviews of the system he/she is administering.
- iv. An Information Security Officer (ISO) shall not be a system administrator.

	<h1 style="margin: 0;">Access Control Policy</h1>		Document No. SCIO-SEC-301-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 8 of 20

- v. A Database administrator (DBA) shall have the minimum level of operating system rights necessary to create, edit and delete rights over the database specific files in the system directory, but no directory level rights in the system directory.
- k. Prohibit development staffs (who have powerful privileges in the development environment) from extending their administrative privileges to the operational environment.
- l. Separation of duties in programming shall be enforced to eliminate trapdoors, software hooks, covert channels, and Trojan code.


AC-6 - Least Privilege

Agencies shall employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with agency missions and business functions. Least privilege applies to the development, implementation, and production lifecycle of information systems. Agencies shall enforce the following.

- a. Only authorized individuals shall perform updates to restricted or highly restricted data such as citizen and business databases, protected health information (PHI), or FTI.
- b. The agency shall explicitly authorize access to security functions and security-relevant information. Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.

Explicitly authorized personnel include security administrators, system and network administrators, system maintenance personnel, system programmers, and other privileged users.

- c. The agency shall restrict privileged accounts on the information system to a limited number of authorized individuals with a need to perform administrative duties. Privileged accounts, including super user accounts, are typically described as system administrator for various types of systems.
 - i. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions.
 - ii. Agencies may differentiate in an application between allowed privileges for local accounts and for domain accounts provided the agency retains the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk.
- d. Information systems shall prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.
 - i. Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities.

	<h1 style="margin: 0;">Access Control Policy</h1>		Document No. SCIO-SEC-301-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 9 of 20


- ii. Non-privileged users are individuals that do not possess appropriate authorizations.
- iii. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.
- e. Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on agencies. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT). Information systems shall do the following:
 - i. Audit the execution of privileged functions as described in the Audit and Accountability Policy, SCIO-SEC-303, Section AU-2, Audit Events.
 - ii. Prevent non-privileged users from executing privileged functions; including disabling, circumventing, or altering implemented security safeguards/countermeasures.
- f. Administrators of multi-user systems, systems that allow for concurrent usage of the system by multiple persons, must have at least two user credentials. One of these user credentials must provide privileged access, with all activities logged; the other must be a normal user credential for performing the day-to-day work of an ordinary user.
- g. Users of information system accounts, or roles, with access to sensitive information, shall use non-privileged accounts or roles when accessing non-privileged functions. This control enhancement limits exposure when operating from within privileged accounts or roles.

AC-7 - Unsuccessful Logon Attempts

- a. To the extent possible, an information system shall limit unsuccessful logon attempts to three (3) during a 120-minute period before the user's account is disabled. For example, if an incorrect password is provided three (3) consecutive times, remote access systems shall drop the connection.
- b. The locked out duration shall be at least thirty (30) minutes, unless the end user successfully unlocks the account through a challenge question scenario or a system or security administrator or an authorized service desk staff member re-enables the user's account.

AC-8 - System Use Notification

All network systems must use a logon banner containing State approved wording and must provide prompts as needed. Information system shall display to users a notification **before** granting access to the system that provides privacy and security notices consistent with applicable federal and state laws. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. The standard statewide logon banner is as follows:

	<h1 style="margin: 0;">Access Control Policy</h1>		Document No. SCIO-SEC-301-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 10 of 20

This is a government computer system and is the property of the State of North Carolina. This system may contain U.S. Government information, which is restricted to authorized users ONLY. Unauthorized access, use, misuse, or modification of this computer system or of the data contained herein or in transit to/from this system may subject the individual to administrative disciplinary actions, criminal and civil penalties. Users have no expectation of privacy. This system and equipment are subject to monitoring to ensure proper performance of applicable security features or procedures. Such monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed, or stored in this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to Law Enforcement Personnel. ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING.

For publicly accessible systems:

- a. Displays system use information before granting further access;
- b. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
- c. Includes a description of the authorized uses of the systems

AC-9 – Previous Logon (Access) Notification (Optional)

This control is optional for LOW and MODERATE risk information systems.

AC-10 – Concurrent Session Control (Optional)

This control is optional for LOW and MODERATE risk information systems.


AC-11 - Session Lock

Agencies shall ensure the following:

- a. The agency information system prevents further end user access to the system by initiating a session lock after 15 minutes of inactivity or upon receiving a request from a user.
- b. The agency information system shall retain the session lock until the user reestablishes access using established identification and authentication procedures.

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

Agency information systems shall conceal, via the session lock, information previously visible on the display with a publicly viewable image, such as a screen saver, photographic image, blank screen, solid colors, clock, etc. Screen saver images shall not convey sensitive information.

	<h1>Access Control Policy</h1>		Document No. SCIO-SEC-301-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 11 of 20

AC-12 - Session Termination

A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an agency information system.

- a. Network-connected single-user systems, such as laptops and PCs, shall employ agency-approved hardware or software mechanisms that control system booting and that include a time-out-after-no-activity (for example, a screen saver).
- b. The time-out system must terminate all sessions that have had no activity for a period of thirty (30) minutes or less. For some higher risk information systems, the requirement for a session idle timeout may be more stringent as determined by agency policy, industry standard (e.g., PCI DSS) or other regulations.


AC-13 - Supervision and Review – Access Control

Withdrawn: Incorporated into AC-2 and AU-6.

AC-14 - Permitted Actions Without Identification or Authentication

Agencies shall determine what access controls are required, if any, for those specific instances where an agency determines 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, but rather to situations where identification and/or authentication have not yet occurred. FTI may not be disclosed to individuals on the information system without identification and authentication.

- a. Users may access public websites or publicly available information on accessible State information systems without identification and authentication.
- b. System/business owners, in collaboration with service provided must identify, provide justification and develop supporting documentation for user actions that can be performed on systems not requiring identification and authentication. Justification must specify the following:
 - i. 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.
 - ii. Identification of responsible person for ensuring access control and monitoring is conducted
 - iii. Supporting rationale for not requiring identification and authentication
- c. Implement compensating security controls at the directory and file level for all application specific and system accounts which do not require passwords. Implement only using least privilege, with access given only to necessary directories and files.

	<h1 style="margin: 0;">Access Control Policy</h1>		Document No. SCIO-SEC-301-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 12 of 20

AC-15 – Automated Marking

Withdrawn: Incorporated into MP-3.


AC-16 – Security Attributes (Optional)

This control is optional for LOW and MODERATE risk information systems.

AC-17 - Remote Access

Where there is a business need and prior agency management approval, authorized users of agency computer systems, the State Network and data repositories shall be permitted to remotely connect to those systems, networks and data repositories to conduct State-related business through secure, authenticated and carefully managed agency approved access methods. Remote access is defined as access to State information by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet) that are not publicly accessible (e.g. agency LAN).


- a. Access to the State Network and agency internal networks via external connections from local or remote locations shall not be automatically granted with network or system access. Systems shall be available for on- or off-site remote access only after an explicit request is made by the user and approved by the manager for the system in question.
- b. Agencies shall establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.
- c. Agencies authorize remote access to the information system prior to allowing such connections.
- d. When unauthorized remote access is detected on State systems: (1) An alert shall be sent to appropriate system and security personnel, and (2) an alert is sent every hour thereafter until the device is removed from the network or authorized by the configuration management process.
- e. Agencies shall require adequate security measures (e.g., virus and spam protection, firewall, intrusion detection) on client computers prior to allowing remote or adequately protected virtual private network (VPN) access. Access to the State Network is a privilege and shall be denied, at the State CIO's discretion, to clients attached to networks deemed unacceptably vulnerable.
- f. All users wishing to establish a remote connection via the Internet to the agency's internal network must first authenticate themselves at a firewall or security device.
- g. Remote access for system administration functions that originate from networks external to the State Network, such as the Internet, must be accomplished, at a minimum, using multi-factor authentication (MFA).
- h. Remote access to systems for end users, specifically for access to either Restricted or Highly Restricted data, shall be achieved using MFA technologies.

	<h1 style="margin: 0;">Access Control Policy</h1>		Document No. SCIO-SEC-301-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 13 of 20

- i. All users who require remote access privileges shall be responsible for the activity performed with their user credentials. User credentials shall never be shared with those not authorized to use the credential. User credentials shall not be utilized by anyone but the individuals to whom they have been issued. Similarly, users shall be forbidden to perform any activity with user credentials belonging to others.
- j. Remote access shall be revoked at any time for reasons including non-compliance with security policies, request by the user's supervisor, or negative impact on overall network performance attributable to remote connections. Remote access privileges shall be terminated upon an employee's or contractor's termination from service. Remote access privileges shall be reviewed upon an employee's or contractor's change of assignments and in conjunction with other regularly scheduled user account reviews.
- k. With the exception of Web servers or other systems where regular users are anonymous, users are prohibited from remotely logging into any state computer system or network anonymously (for example, using "guest" accounts). If users employ system facilities that allow them to change the active user ID to gain certain privileges, such as the switch user (su) command in Unix/Linux, they must have initially logged in with a user ID that clearly indicates their identity.
- l. If an agency computer or network access control system is not functioning properly, it shall default to denial of access privileges to users. If access control systems are malfunctioning, the systems they support must remain unavailable until such time as the problem has been rectified.
- m. Split tunneling shall be disabled for all VPN solutions.
- n. Remote access to single-equipment hosts (e.g., agency servers) shall be permitted provided the equipment requires authenticated access, is appropriately protected by a VPN, and prevents onward connection to the State Network.
- o. Users requiring telecommunications access, such as dial-up modem access, for "out of band" management or special needs must obtain agency management approval.

AC-17 (1) - Remote Access – Automated Monitoring / Control (Moderate Control)

The information system shall use automated functions to monitor and control remote access methods. Systems shall log all remote access occurrences, including both end user and administrator activity (user credential, date/time, and duration of connection at a minimum). Automated monitoring and control of remote access sessions allows organizations to detect cyber attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of information system components (e.g., servers, workstations, laptops, smart phones, and tablets).

	<h1 style="margin: 0;">Access Control Policy</h1>		Document No. SCIO-SEC-301-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 14 of 20

AC-17 (2) - Remote Access – Protection of Confidentiality / Integrity Using Encryption (Moderate Control)

The agency shall implement encryption to protect the confidentiality and integrity of remote access sessions. Access through an agency-managed secure tunnel such as a Virtual Private Network (VPN) or Internet Protocol Security (IPSec) shall employ FIPS 140-2 compliant encryption techniques for encryption and secure authentication.

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

Agencies shall route all remote accesses through managed network access control points. Limiting the number of access control points for remote accesses reduces the attack surface for organizations.


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

Agencies shall authorize the execution of privileged commands and access to security-relevant information, e. g. logging into a firewall device for administrative functions. Remote access under these conditions shall be authorized only for compelling operational needs and the agency shall document the rationale for such access. Such actions shall be logged and audited.

AC-18 - Wireless Access

Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless devices include such things as laptops, smartphones, tablets, and Internet of Things (IoT) that access a network wirelessly. Agencies shall have the following security measures implemented to prevent electronic eavesdropping by unauthorized personnel for wireless network access.

- a. Access points shall be segmented from an agency's internal wired local area network (LAN) using a gateway device.
- b. The SSID may indicate the name of the agency. The SSID name should be communicated to agency employees utilizing the wireless network (WLAN) to ensure they are connecting to the agency network and not a rogue access point attempting to impersonate an official agency WLAN.
- c. A device must be prevented from connecting to a WLAN unless it can provide the correct SSID.
- d. Every device used to access the State Network wirelessly, when not in use for short periods of time, shall be locked via operating system features. Devices shall be turned off when not in use for


	<h1 style="color: white; background-color: #4F81BD; padding: 10px; margin: 0;">Access Control Policy</h1>		Document No. SCIO-SEC-301-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 15 of 20

extended periods of time, unless the device is designed to provide or utilize continuous network connectivity (e.g. wireless cameras, RFID tag readers, and other portable wireless devices).

- e. If supported, auditing features on wireless devices shall be enabled and the audits reviewed periodically by designated staff.
- f. Agencies shall ensure that endpoint protection systems are configured to disallow “dual-homed” wireless/wired connections, e.g. a laptop shall not be permitted to be connected to a State system via a wired connection while using a wireless connection to a non-State external system.
- g. Authentication shall be performed when point-to-point wireless access points are used between routers to replace traditional common carrier lines.
- h. Agencies shall employ a wireless intrusion detection system (WIPS) that access State resources in order to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the agency’s information system.
- i. Security event logs for wireless networks connected to the State infrastructure shall be sent to a centralized log management tool.
- j. Agencies shall conduct periodic war driving exercises in and around agency facilities to detect unauthorized access points and ad hoc networks that are attached to the agency’s network. Agencies shall remove and report through incident response procedures any unauthorized devices that are found.

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

- a. Agencies shall use authentication technologies to protect wireless access to information systems.
 - i. All wireless access to the State Network via an 802.11 wireless network shall be authenticated by requiring the user to supply the appropriate credentials as supported by the Wi-Fi directly or via the Extensible Authentication Protocol (EAP) extensions.
 - ii. Where a documented business case exists, user devices may authenticate using compliant service accounts but must require a user to re-authenticate to the Wi-Fi once the user has authenticated to the device.
 - iii. 802.1x credentials for individual users shall be deactivated in accordance with an agency’s user management policy or within twenty-four (24) hours of notification of a status change (for example, employee termination or change in job function).
 - iv. Agency approved guest access shall give users access to only the Internet and shall use a captive portal that at least requires the guest users to agree to terms of service and states user activity on the wireless network is monitored.

	<h1 style="margin: 0;">Access Control Policy</h1>		Document No. SCIO-SEC-301-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 16 of 20


- b. Agencies shall use FIPS 140-2 compliant encryption to protect wireless access to information system. For a list of validated cryptographic modules and products, refer to the following NIST publication: <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>.

AC-19 – Access Control for Mobile Devices

NIST defines a mobile device as a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source.

Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, smartphones, tablets, e-readers, smart watches, digital cameras and audio recording devices). Some of these devices are multifunctional and may be used for voice calls, text messages, email, Internet access, and may allow access to computers and/or networks. Agencies shall protect state resources and information while using mobile communication devices through the following requirements:

- a. Agencies that allow mobile communication devices (personal or business owned) to connect to state systems, such as email, shall require the following:
 - i. A minimum 4-digit numeric, user defined, personal identification number (PIN) that is changed every 90 days.
 - ii. A time out of inactivity that is 10 minutes or less.
 - iii. If technically possible, the ability to remotely erase the contents of the device, at the user's request, management request via a help desk service request, or by the user's own action.
Agencies shall make end users aware they are accepting the risk of personal data being lost.
- b. Disable wireless functionality (i.e., Wi-Fi or Bluetooth) on appropriate devices that have wireless functionality (i.e., Wi-Fi or Bluetooth) when the device is not in use for an extended period of time.
- c. Purge/wipe information from mobile devices based on 10 consecutive, unsuccessful device logon attempts (e.g., personal digital assistants, smartphones and tablets). Laptop computers are excluded from this requirement.
- d. Agencies shall comply with legal and regulatory requirements associated with information that is stored on the device, such as requirements for confidentiality, security and record retention.
- e. When unauthorized connections are detected, i) an alert shall be sent to appropriate system personnel, and ii) the device shall be isolated from the network.
- f. Agencies shall ensure users adhere to the guiding principles and framework established in the Statewide Acceptable Use Policy (AUP).

	<h1 style="margin: 0;">Access Control Policy</h1>		Document No. SCIO-SEC-301-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 17 of 20


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

Agencies shall employ either full-device encryption or container encryption to protect the confidentiality and integrity of information on agency provided mobile devices. Where feasible, agencies shall encrypt all data stored on mobile devices.

AC-20 - Use of External Information Systems

External information systems are information systems or components of information systems that are outside of the authorization boundary established by an agency and for which the agency typically has no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. External information systems include, but are not limited to, the following examples: personally owned computers, personally owned mobile computing devices; privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, shopping malls, or airports); information systems owned or controlled by other governmental (Federal, State, or Local) organizations; and cloud computing services that are accessed from agency information systems.

- a. Access to restricted or highly restricted information from external information systems, other than through a virtual private network (VPN) is prohibited.
- b. Agencies may allow the use of personally-owned devices with access to FTI, without notification, only for the following purposes:
 - i. Bring Your Own Device (BYOD) used to access e-mail, where all requirements in IRS 1075 Section 9.4.8 Mobile Devices are met.
 - ii. Remote access through a virtual desktop infrastructure (VDI) environment, where all requirements in IRS 1075 Section 9.4.13 Virtual Desktop Infrastructure are met.
- c. Use of non-agency-owned information systems, system components, or devices to process, store, or transmit restricted or highly restricted data requires agency-pre-approval prior to implementation.
- d. Require that Cloud Service Providers (CSPs) configure systems such that access is consistent with defined, documented, and approved user access requirements, roles and responsibilities and account privileges and adhere to the following:
 - i. System accounts and access are reviewed at least monthly to ensure that only the appropriate levels of access are allowed.
 - ii. Access is granted only to authorized personnel.
 - iii. Users' access rights are limited to least privilege.

	<h1 style="margin: 0;">Access Control Policy</h1>		Document No. SCIO-SEC-301-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 18 of 20

AC-20 (1) - Use of External Information Systems – Limits on Authorized Use (Moderate Control)

Agencies shall permit authorized individuals to use an external information system to access the information system or to process, store, or transmit State data only when the agency does one of the following:

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

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


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

Agencies shall restrict the use of agency-controlled portable storage devices by authorized individuals on external information systems. Limits on the use of agency-controlled portable storage devices in external information systems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.

AC-21 - Information Sharing

Agencies shall protect the State's restricted and highly restricted data while utilizing software or information systems.

- a. State agencies that share data or systems must have written agreements that address the business, security and technical requirements regarding the use and custodial responsibilities of the data and systems. These agreements can take the form of 1) 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 2) a combined agreement.
- b. 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

	<h1>Access Control Policy</h1>		Document No. SCIO-SEC-301-00
Status Final	Effective Date 01/29/2018	Version 1	Page No. 19 of 20

Agreement (SLA) that clearly defines the responsibilities, services, priorities and performance metrics of the services to be provided.

- c. Agency software or information systems that allow the sharing of files and data containing restricted and/or highly restricted information shall be used to share data only if the appropriate security controls are properly configured and implemented.
- d. Appropriate security controls shall include the following:
 - i. Authentication controls to ensure that authorized users are identified.
 - ii. 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.
 - iii. Authorization controls to enforce version control and record retention requirements such that only designated individuals are able to modify or delete sensitive or critical records.
 - iv. Audit controls that record individual actions on files and records, such as file modification.
 - v. Audit logs shall be retained in accordance with the agency records retention policy or the General Schedule for State Agency Records, Information Technology Records.
 - vi. These controls may be supplemented by operating-system-level controls (*e.g.*, file and directory access control lists and system audit logs).
- e. This control is optional for LOW risk information systems.

AC-22 - Publically Accessible Content

Agency CIOs shall ensure that business owners do the following:

- a. Designate individuals as authorized to post information onto publicly accessible information systems.
- b. Train designated individuals to ensure that publicly accessible information does not contain non-public information.
- c. Review the proposed content of publicly accessible information to ensure non-public information is not included prior to posting onto the information system.
- d. Review content on the publicly accessible information system for non-public information and remove such information if discovered.
- e. Content shall be reviewed at a minimum quarterly for the identification and removal of non-public data.

AC-23 – Data Mining Protection (Optional)

This control is optional for LOW and MODERATE risk information systems.

