SOUTH CAROLINA
DEPARTMENT OF EDUCATION

**TITLE OF POLICY**: SC Access Control Policy

**SECTION**: Information Security and Privacy

**SUBSECTION**: Device and Access Security

**POLICY NUMBER**: 702.4

**OFFICE OF RESPONSIBILITY**: CISO

**EFFECTIVE DATE**: May 01, 2025



**THE RELEVANT DEPARTMENT OF ADMINISTRATION POLICY IS ATTACHED. BELOW IS A SYNOPSIS OF THE POLICY CONTENTS:**

## 1. Purpose and Scope

This policy is part of the South Carolina statewide information security framework and establishes requirements for managing access to information systems and resources. Its purpose is to ensure that only authorized users, devices, and processes can access systems, data, and functionalities.

The policy applies to all state agencies and supports the broader security and privacy program. Agencies must comply with these baseline requirements while also meeting any additional regulatory obligations and may implement supplemental guidance tailored to their operations.

## 2. Core Objective

The policy's primary objective is to enforce strong access control practices to:

- Prevent unauthorized access to systems and data
- Protect the confidentiality, integrity, and availability of information
- Ensure accountability for system usage
- Reduce the risk of misuse, data breaches, and insider threats

## 3. Key Policy Requirements

### A. Governance and Oversight (AC-1)

- Agencies must develop, document, and maintain access control policies and procedures.
- A designated official must oversee implementation and ongoing updates.
- Policies must align with applicable legal, regulatory, and organizational requirements.

### B. Account Management (AC-2)

- Agencies must define and manage all account types, including user, group, and privileged accounts.
- Account creation, modification, and removal must follow formal approval and authorization processes.
- Accounts must be monitored, reviewed regularly, and promptly disabled when no longer needed.
- Privileged accounts must be tightly controlled, monitored, and restricted to authorized roles.
- Temporary and emergency accounts must automatically expire after a defined period.

### C. Access Enforcement (AC-3)

- Access to systems and resources must be enforced based on approved authorizations.
- Role-based access control must be implemented to ensure users only have access appropriate to their roles.

### D. Information Flow Enforcement (AC-4)

- Agencies must control how information flows within systems and between connected systems to prevent unauthorized data transfer.

### E. Separation of Duties (AC-5)

- Duties must be divided among individuals to reduce the risk of fraud, error, or unauthorized activity.
- Access permissions must reflect these separations.

### F. Least Privilege (AC-6)

- Users must be granted only the minimum access necessary to perform their job functions.
- Privileged access must be restricted, monitored, and periodically reviewed.

- Non-privileged accounts should be used for routine activities whenever possible.

**G. Authentication Controls and Session Security (AC-7, AC-8, AC-11, AC-12)**

- Systems must limit failed login attempts and lock accounts after repeated failures.
- Users must be presented with system use notifications and consent to monitoring.
- Devices must automatically lock after inactivity and require reauthentication.
- Sessions must be terminated after defined periods or conditions.

**H. Remote, Wireless, and Mobile Access (AC-17, AC-18, AC-19)**

- Remote access must be authorized, monitored, and secured using encryption.
- Wireless access must be controlled, authenticated, and protected with encryption.
- Mobile device access must follow defined security requirements and include encryption to protect data.

**I. Use of External Systems (AC-20)**

- Agencies must define conditions for accessing systems from external environments.
- External systems must meet required security controls before use.
- Use of unauthorized external systems and portable storage devices must be restricted.

**J. Information Sharing (AC-21)**

- Agencies must ensure that information sharing aligns with access permissions and data handling requirements.
- Tools or processes must support users in making appropriate sharing decisions.

**K. Public Access and Content Management (AC-22)**

- Only authorized personnel may publish publicly accessible information.
- Content must be reviewed to ensure sensitive or nonpublic information is not exposed.
- Publicly accessible systems must be monitored and reviewed regularly.

## 4. Security and Compliance

- Must comply with FERPA, state privacy laws, and the South Carolina Public Records Act.
- Content may be considered public record and is subject to audit or disclosure.

- This policy will be reviewed annually. Violations may result in disciplinary action or loss of access.

**5. Related Policies:**

- SC Risk Assessment Policy Draft (701.3)
- SC Personally Identifiable Information Processing and Transparency Draft (704.1)
- SC Audit and Accountability Policy Draft (706.3)

# Information Security and Privacy Policy – Access Control

## Division of Information Security

May 01, 2025

# Revision History

| Version Number | Date | Author(s) | Description |
|---|---|---|---|
| 2.0 | May 1, 2025 | Division of Information Security | Updated for SCDIS-200 v2.0 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# CONTENTS

# 1.0 INTRODUCTION

## A. Purpose

The South Carolina Statewide Information Security Program (SC Infosec Program) consists of information security policies, standards and guidelines that establish a baseline information security framework to protect the information technology systems of South Carolina state government agencies[1].

Implementing the baseline framework is critical to the development of an agency information security and privacy program. An effective information security and privacy program continually improves the overall security posture for the state, as it integrates and matures toward support of the state and organizational mission, goals and objectives.

This *Access Control Policy* establishes the requirements for the management of access to information systems and resources, ensuring only authorized individuals or processes can access specific data and functionalities.

## B. Authority and Responsibilities

The organizational and functional responsibilities for the South Carolina Division of Information Security (DIS) and Agency are established in the SC Infosec Program's "Master Policy."

## C. Scope

Organizations shall comply with the SC Infosec Program's policies, standards and guidelines. Implementation of the SC Infosec Program's policies, standards and guidelines is not meant or intended to replace, supersede or otherwise nullify agency compliance requirements identified in other applicable federal, state, local, agency or institutional regulations, policies or guidance. Likewise, compliance with the SC Infosec Program's policies, standards and guidelines does not convey compliance with other regulatory requirements agencies may have for information security.

Organizations may implement policies, standards and guidelines "as-is," but are encouraged to develop additional agency or institution-specific guidance to address unique components of their business operations.

[1] The term "Agency" will be used to refer to SC state government agencies as described in the SC Infosec Program's "Master Policy."

# 2.0 ACCESS CONTROL POLICY STATEMENTS

## A. Policy and Procedures [AC-1]

*NIST CSF Reference: GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03, PR.AA-01, PR.AA-05*

1. Agencies shall develop, document and disseminate:
    a. An access control policy that addresses purpose, scope, roles, responsibilities management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards and guidelines.
    b. Procedures to facilitate the implementation of the *Access Control Policy* and the associated access controls.
2. Agencies shall designate an official to manage the development, documentation and dissemination of the access control policy and procedures.
3. Agencies shall review and update the current access control policy and procedures on a defined schedule and following defined events.

## B. Account Management Policy [AC-2]

*NIST CSF Reference: PR.AA-01, PR.AA-05, PR.DS-10, DE.CM-01, DE.CM-03*

1. Account Management [AC-2]:
    a. Agencies shall define and document the types of accounts allowed and specifically prohibited for use within the system.
    b. Agencies shall assign account managers.
    c. Agencies shall require prerequisites and criteria be satisfied for group and role membership.
    d. Agencies shall specify authorized users of the system, group and role membership, and access authorizations for each account.
    e. Agencies shall require approvals by designated officials for requests to create accounts.
    f. Agencies shall create, enable, modify, disable and remove accounts in accordance with defined policy, procedures, prerequisites and criteria.
    g. Agencies shall monitor the use of accounts.
    h. Agencies shall notify account managers and designated personnel or roles when accounts are no longer required, users are terminated or transferred, and system usage or need-to-know changes for an individual.
    i. Agencies shall authorize access to the system based on a valid access authorization and intended system usage.

j. Agencies shall review accounts for compliance with account management requirements on a defined frequency.

k. Agencies shall establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group.

l. Agencies shall align account management processes with personnel termination and transfer processes.

2. Automated Temporary and Emergency Account Management [AC-2 (2)]:

   Agencies shall automatically disable temporary and emergency accounts after a defined time period for each type of account.

3. Disabled Accounts [AC-2 (3)]:

   Agencies shall disable accounts within the defined time period when the accounts have expired, are no longer associated with a user or individual, are in violation of organizational policy, or have been inactive for a defined time period.

4. Privileged User Accounts [AC-2 (7)]:

   Agencies shall:

   a. Establish and administer privileged user accounts in accordance with a role-based access scheme or attribute-based access scheme.

   b. Monitor privileged roles.

   c. Monitor changes to roles.

   d. Revoke access when privileged roles are no longer appropriate.

5. Restrictions on Use of Shared and Group Accounts [AC-2 (9)]:

   Agencies shall only permit the use of shared and group accounts to meet agency-defined conditions for establishing shared and group accounts.

## C. Access Enforcement [AC-3]

*NIST CSF Reference: PR.AA-05, PR.DS-10, PR.IR-01*

1. Access Enforcement [AC-3]:

   Agencies shall enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

2. Role-based Access Control [AC-3 (7)]:

   Agencies shall enforce a role-based access control policy over defined subjects and objects, and control access based upon agency-defined roles and users authorized to assume such roles.

## D. Information Flow Enforcement [AC-4]

*NIST CSF Reference: ID.AM-03, PR.DS-10, PR.IR-01, DE.CM-09*

Agencies shall enforce approved authorizations for controlling the flow of information within the system and between connected systems based on information flow control policies.

## E. Separation of Duties [AC-5]

*NIST CSF Reference: PR.AA-05*

Agencies shall identify and document duties of individuals requiring separation of duties and define system access authorizations to support separation of duties.

## F. Least Privilege [AC-6]

*NIST CSF Reference: PR.AA-05*

1. Least Privilege [AC-6]:

   Agencies shall employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) necessary to accomplish assigned organizational tasks.

2. Authorize Access to Security Functions [AC-6 (1)]:

   Agencies shall authorize access to security functions and security-relevant information.

3. Non-Privileged Access for Nonsecurity Functions [AC-6 (2)]:

   Agencies shall require users of system accounts (or roles) with access to security functions or security-relevant information use non-privileged accounts or roles, when accessing nonsecurity functions.

4. Network Access to Privileged Commands [AC-6 (3)]:

   Agencies shall authorize network access to privileged commands only for compelling operational needs and document the rationale for such access in the security plan for the system.

5. Privileged Accounts [AC-6 (5)]:

   Agencies shall restrict privileged accounts on the system to authorized personnel or roles.

6. Privileged Access by Non-organizational Users [AC-6 (6)]:

   Agencies shall prohibit privileged access to the system by non-agency users.

7. Review of User Privileges [AC-6 (7)]:

   a. Agencies shall annually review the privileges assigned to agency-defined roles to validate the need for such privileges.

   b. Agencies shall reassign or remove privileges, if necessary, to correctly reflect agency mission and business needs.

## G. Unsuccessful Logon Attempts [AC-7]

*NIST CSF Reference: PR.AA-03*

Agencies shall enforce a limit of a defined number of consecutive invalid logon attempts by a user during a defined time period, and automatically lock the account or node until released by an administrator.

## H. System Notification [AC-8]

*NIST CSF Reference: None*

1. Agencies shall display an authorized notification message or banner to users before granting access to the system that provides privacy and security notices, consistent with applicable laws, executive orders, directives, regulations, policies, standards and guidelines and state that:
    a. Users are accessing a South Carolina state government system.
    b. System usage may be monitored, recorded and subject to audit.
    c. Unauthorized use of the system is prohibited and subject to criminal and civil penalties.
    d. Use of the system indicates consent to monitoring and recording.
2. Agencies shall retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system.
3. For publicly accessible systems, agencies shall:
    a. Display system use information conditions before granting further access to the publicly accessible system.
    b. Display references, if any, to monitoring, recording, or auditing consistent with privacy accommodations for such systems generally prohibiting those activities.
    c. Include a description of the authorized uses of the system.

## I. Device Lock [AC-11]

*NIST CSF Reference: None*

1. Agencies shall:
    a. Configure systems to initiate a device lock after a defined period of in-activity.
    b. Require users to initiate a device lock before leaving the system unattended.
2. Agencies shall ensure device locks are retained until the user reestablishes access using established identification and authentication procedures.

## J. Session Termination [AC-12]

*NIST CSF Reference: PR.AA-03*

Agencies shall automatically terminate a user session after defined conditions or events requiring session disconnect.

## K. Permitted Actions Without Identification and Authentication [AC-14]

*NIST CSF Reference: PR.AA-01*

Agencies shall identify user actions allowed on the system without identification or authentication, consistent with organizational mission and business functions, and document and provide supporting rationale in the security plan for the system.

## L. Remote Access [AC-17]

*NIST CSF Reference: PR.AA-05*

1. Remote Access [AC-17]:
   a. Agencies shall establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.
   b. Agencies shall authorize each type of remote access to the system prior to allowing such connections.
2. Monitoring and Control [AC-17 (1)]:

   Agencies shall employ automated mechanisms to monitor and control remote access methods.
3. Protection of Confidentiality and Integrity Using Encryption [AC-17 (2)]:

   Agencies shall implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
4. Managed Access Control Points [AC-17 (3)]:

   Agencies shall route remote accesses through authorized and managed network access control points.

## M. Wireless Access [AC-18]

*NIST CSF Reference: PR.AA-05*

1. Wireless Access [AC-18]:

   Agencies shall establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and authorize each type of wireless access to the system prior to allowing such connections.
2. Authentication and Encryption [AC-18 (1)]:

   Agencies shall protect wireless access to the system using authentication and encryption.

3. Disable Wireless Networking [AC-18 (3)]:

   Agencies shall disable, when not intended for use, wireless networking capabilities embedded within system components.

4. Restrict Configurations by Users [AC-18 (4)]:

   Agencies shall identify and explicitly authorize users allowed to independently configure wireless networking capabilities.

## N. Access Control for Mobile Devices [AC-19]

*NIST CSF Reference: PR.AA-05*

1. Access Control for Mobile Devices [AC-19]:
   a. Agencies shall establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas.
   b. Agencies shall authorize the connection of mobile devices to organizational systems.
2. Full Device or Container Based Encryption [AC-19 (5)]:

   Agencies shall employ encryption to protect the confidentiality and integrity of information on mobile devices.

## O. Use of External Systems [AC-20]

*NIST CSF Reference: ID.AM-02, ID.AM-04*

1. Use of External Systems [AC-20]:
   a. Agencies shall establish terms and conditions and identify controls asserted to be implemented on external systems consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to access the system from external systems, and process, store, or transmit organization-controlled information using external systems.
   b. Agencies shall prohibit the use of unauthorized types of external systems.
2. Limits on Authorized Use [AC-20 (1)]:

   Agencies shall store or transmit organization-controlled information only after:

   a. Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans.
   b. Retention of approved system connection or processing agreements.
3. Portable Storage Devices – Restricted Use [AC-20 (2)]:

   Agencies shall restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using defined restrictions.

4. Non-organizationally Owned Systems — Restricted Use [AC-20 (3)]:

   Agencies shall restrict the use of non-agency owned systems or system components to process, store or transmit agency information using agency-defined restrictions.

## P. Information Sharing [AC-21]

*NIST CSF Reference: None*

1. Agencies shall enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for information sharing circumstances where user discretion is required.
2. Agencies shall employ authorized automated mechanisms or manual processes to assist users in making information sharing and collaboration decisions.

## Q. Publicly accessible content [AC-22]

*NIST CSF Reference: None*

Agencies shall:

1. Designate individuals authorized to make information publicly accessible.
2. Train authorized individuals to ensure publicly accessible information does not contain nonpublic information.
3. Review the proposed content of information prior to posting onto the publicly accessible system.
4. Review the content on the publicly accessible system for nonpublic information and remove such information, if discovered.