Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: Access Control Policy
Policy Version: 1.1
Authority: A.C.A. § 25-1-128
Effective Date: 10/1/2024

Related Controls: 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

---

1. Purpose

To ensure that public and state entities of Arkansas have adequate controls to restrict access to systems and data. Access controls are necessary to ensure that only authorized users can obtain access to state information and systems. Access controls manage the admittance of users to system and network resources by granting users access only to the specific resources they require to complete their job-related duties.

2. Applicability

This policy applies to all systems and applications managed within public and state entities that store, process, or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

3. Definitions

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

4. Policy

a. Access to information systems will only be provided to users based on business requirements, job function, responsibilities, need-to-know and least privilege.
b. Requests for access will be formally documented and appropriately approved.
c. Application and service accounts must only be used by the components requiring authentication.

d. Standards shall be documented in accordance with NIST 800-53 Moderate and any applicable federal regulations and state laws.
e. Procedures shall be created to facilitate the implementation of the Access Control Standard and associated controls.
f. Reviews and updates to the current Access Control Policy, Standard, and Procedures will occur according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet.

5. Authority

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

6. Compliance

This control shall take effect upon publication. Compliance is expected with all public and state entity controls. Employees not following this public and state entity control are subject to the standard disciplinary procedures set by the entity.

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.

7. Related Documentation

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

8. Revision History

This policy shall be subject to periodic 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 Officer
07/01/2024	Updated for Compliance and Related Controls	Gary Vance, Chief Information Security Officer

Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: Awareness and Training Policy
Policy Version: 1.1
Authority: A.C.A. § 25-1-128
Effective Date: 10/1/2024

Related Controls: AC-03, AC-17, AC-22, AT-02, AT-03, AT-04, CP-03, IA-04, IR-02, IR-04, IR-07, IR-09, PL-04, PM-09, PM-12, PM-13, PM-14, PM-21, PM-23, PS-07, PS-08, PS-09, PT-02, SA-03, SA-08, SA-11, SA-16, SI-12, SR-05, SR-06, SR-11

---

1. Purpose

To ensure that public and state entities of Arkansas provide the appropriate level of information security awareness training to all users of Information Technology (IT).

2. Applicability

This policy applies to the workforce (employees, contractors, & vendors) of public and state entities, associated data centers, and related properties.

3. Definitions

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

4. Policy

a. Establish, document and maintain a security awareness training program that:
    - incorporates all applicable regulations, State and Federal laws;
    - provides role-based training;
    - is performed prior to the authorization of system access;
    - is monitored and tracked.
b. Standards shall be documented in accordance with NIST 800-53 Moderate and any applicable federal regulations and state laws.
c. Procedures shall be created to facilitate the implementation of the Awareness and Training Standard.
d. Reviews and updates to the current Awareness and Training Control Policy, Standard, and Procedures will occur according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet.
e. For regulated data areas (e.g., Centers for Medicare & Medicaid Services, Criminal Justice Information Services, Federal Tax Information), the State Cybersecurity Office

(SCSO) considers all employees as requiring the same level of security awareness training.

5. Authority

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

6. Compliance

This control shall take effect upon publication. Compliance is expected with all public and state entity controls. Employees not following this public and state entity control are subject to the standard disciplinary procedures set by the entity.

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.

7. Related Documentation

Awareness and Training Procedures
SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings
Standard_AT_Awareness and Training

8. Revision History

This policy shall be subject to periodic 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 Officer
07/01/2024	Updated for Compliance and Related Controls	Gary Vance, Chief Information Security Officer

Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: Audit and Logging Policy
Policy Version: 1.1
Authority: A.C.A. § 25-1-128
Effective Date: 10/1/2024

Related Controls: AC-02, AC-03,AC-05, AC-06, AC-07, AC-08, AC-16, AC-17, AU-02, AU-03, AU-04, AU-05, AU-06, AU-07, AU-08, AU-09, AU-11, AU-12, AU-14, AU-15, AU-16, CA-02, CA-07, CM-02, CM-03, CM-05, CM-06, CM-10, CM-11, CM-13, IA-02, IA-03, IA-05, IA-08, IR-04, IR-05, MA-04, MP-02, MP-04, MP-06, PE-03, PE-06, PE-2, PL-09, PM-07, PM-09, PM-12, PM-21, PS-08, PT-02, PT-07, RA-05, RA-08, SA-08, SC-07, SC-08, SC-18, SC-45, SI-03, SI-04, SI-07, SI-10, SI-11, SI-12

---

1. Purpose

To provide accurate and comprehensive audit logs in order to detect and react to inappropriate access to, or use of, information systems or data.

2. Applicability

This policy applies to all systems and applications managed within public and state entities that store, process, or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

3. Definitions

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

4. Policy

a. Access to information systems and data, as well as significant system events, must be logged by the information system.
b. Information system audit logs must be protected from unauthorized access or modification.
c. Information system audit logs must be retained for an appropriate period of time, based on the *Records Retention Standard* and State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet. Audit logs that have exceeded this retention period should be destroyed according to the *Electronic Media Destruction Standard and Procedure*.
d. Standards shall be documented in accordance with NIST 800-53 Moderate and any applicable federal regulations and state laws.
e. Procedures shall be created to facilitate the implementation of the Audit Standards.

f. Reviews and updates to the current Audit Policy, Standards, and Procedures will occur according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet.

5. Authority

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

6. Compliance

This control shall take effect upon publication. Compliance is expected with all public and state entity controls. Employees not following this public and state entity control are subject to the standard disciplinary procedures set by the entity.

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.

7. Related Documentation

Audit and Logging Procedures
Electronic Media Destruction Standard and Procedure
Records Retention Standard
SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings
Standard_AU_Audit and Accountability
Standard_AU_Audit and Logging

8. Revision History

This policy shall be subject to periodic 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
07/01/2024	Updated for Compliance and Related Controls	Gary Vance, Chief Information Security Officer

Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: Security Assessments and Authorizations Policy
Policy Version: 1.1
Authority: A.C.A. § 25-1-128
Effective Date: 10/1/2024

Related Controls: AC-02, AC-03, AC-04, AC-06, AC-17, AC-18, AC-19, AC-20, AT-04, AU-06, AU-13, AU-16, CA-02, CA-03, CA-05, CA-06, CA-07, CM-02, CM-03, CM-04, CM-06, CM-11, IA-03, IA-05, IR-04, IR-05, MA-02, MA-03, MA-04, PE-03, PE-06, PE-14, PE-16, PE-20, PL-02, PM-04, PM-06, PM-09, PM-10, PM-12, PM-14, PM-23, PM-28, PM-31, PS-07, PS-08, PT-07, RA-03, RA-05, RA-07, RA-10, SA-08, SA-09, SA-10, SA-11, SC-05, SC-07, SC-18, SC-38, SC-43, SI-02, SI-03, SI-04, SI-12, SR-02, SR-03, SR-06

---

1. Purpose

To ensure that public and state entities of Arkansas have security controls for information systems, and the environments in which those systems operate, as part of initial and ongoing security authorizations, annual assessments, continuous monitoring, and system development life cycle activities.

2. Applicability

This policy applies to all systems and applications managed within public and state entities that store, process, or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

3. Definitions

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

4. Policy

a. Develop a security assessment and authorization plan that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
b. Document and maintain the authorization of system interconnections with Interconnection Security Agreements (ISA).
c. Establish and implement a continuous monitoring program.
d. Internal system connections must be authorized and documented.
e. Standards shall be documented in accordance with NIST 800-53 Moderate and any applicable federal regulations and state laws.

f. Procedures shall be created to facilitate the implementation of the Security Assessments and Authorizations Standard.
g. Reviews and updates to the current Security Assessments and Authorizations Policy, Standard, and Procedures will occur according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet.

5. Authority

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

6. Compliance

This control shall take effect upon publication. Compliance is expected with all public and state entity controls. Employees not following this public and state entity control are subject to the standard disciplinary procedures set by the entity.

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.

7. Related Documentation

Security Assessments and Authorizations Procedures
SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings
Standard_CA_Security Assessments and Authorizations

8. Revision History

This policy shall be subject to periodic 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 Officer
07/01/2024	Updated for Compliance and Related Controls	Gary Vance, Chief Information Security Officer

Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: Configuration Management Policy
Policy Version: 1.1
Authority: A.C.A. § 25-1-128
Effective Date: 10/1/2024

Related Controls: AC-02, AC-03, AC-04, AC-05, AC-06, AC-17, AC-18, AC-19, AC-23, AU-02, AU-06, CA-07, CA-09, CM-01, CM-02, CM-03, CM-04, CM-05, CM-06, CM-07, CM-08, CM-09, CM-10, CM-11, CM-13, CP-02, CP-07, CP-09, CP-10, CP-12, IA-03, IA-05, MA-02, MA-06, MP-04, MP-05, PE-03, PE-16, PE-20, PL-02, PL-04, PL-08, PL-09, PM-05, PM-09, PM-16, PM-30, PS-06,PS-08, PT-06, RA-02, RA-03, RA-05, RA-08, SA-04, SA-05, SA-08, SA-09, SA-10, SA-11, SA-15, SA-17, SC-02, SC-03, SC-04, SC-07, SC-16, SC-18, SC-28, SC-34, SC-37, SC-39, SC-43, SC-44, SI-02, SI-03, SI-04, SI-06, SI-07, SI-10, SI-12, SR-04, SR-11

---

1. Purpose

To ensure that public and state entities of Arkansas have IT assets inventoried, documented with their interdependencies, and configured in compliance with IT security policies, standards, and procedures.

2. Applicability

This policy covers all systems developed by, or on behalf of public and state entities. This includes all development, test, quality assurance, production, and other ad hoc systems.

3. Definitions

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

4. Policy

a. A baseline for system configurations must be documented.
b. Systems must only be configured with least functionality.
c. Standards shall be documented in accordance with NIST 800-53 Moderate and any applicable federal regulations and state laws.
d. Procedures shall be created to facilitate the implementation of the Configuration Management Standard and associated access controls.
e. Reviews and updates to the current Configuration Management Policy, Standard, and Procedures will occur according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet.

5. Authority

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

6. Compliance

This control shall take effect upon publication. Compliance is expected with all public and state entity controls. Employees not following this public and state entity control are subject to the standard disciplinary procedures set by the entity.

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.

7. Related Documentation

Configuration Management Procedures
SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings
Standard_CM_Configuration Management
Standard_SI_System & Information Integrity

8. Revision History

This policy shall be subject to periodic review according to the 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
07/01/2024	Updated for Compliance and Related Controls	Gary Vance, Chief Information Security Officer

Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: Contingency Planning Policy
Policy Version: 1.1
Authority: A.C.A. § 25-1-128
Effective Date: 10/1/2024

Related Controls: AT-02, AT-03, AT-04, CM-08, CP-02, CP-03, CP-04, CP-06, CP-07, CP-08, CP-09, CP-10, CP-11, CP-13, IR-02, IR-03, IR-04, IR-06, IR-08, IR-09, MA-06, MP-02, MP-04, MP-05, PE-03, PE-11, PE-12, PE-17, PL-02, PM-08, PM-09, PM-11, PM-14, PS-08, RA-03, RA-09, SA-08, SA-15, SA-20, SC-07, SC-08, SC-12, SC-13, SC-23, SC-24, SC-28, SC-36, SI-04, SI-12, SI-13, SR-02

---

1. Purpose

To ensure that public and state entities of Arkansas have adequate controls in place for responding to a system emergency. This policy defines the overall contingency objectives and establishes the organizational framework and responsibilities for system contingency planning.

2. Applicability

This policy applies to all systems and applications managed within public and state entities that store, process, or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

3. Definitions

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

4. Policy

a. Contingency plans must be documented for information systems that are mission critical to public and state entities.
b. The plans must provide preventive measures, recovery strategies, and technical considerations in the event of a disruption.
c. Contingency plans must include the following:

- Procedures for restoring the information system, including the acquisition and maintenance of resources needed to facilitate the recovery and/or continuity of essential system functions;
- Processes for acquiring and maintaining the resources necessary to ensure viability of the restoration procedures;
- Training for personnel to execute contingency procedures;

- Assignment of responsibilities to designated staff or positions involved in the execution of the plan; and
- Readiness and preparedness procedures for the annual review and testing of the plan.

d. Standards shall be documented in accordance with NIST 800-53 Moderate and any applicable federal regulations and state laws.
e. Procedures shall be created to facilitate the implementation of the Contingency Planning Standard.
f. Reviews and updates to the current Contingency Planning Policy, Standard, and Procedures will occur according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet.

5. Authority

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

6. Compliance

This control shall take effect upon publication. Compliance is expected with all public and state entity controls. Employees not following this public and state entity control are subject to the standard disciplinary procedures set by the entity.

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.

7. Related Documentation

Contingency Planning Procedures for System Recovery
SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings
Standard_CP_Contingency Planning

8. Revision History

This policy shall be subject to periodic 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 Officer
07/01/2024	Updated for Compliance and Related Controls	Gary Vance, Chief Information Security Officer

Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: Identification and Authentication Policy
Policy Version: 1.1
Authority: A.C.A. § 25-1-128
Effective Date: 10/1/2024

Related Controls: AC-01, AC-02, AC-03, AC-04, AC-05, AC-06, AC-11, AC-14, AC-17, AC-18, AC-19, AU-01, AU-06, CA-03, CA-09, CM-06, IA-01, IA-02, IA-03, IA-04, IA-05, IA-06, IA-07, IA-08, IA-09, IA-10, IA-11, IA-12, MA-04, MA-05, PE-02, PE-03, PE-04, PL-04, PM-09, PM-12, PS-03, PS-04, PS-05, PS-08, RA-02, RA-03, SA-04, SA-08, SC-08, SC-12, SC-13, SC-17, SC-37, SI-04, SI-12

---

1. Purpose

To ensure that public and state entities of Arkansas have adequate controls to restrict access to systems and data to only users and devices who are properly identified and authenticated. Authentication controls are necessary to ensure that only authorized users and devices can obtain access to public and state entity information and systems.

2. Applicability

This policy applies to all systems and applications managed within public and state entities that store, process, or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

3. Definitions

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

4. Policy

a. Access to information systems will only be provided to users and devices when successfully identified and authenticated.
b. Requests for identification will be formally documented and appropriately approved.
c. Devices must only be used by the components requiring authentication.
d. Standards shall be documented in accordance with NIST 800-53 Moderate and any applicable federal regulations and state laws.
e. Procedures shall be created to facilitate the implementation of the Identification and Authentication Standard.
f. Reviews and updates to the current Identification and Authentication Policy, Standard, and Procedures will occur according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet.

5. Authority

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

6. Compliance

This control shall take effect upon publication. Compliance is expected with all public and state entity controls. Employees not following this public and state entity control are subject to the standard disciplinary procedures set by the entity.

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.

7. Related Documentation

Identification and Authentication Procedures
SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings
Standard_IA_Identification and Authentication

8. Revision History

This policy shall be subject to periodic 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 Officer
07/01/2024	Updated for Compliance and Related Controls	Gary Vance, Chief Information Security Officer

Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: Incident Response Policy
Policy Version: 1.1
Authority: A.C.A. § 25-1-128
Effective Date: 10/1/2024

Related Controls: AC-02, AC-19, AT-02, AT-03, AT-04, AU-06, AU-07, CM-06, CP-02, CP-03, CP-04, IR-02, IR-03, IR-04, IR-05, IR-06, IR-07, IR-08, IR-09, PE-06, PL-02, PM-05, PM-09, PM-12, PM-14, PM-22, PM-26, PS-08, SA-08, SA-09, SA-15, SC-05, SC-07, SI-03, SI-04, SI-07, SI-12, SI-18, SR-08

---

1. Purpose

To ensure that public and state entities of Arkansas have adequate controls in place for responding to a system emergency. This policy defines the requirements and responsibilities in reporting and responding to information security incidents or events in a manner that minimizes negative impacts to the confidentiality, integrity, and availability of public and state entity information.

2. Applicability

This policy applies to all systems and applications managed within public and state entities that store, process, or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

3. Definitions

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

4. Policy

a. All public and state entities must report to the CISO or designee any information security incident or event that has the potential to negatively impact the confidentiality, integrity, or availability of any information system that stores, processes, or transmits public and state entity information.
   - Information security incident reporting and its timeliness must be determined by risk and regulatory requirements and in accordance with the procedures defined in the Incident Response Standard.
   - Unsuccessful security incidents are foreseeable and expected, are not required to be reported, but may be reported if any uncertainty exists. Unsuccessful security incidents include, but are not limited to, pings on a firewall, unsuccessful attempts to log onto a system with an invalid password or username, unsuccessful attempts

to load malware, denial-of-service attacks that do not result in a server being taken off-line, and other events that do not result in actual impermissible use, disclosure, access or acquisition of public and state entity information resources or a substantial risk thereof.

b. The CISO or designee must direct information security incident responses and investigations in coordination and collaboration with the affected system owners.
c. The CISO or designee must be responsible for coordinating with any required external entities the reporting of information security incidents, such as regulators, Arkansas Attorney General, Arkansas Legislative Audit, contractual counterparties, affected data owners, or others as determined by the State Cybersecurity Office.
d. Standards shall be documented in accordance with NIST 800-53 Moderate and any applicable federal regulations and state laws.
e. Procedures shall be created to facilitate the implementation of the Incident Response Standard.
f. Reviews and updates to the current Incident Response Policy, Standard, and Procedures will occur according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet.

5. Authority

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

6. Compliance

This control shall take effect upon publication. Compliance is expected with all public and state entity controls. Employees not following this public and state entity control are subject to the standard disciplinary procedures set by the entity.

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.

7. Related Documentation

Incident Response Procedures
SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings
Standard_IR_Incident Response

8. Revision History

This policy shall be subject to periodic 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 Officer
07/01/2024	Updated for Compliance and Related Controls	Gary Vance, Chief Information Security Officer

Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: System Maintenance Policy
Policy Version: 1.1
Authority: A.C.A. § 25-1-128
Effective Date: 10/1/2024

Related Controls: AC-02, AC-03, AC-05, AC-06, AC-17, AU-02, AU-03, CM-02, CM-03, CM-04, CM-05, CM-08, CP-02, CP-07, IA-02, IA-04, IA-05, IA-08, MA-02, MA-04, MA-05, MP-02, MP-06, PE-02, PE-03, PE-16, PL-02, PM-09, PS-07, PS-08, RA-03, RA-07, SA-15, SC-07, SC-10, SI-02, SI-03, SI-07, SI-12, SI-13, SR-02, SR-03, SR-04, SR-11

---

1. Purpose

To ensure that public and state entity resources are maintained in compliance with IT security policies, standards, and procedures.

2. Applicability

This policy applies to all systems and applications managed within public and state entities that store, process, or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

3. Definitions

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

4. Policy

a. Schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or requirements conducted by the State Cybersecurity Office, local IT, and/or outsourced IT entities.
b. Approve and monitor all maintenance activities, whether performed on-site or remotely and whether the equipment is serviced on-site or removed to another location.
c. Ensure that system owners and IT approve, control, and monitor information system maintenance tools.
d. Approve and monitor non-local maintenance and diagnostic activities.
e. Document in the security plan for the information system, the policies and procedures for the establishment and use of non-local maintenance and diagnostic connections.
f. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.

g. Standards shall be documented in accordance with NIST 800-53 Moderate and any applicable federal regulations and state laws.
h. Procedures shall be created to facilitate the implementation of the System Maintenance Standard.
i. Reviews and updates to the current System Maintenance Policy, Standard, and Procedures will occur according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet.

5. Authority

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

6. Compliance

This control shall take effect upon publication. Compliance is expected with all public and state entity controls. Employees not following this public and state entity control are subject to the standard disciplinary procedures set by the entity.

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.

7. Related Documentation

System Maintenance Procedures
SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings
Standard_MA_Maintenance

8. Revision History

This policy shall be subject to periodic 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 Officer
07/01/2024	Updated for Compliance and Related Controls	Gary Vance, Chief Information Security Officer

Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: Media Protection Policy
Policy Version: 1.1
Authority: A.C.A. § 25-1-128
Effective Date: 10/1/2024

Related Controls: AC-03, AC-07, AC-16, AC-19, AC-20, AU-09, AU-11, CP-02, CP-06, CP-09, CP-10, MA-02, MA-03, MA-04, MA-05, MP-02, MP-03, MP-04, MP-05, MP-06, MP-07, PE-02, PE-03, PE-16, PE-22, PL-02, PL-04, PM-09, PM-12, PM-22, PS-08, SC-12, SC-13, SC-28, SC-34, SC-41, SI-12, SI-18, SI-19, SR-11

---

1. Purpose

To ensure that public and state entities of Arkansas control access to and dispose of media resources in compliance with IT security policies, standards, and procedures.

2. Applicability

This policy applies to all systems and applications managed within public and state entities that store, process, or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

3. Definitions

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

4. Policy

a. Organizational media must be labeled indicating the distribution limitations, handling caveats, and applicable security markings of digital and non-digital information media.
b. Media must be protected until it is destroyed or sanitized using approved equipment, techniques, and procedures.
c. Limit the transport of information system media to authorized personnel.
d. Standards shall be documented in accordance with NIST 800-53 Moderate and any applicable federal regulations and state laws.
e. Procedures shall be created to facilitate the implementation of the Media Protection Standard.
f. Reviews and updates to the current Media Protection Policy, Standard, and Procedures will occur according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet.

5. Authority

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

6. Compliance

This control shall take effect upon publication. Compliance is expected with all public and state entity controls. Employees not following this public and state entity control are subject to the standard disciplinary procedures set by the entity.

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.

7. Related Documentation

Media Protection Procedures
SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings
Standard_MP_Media Protection

8. Revision History

This policy shall be subject to periodic 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 Officer
07/01/2024	Updated for Compliance and Related Controls	Gary Vance, Chief Information Security Officer

Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: Physical and Environmental Protection Policy
Policy Version: 1.1
Authority: A.C.A. § 25-1-128
Effective Date: 10/1/2024

Related Controls: AC-17, AC-18, AT-03, AU-02, AU-06, AU-09, AU-12, AU-13, CA-07, CM-03, CM-08, CP-02, CP-07, CP-10, IA-03, IA-04, IA-08, IR-04, IR-08, MA-02, MA-03, MA-05, MP-02, MP-04, MP-05, PE-02, PE-03, PE-04, PE-05, PE-06, PE-08, PE-09, PE-10, PE-15, PE-18, PE-20, PM-09, PM-12, PS-02, PS-03, PS-04, PS-05, PS-06, PS-07, PS-08, RA-03, SC-07, SC-08, SC-28, SI-04, SI-12, SR-02, SR-03, SR-04, SR-06

---

1. Purpose

To ensure that that public and state entities of Arkansas information technology (IT) resources are protected by physical and environmental security measures that prevent physical tampering, damage, theft, or unauthorized physical access.

2. Applicability

This policy applies to all systems and applications managed within public and state entities that store, process, or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

3. Definitions

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

4. Policy

a. The data center information assets of public and state entities shall be protected from tampering, damage, theft, or unauthorized physical access.
b. Environmental controls shall be established, monitored, and maintained to prevent damage or failure.
c. Data center utilities services of public and state entities shall be secured, monitored, and maintained to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.
d. Standards shall be documented in accordance with NIST 800-53 Moderate and any applicable federal regulations and state laws.

e. Procedures shall be created to facilitate the implementation of the Physical and Environmental Protection Standard.
f. Reviews and updates to the current Physical and Environment Protection Policy, Standard, and Procedures will occur according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet.

5. Authority

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

6. Compliance

This control shall take effect upon publication. Compliance is expected with all public and state entity controls. Employees not following this public and state entity control are subject to the standard disciplinary procedures set by the entity.

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.

7. Related Documentation

Physical and Environmental Protection Procedures
SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings
Standard_ PE_Physical and Environmental Protection

8. Revision History

This policy shall be subject to periodic 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 Officer
07/01/2024	Updated for Compliance and Related Controls	Gary Vance, Chief Information Security Officer

Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: Planning Policy
Policy Version: 1.1
Authority: A.C.A. § 25-1-128
Effective Date: 10/1/2024

Related Controls: AC-02, AC-06, AC-08, AC-09, AC-14, AC-17, AC-18, AC-19, AC-20, AC-22, AT-02, AT-03, AU-13, CA-02, CA-03, CA-07, CM-02, CM-06, CM-09, CM-11, CM-13, CP-02, CP-04, IA-02, IA-04, IA-05, IR-04, IR-08, MA-04, MA-05, MP-04, MP-05, MP-07, PL-02, PL-07, PL-08, PL-09, PL-10, PL-11, PM-01, PM-05, PM-07, PM-08, PM-09, PM-10, PM-11, PS-06, PS-08, RA-02, RA-03, RA-08, RA-09, SA-03, SA-05, SA-08, SA-17, SA-22, SC-07, SI-12, SR-02, SR-04

---

1. Purpose

To ensure that information technology resources are established with effective security controls and control enhancements that reflect applicable federal and state laws.

2. Applicability

This policy applies to all systems and applications managed within public and state entities that store, process, or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

3. Definitions

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

4. Policy

a. System Security Plans shall be developed for all systems.
b. Establish rules of behavior that include responsibilities and expected behavior regarding system usage.
c. Develop information security architecture that facilitates a defense-in-depth approach for organizational protection.
d. Standards shall be documented in accordance with NIST 800-53 Moderate and any applicable federal regulations and state laws.
e. Procedures shall be created to facilitate the implementation of the Planning Standard.
f. Reviews and updates to the current Planning Policy, Standard, and Procedures will occur according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet.

5. Authority

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

6. Compliance

This control shall take effect upon publication. Compliance is expected with all public and state entity controls. Employees not following this public and state entity control are subject to the standard disciplinary procedures set by the entity.

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.

7. Related Documentation

Planning Procedures
SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings
Standard_PL_Planning

8. Revision History

This policy shall be subject to periodic 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 Officer
07/01/2024	Updated for Compliance and Related Controls	Gary Vance, Chief Information Security Officer

Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: Program Management Policy
Policy Version: 1.1
Authority: A.C.A. § 25-1-128
Effective Date: 10/1/2024

---

1. Purpose

To ensure that public and state entities of Arkansas security considerations are planned for early and handled consistently in the project lifecycle.

2. Applicability

This policy applies to all systems and applications managed within public and state entities that store, process, or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

3. Definitions

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

4. Policy

a. Establish, document, and maintain the requirements for the security program.
b. Standards shall be documented in accordance with NIST 800-53 Moderate and any applicable federal regulations and state laws.
c. Procedures shall be created to facilitate the implementation of the Program Management Standard.
d. Review and update the current Program Management Policy, Standard, and Procedures will occur according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet.

5. Related Controls

NIST: AC-1, AC-2, AC-3, AC-4, AC-6, AC-17, AT-1, AT-2, AT-3, AT-4, AU-1, AU-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-1, CA-2, CA-5, CA-6, CA-7, CM-1, CM-3, CM-4, CM-6, CM-8, CM-10, CM-11, CM-12, CM-13, CP-1, CP-2, CP-4, IA-1, IA-4, IA-5, IR-1, IR-3, IR-4, IR-5, IR-7, IR-9, MA-1, MA-2, MA-3, MA-4, MP-1, MP-7, PE-1, PE-14, PE-16, PE-18, PE-2, PE-3, PE-6, PE-20, PL-1, PL-2, PL-8, PS-1, PS-3, PS-4, PS-5, PS-7, PS-8, PT-1, PT-2, PT-3, PT-5, PT-6, PT-7, PT-8, RA-1, RA-2, RA-3, RA-5, RA-7, RA-8, RA-9, SA-1, SA-2, SA-3, SA-4, SA-8, SA-

9, SA-11, SA-17, SC-1, SC-5, SC-7, SC-18, SC-38, SC-43, SI-1 , SI-3, SI-4, SI-5, SI-12, SI-18, SI-19, SR-1, SR-2, SR-3, SR-4, SR-5, SR-6, SR-7, SR-8, SR-9, SR-11

6. Authority

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

7. Compliance

This control shall take effect upon publication. Compliance is expected with all public and state entity controls. Employees not following this public and state entity control are subject to the standard disciplinary procedures set by the entity.

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.

8. Related Documentation

Program Management Procedures
SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings
Standard_PM_Program Management

9. Revision History

This policy shall be subject to periodic 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 Officer
07/01/2024	Updated for Compliance	Gary Vance, Chief Information Security Officer

Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: Personnel Security Policy
Policy Version: 1.1
Authority: A.C.A. § 25-1-128
Effective Date: 10/1/2024

Related Controls: AC-02, AC-05, AC-17, AT-02, AT-03, IA-04, MA-05, PE-02, PE-03, PL-02, PL-04, PM-09, PM-12, PS-02, PS-03, PS-04, PS-05, PS-06, PS-07, PS-08, PT-01, SA-05, SA-09, SA-21, SI-12

---

1. Purpose

To ensure that public and state entities of Arkansas security safeguards for personnel are applied to the access and use of information technology resources and data.

2. Applicability

This policy applies to the workforce (employees, contractors & vendors) of public and state entity data centers and related properties.

3. Definitions

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

4. Policy

a. Ensure personnel screening and rescreening activities reflect applicable state and federal laws, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions.
b. Develop and document access agreements for information systems.
c. Ensure that individuals requiring access to information and information systems sign appropriate access agreements prior to being granted access.
d. Require third-party providers to comply with personnel security policies and procedures established by the entity.
e. Standards shall be documented in accordance with NIST 800-53 Moderate and any applicable federal regulations and state laws.
f. Procedures shall be created to facilitate the implementation of the Personnel Security Standard.
g. Reviews and updates to the current Personnel Security Policy, Standard, and Procedures will occur according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet.

5. Authority

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

6. Compliance

This control shall take effect upon publication. Compliance is expected with all public and state entity controls. Employees not following this public and state entity control are subject to the standard disciplinary procedures set by the entity.

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.

7. Related Documentation

Personnel Security Procedures
SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings
Standard_PS_Personnel Security

8. Revision History

This policy shall be subject to periodic 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 Officer
07/01/2024	Updated for Compliance and Related Controls	Gary Vance, Chief Information Security Officer

Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: PII Processing and Transparency Policy
Policy Version: 1.1
Authority: A.C.A. § 25-1-128
Effective Date: 10/1/2024

Related Controls: AC-2, AC-3, AC-16, AT-3, CA-6, CM-12, CM-13, IA-4, IR-9, PM-5, PM-9, PM-20, PM-21, PM-22, PM-24, PM-25, RA-3, RA-8, SC-16, SC-42, SC-43, SI-10, SI-12, SI-15, SI-18, SI-19

---

1. Purpose

To establish requirements for public and state entities of Arkansas to safeguard the collection, access, use, dissemination, and storage of personally identifiable information (PII).

2. Applicability

This policy applies to all systems and applications managed within public and state entities that store, process, or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

3. Definitions

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

4. Policy

a. Establish, document, and maintain requirements for personally identifiable information processing and transparency that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance with data center policies and standards.
b. Standards shall be documented in accordance with NIST 800-53 Moderate and any applicable federal regulations and state laws.
c. Procedures shall be created to facilitate the implementation of the PII Processing and Transparency Standard.
d. Reviews and updates to the current PII Processing and Transparency Policy, Standard, and Procedures will occur according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet.

5. Authority

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

6. Compliance

This control shall take effect upon publication. Compliance is expected with all public and state entity controls. Employees not following this public and state entity control are subject to the standard disciplinary procedures set by the entity.

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.

7. Related Documentation

PII Processing and Transparency Procedures
SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings
Standard_PT_PII Processing and Transparency

8. Revision History

This policy shall be subject to periodic 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 Officer
07/01/2024	Updated for Compliance	Gary Vance, Chief Information Security Officer
12/19/2024	Moved “Related Controls” to the header.	Ray Girdler, State IT Security Specialist

Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: Risk Assessment Policy
Policy Version: 1.1
Authority: A.C.A. § 25-1-128
Effective Date: 10/1/2024

Related Controls: CA-02, CA-03, CA-05, CA-06, CA-07, CA-08, CM-02, CM-04, CM-06, CM-08, CM-13, CP-02, CP-06, CP-07, IA-08, IR-09, MA-05, MP-04, PE-03, PE-08, PE-18, PL-02, PL-08, PL-10, PL-11, PM-01, PM-04, PM-07, PM-08, PM-09, PM-11, PM-17, PM-28, PM-30, PS-08, PT-02, PT-07, RA-02, RA-03, RA-05, RA-07, RA-08, RA-09, SA-08, SA-09, SA-11, SA-15, SA-20, SC-07, SC-38, SI-02, SI-03, SI-04, SI-05, SI-07, SI-12, SR-02, SR-05, SR-11

---

1. Purpose

To establish a set of management processes to assess risks and implement plans to address them within public and state entities of Arkansas. The risk assessment will determine risk priorities and the probability of identified risk. Effective implementation will maximize security and minimize the potential exploitation of risk to information and technology.

2. Applicability

This policy covers all systems developed by, or on behalf of public and state entities. This includes all development, test, quality assurance, production, and other ad hoc systems.

3. Definitions

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

4. Policy

a. Organizational risk must be identified, continuously monitored, and controlled.
b. Risk assessments must identify, quantify, and prioritize risk acceptance and objectives relevant to public and state entities.
c. Applicable security requirements will be monitored for updates and risk reassessed within public and state entities when published.
d. Standards shall be documented in accordance with NIST 800-53 Moderate and any applicable federal regulations and state laws.
e. Procedures shall be created to facilitate the implementation of the Risk Assessment Standard and associated controls.

f. Reviews and updates to the current Risk Assessment Policy, Standard, and Procedures will occur according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet.

5. Authority

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

6. Compliance

This control shall take effect upon publication. Compliance is expected with all public and state entity controls. Employees not following this public and state entity control are subject to the standard disciplinary procedures set by the entity.

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.

7. Related Documentation

Risk Assessment Procedures
SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings
Standard_RA_Risk Assessment

8. Revision History

This policy shall be subject to periodic 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 Officer
07/01/2024	Updated for Compliance and Related Controls	Gary Vance, Chief Information Security Officer

Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: System and Services Acquisition Policy
Policy Version: 1.1
Authority: A.C.A. § 25-1-128
Effective Date: 10/1/2024

Related Controls: AC-20, AT-03, CA-02, CA-03, CA-07, CM-02, CM-03, CM-04, CM-06, CM-07, CM-08, CM-09, CP-02, IA-02, IA-08, IR-04, IR-07, MA-06, PL-02, PL-04, PL-07, PL-08, PL-10, PL-11, PM-03, PM-07, PM-09, PM-11, PS-02, PS-07, PS-08, RA-02, RA-03, RA-09, SA-02, SA-03, SA-04, SA-05, SA-08, SA-09, SA-10, SA-11, SA-15, SA-16, SA-17, SA-20, SA-21, SA-22, SC-02, SC-03, SC-32, SC-39, SI-02, SI-12, SR-02, SR-03, SR-04, SR-05, SR-06, SR-07, SR-09

---

1. Purpose

To ensure that resources and information systems for public and state entities of Arkansas are acquired with security requirements to meet the information systems mission and business objectives.

2. Applicability

This policy applies to all systems and applications managed within public and state entities that store, process, or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

3. Definitions

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

4. Policy

a. Determine, document, and allocate the resources required to protect the information systems as part of the capital planning and investment control process.
b. The system development life cycle must include information security risk management processes.
c. Public and state entities shall manage information systems using the system development life cycle to ensure incorporation of information security considerations.
d. The acquisition process must include security requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service.

e. Require that providers of external information system services comply with organizational information security requirements and employ security controls in accordance with data center policies, standards, and procedures.
f. Standards shall be documented in accordance with NIST 800-53 Moderate and any applicable federal regulations and state laws.
g. Procedures shall be created to facilitate the implementation of the System and Services Acquisition Standard.
h. Reviews and updates to the current System and Services Acquisition Policy, Standard, and Procedures will occur according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet.

5. Authority

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

6. Compliance

This control shall take effect upon publication. Compliance is expected with all public and state entity controls. Employees not following this public and state entity control are subject to the standard disciplinary procedures set by the entity.

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.

7. Related Documentation

System and Services Acquisition Procedures
SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings
Standard_SA_System and Services Acquisition

8. Revision History

This policy shall be subject to periodic 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 Officer
07/01/2024	Updated for Compliance and Related Controls	Gary Vance, Chief Information Security Officer

Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: System and Communications Protection Policy
Policy Version: 1.1
Authority: A.C.A. § 25-1-128
Effective Date: 10/1/2024

Related Controls: AC-02, AC-03, AC-04, AC-06, AC-07, AC-17, AC-18, AC-19, AC-20, AC-21, AC-25, AU-02, AU-09, AU-10, AU-12, AU-13, CA-03, CA-07, CM-02, CM-03, CM-04, CM-05, CM-06, CM-07, CM-10, CM-11, CP-02, CP-08, CP-09, CP-10, IA-03, IA-05, IA-07, IA-08, IA-09, IR-04, MA-04, MP-02, MP-04, MP-05, PE-03, PE-04, PL-08, PM-09, PM-12, PS-08, SA-04, SA-08, SA-09, SA-17, SC-02, SC-03, SC-05, SC-06, SC-07, SC-08, SC-10, SC-11, SC-12, SC-13, SC-16, SC-17, SC-20, SC-21, SC-22, SC-23, SC-24, SC-26, SC-28, SC-32, SC-34, SC-35, SC-37, SC-39, SC-40, SC-42, SC-43, SI-03, SI-07, SI-12, SI-16

---

1. Purpose

To establish a set of rules to properly create network segmentation, boundary protection, and cryptography implementation within public and state entities of Arkansas. Effective implementation will maximize security and minimize the potential risk of unauthorized access to information and technology.

2. Applicability

This policy covers all systems developed by, or on behalf of public and state entities. This includes all development, test, quality assurance, production, and other ad hoc systems.

3. Definitions

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

4. Policy

a. Organizational communications must be monitored, controlled, and protected (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
b. Secure architectural designs, software development techniques, and systems engineering must be used within organizational information systems.
c. Subnetworks for publicly accessible system components must be physically or logically separated from internal networks.

d. Cryptographic mechanisms must be utilized to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical safeguards.
e. Standards shall be documented in accordance with NIST 800-53 Moderate and any applicable federal regulations and state laws.
f. Procedures shall be created to facilitate the implementation of the System and Communications Protection Standard and associated controls.
g. Reviews and updates to the current System and Communications Protection Policy, Standard, and Procedures will occur according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet.

5. Authority

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

6. Compliance

This control shall take effect upon publication. Compliance is expected with all public and state entity controls. Employees not following this public and state entity control are subject to the standard disciplinary procedures set by the entity.

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.

7. Related Documentation

System and Communications Protection Procedures
SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings
Standard_SC_System Communications

8. Revision History

This policy shall be subject to periodic 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 Officer
07/01/2024	Updated for Compliance and Related Controls	Gary Vance, Chief Information Security Officer

Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: System and Information Integrity Policy
Policy Version: 1.1
Authority: A.C.A. § 25-1-128
Effective Date: 10/1/2024

Related Controls: AC-02, AC-03, AC-04, AC-08, AC-16, AC-17, AC-19, AC-25, AU-02, AU-03, AU-04, AU-05, AU-06, AU-07, AU-09, AU-11, AU-12, AU-13, AU-14, CA-02, CA-03, CA-05, CA-06, CA-07, CA-09, CM-03, CM-04, CM-05, CM-06, CM-07, CM-08, CM-09, CM-11, CP-02, IA-10, IR-04, IR-05, IR-08, MA-02, MA-03, MA-04, MP-02, MP-03, MP-04, MP-06, PE-06, PL-02, PL-04, PL-09, PM-04, PM-08, PM-09, PM-12, PM-15, PM-23, PM-25, PS-02, PS-06, PS-08, PT-02, PT-03, RA-02, RA-03, RA-05, RA-10, SA-05, SA-08, SA-09, SA-10, SA-11, SC-03, SC-05, SC-07, SC-08, SC-12, SC-13, SC-18, SC-23, SC-26, SC-28, SC-31, SC-35, SC-36, SC-37, SC-38, SC-43, SC-44, SI-02, SI-03, SI-04, SI-05, SI-06, SI-07, SI-08, SI-11, SI-12, SI-15, SR-02, SR-03, SR-04, SR-05, SR-06, SR-09, SR-10, SR-11

---

1. Purpose

To ensure that resources and information systems for public and state entities of Arkansas are established with system integrity monitoring to include areas of concern such as malware, application and source code flaws, industry supplied alerts and remediation of detected or disclosed integrity issues.

2. Applicability

This policy applies to all systems and applications managed within public and state entities that store, process, or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

3. Definitions

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

4. Policy

a. Identify, report, and correct information system flaws.
b. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.
c. Monitor the information system to detect attacks, indicators of potential attacks, unauthorized local, network, and remote connections.
d. Generate internal security alerts, advisories, and directives as deemed necessary.

e. Ensure the integrity of software, firmware, and information.
f. Standards shall be documented in accordance with NIST 800-53 Moderate and any applicable federal regulations and state laws.
g. Procedures shall be created to facilitate the implementation of the System and Information Integrity Standard.
h. Reviews and updates to the current System and Information Integrity Policy, Standard, and Procedures will occur according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet.

5. Authority

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

6. Compliance

This control shall take effect upon publication. Compliance is expected with all public and state entity controls. Employees not following this public and state entity control are subject to the standard disciplinary procedures set by the entity.

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.

7. Related Documentation

System and Information Integrity Procedures
SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings
Standard_SI_System and Information Integrity

8. Revision History

This policy shall be subject to periodic 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 Officer
07/01/2024	Updated for Compliance and Related Controls	Gary Vance, Chief Information Security Officer

Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: Supply Chain Risk Management Policy
Policy Version: 1.1
Authority: A.C.A. § 25-1-128
Effective Date: 10/1/2024

Related Controls: AT-03, CA-02, CM-03, CP-04, IR-04, IR-06, IR-08, MA-02, MA-04, MA-06, MP-06, PE-03, PE-16, PL-02, PL-08, PM-09, PM-30, PS-08, RA-03, RA-07, SA-02, SA-03, SA-04, SA-05, SA-08, SA-09, SA-10, SA-15, SC-07, SC-29, SC-30, SC-38, SI-04, SI-07, SI-12, SR-03, SR-04, SR-05, SR-06, SR-09, SR-10, SR-11

---

1. Purpose

To ensure that information technology resources and information systems are acquired with security requirements to meet the mission and business objectives for public and state entities of Arkansas.

2. Applicability

This policy applies to all systems and applications managed within public and state entities that store, process, or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

3. Definitions

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

4. Policy

a. Identify information security requirements for the information system or information system service in mission/business process planning.
b. Protect the information system or information system service as part of the capital planning process.
c. Standards shall be documented in accordance with NIST 800-53 Moderate and any applicable federal regulations and state laws.
d. Procedures shall be created to facilitate the implementation of the Supply Chain Risk Management Standard.
e. Reviews and updates to the current Supply Chain Risk Management Policy, Standard, and Procedures according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet.

5. Authority

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

6. Compliance

This control shall take effect upon publication. Compliance is expected with all public and state entity controls. Employees not following this public and state entity control are subject to the standard disciplinary procedures set by the entity.

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.

7. Related Documentation

Supply Chain Risk Management Procedures
SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings
Standard_SR_Supply Chain Risk Management

8. Revision History

This policy shall be subject to periodic 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 Officer
07/01/2024	Updated for Compliance and Related Controls	Gary Vance, Chief Information Security Officer

Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: Technology Resources Policy
Policy Version: 1.0
Authority: A.C.A. § 25-1-128
Effective Date: 1/1/2024

---

1. Purpose

To ensure responsible and lawful utilization of state technology resources with public and state entities of Arkansas.

2. Applicability

This policy applies to all individuals, including employees, contractors, and users of state resources, associated with public and state entities.

3. Definitions

Technology resources means:

a. The machines, devices, and transmission facilities used in information processing, including computers, word processors, terminals, telephones, cables, software, and related products;

b. The devices used to process information through electronic capture, collection, storage, manipulation, transmission, retrieval, and presentation of information in the form of data, text, voice, or image and includes telecommunications and office automation functions;

c. Any component related to information processing and wired and wireless telecommunications, including data processing and telecommunications hardware, software, services, planning, personnel, facilities, and training;

d. The procedures, equipment, and software that are designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and the associated personnel, including consultants and contractors; and

e. All electronic mail accounts issued by a public entity.

4. Policy

State technology resources shall only be used in an approved manner. They shall not be used to:

a. Express a political opinion to an elected official unless the opinion is:
    a. Within the scope of the employee's regular job duties; or
    b. Requested by an elected official or public entity.

b. Engage in lobbying an elected official on a personal opinion if the employee is not a registered lobbyist for the public entity;

c. Engage in illegal activities or activities otherwise prohibited by federal law or state law; or

d. Intentionally override or avoid the security and system integrity procedures of the public entity.

5. Authority

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

6. Compliance

This control shall take effect upon publication. Compliance is expected with all public and state entity controls. Employees not following this public and state entity control are subject to the standard disciplinary procedures set by the entity.

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.

7. Related Documentation

SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings

8. Revision History

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

Date	Description of Change	Reviewer
07/01/2024	Moved from Draft to Final	Gary Vance, Chief Information Security Officer

Department of Transformation and Shared Services
State Cybersecurity Office

Standard Title: Cloud Security Standard
Standard Version: 1.1
Effective Date: 06/01/2022

---

1. Introduction

Historically, servers and other computing resources were planned, procured, configured, deployed, and maintained within a closed system by trusted network architects with clearly defined roles and responsibilities, and strict security standards, policies, procedures, and oversight.

The cloud changed all that – with only a credit card, anyone can deploy a complete infrastructure in matters of minutes, exposing confidential assets and putting a company's reputation in jeopardy.

1.1 Purpose

This document establishes the necessary security requirements to ensure the security of state data in the cloud.

1.2 Scope

This standard applies to cloud platform(s) managed by DIS.

1.3 Authority

The DIS Director and Chief Information Security Officer (CISO) are the designated authority over state networks and state information assets managed by DIS under TSS. As a result, DIS designates the teams and authorizes the processes necessary to secure cloud platforms and related services in use at DIS.

1.4 Roles and Responsibilities

The following standard outlines the primary role(s) associated with state policy, including responsibilities and expectations.

1.4.1. Cloud Engineer

The Cloud Engineer is responsible for implementing and maintaining the operational controls necessary to support the requirements defined in this document.

2. Standard

2.1. Implementation Priority

Each cloud security requirement has an implementation priority, which is defined in the table below.

Implementation Priority	Requirement(s)
HIGH	These controls MUST be implemented for ALL Cloud Environments. All controls marked as HIGH MUST be implemented and validated before any sensitive data is loaded to the Cloud environment.
MEDIUM	These controls must be implemented in due course of the project, with explicitly defined completion dates that are tracked by the project manager or DIS State Cyber Security Office (SCSO) team.
LOW	These controls are to be addressed in due course of the operating model or project, with explicitly defined completion dates that are tracked by the project manager or DIS SCSO.

2.2. Cloud Security Requirements

The following table identifies the Cloud Security Requirements for implementation:

Policy Control ID	Requirement(s)	Implementation Priority	Standard Requirement(s)
DIS-01	The use of a cloud platform root account or like account access with full administration privileges shall be limited. Any use of such credentials shall require multi-factor authentication.	HIGH	The use of root or like account access with full administrative privileges is applied leveraging least privilege practice, limiting the number of employees, and having alert notification when accessed.

		HIGH	All cloud accounts that have elevated privileges are periodically reviewed to ensure utilization of least privilege, that the number of employees with access is limited, and no unauthorized access during the period.
Policy Control ID	Requirement(s)	Implementation Priority	Standard Requirement(s)
		MEDIUM	Upon creation, any access keys associated with a root or like account access are deleted or disabled. In cases where use of root or like accounts with access keys are required, alerts are generated when active keys are associated with them.
		LOW	Multi-factor authentication (MFA) is enabled and monitored to alert if it is disabled.
		MEDIUM	Security questions are registered for the root account, as necessary to permit emergency recovery.
		MEDIUM	A process is utilized to validate, authorize, and permit usage of the "root" or "Super User" account in the case of emergency. Logging of such access is active and immutable.
		HIGH	MFA is enabled and monitored for all accounts with console access.
DIS-02	Multi-factor authentication (MFA) shall be required for all cloud platform accounts with interactive console access.	HIGH	Access management is governed by automated SSO capabilities and dispositioned through upstream capability.

Policy Control ID	Requirement(s)	Implementation Priority	Standard Requirement(s)
DIS-03	All cloud platform accounts with interactive console access that have been inactive for more than 90 days shall be removed or deactivated. All access keys shall be rotated at least every 90 days.	HIGH	Access keys are rotated for service accounts.
		HIGH	The password and other credentials configuration for the accounts are examined upon creation, after major system updates, and when changes are made to DIS security policy to ensure compliance with all DIS policies regarding complexity, composition, length, re-use, rotation, and recovery.
DIS-04	The cloud platform password policy for interactive console accounts must enforce complexity that adheres to DIS policy requirements.	HIGH	Inline and other policies are prohibited and prevented from being directly attached to a user. A registry of exceptions of inline policies is maintained and reviewed periodically. Periodic reviews or automated monitoring and alerting of user access is required to ensure that no prohibited access has been attached.
DIS-05	Cloud platform interactive console policies shall only be applied to groups or roles but never directly to individual user accounts	MEDIUM	Sufficient and adequate contact information is made available to the cloud provider and DIS maintains current cloud provider contact information.

Policy Control ID	Requirement(s)	Implementation Priority	Standard Requirement(s)
DIS-06	All pertinent security and support contact information shall be made available to the cloud platform provider and maintained to ensure current, sufficient information is available in the event of an incident.	MEDIUM	Contact information is available to cloud providers and is kept current and accurate.
		MEDIUM	A responsible group or role is assigned to maintain current and accurate cloud provider contact information.
		MEDIUM	A support role to manage incidents exists and is maintained.
		HIGH	Cloud compute instances utilize roles for authentication and authorization to resources in lieu of stored credentials. Periodic reviews or automated monitoring are employed to ensure compliance. Exceptions are noted and checked periodically for continued visibility.
DIS-07	All access within cloud platform compute instances shall utilize roles for authentication and authorization, in lieu of stored credentials.	HIGH	Logging of all security relevant events is enabled and verified in all regions. Logged information is sufficient to attribute any security relevant action to the responsible individual or entity. Logs are securely retained for a minimum of four years and made readily available to security staff in real-or near-real time.
DIS-08	Logging of all security relevant events and account activity shall be enabled, captured, monitored, and appropriately alarmed for all cloud platform regions in accordance with all applicable policies.	HIGH	Logs are appropriately captured and integrated with a processing sub-system capable of visualizing, identifying anomalies, and generating alerts. Such integration of logs is verified.

		HIGH	Programmatic credentials (i.e., access keys and access secret(s) are not created for user accounts. Machine identities, i.e., service accounts, shall not have interactive console access.
DIS-09	User accounts shall not have access keys and access secrets. Service accounts shall not perform interactive login.	MEDIUM	Evidence demonstrating the effectiveness of this control is periodically reviewed to ensure that interactive users do not have programmatic access and that accounts requiring programmatic access do not have interactive access. Exceptions are noted and checked periodically for continued visibility. Security and administrative personnel are notified when an account violates policy.
		HIGH	Log configuration is periodically checked to validate configuration settings that ensure log security and availability.
DIS-10	Cloud platform logs shall be protected against unauthorized modification and stored in a forensically sound manner.	HIGH	Identity and access management policies are checked programmatically to validate that no policies allow full administrative privileges such as “Effect”, “Allow” with “Action” over “Resource.”
DIS-11	Full administrative privileges shall not be created for any cloud platform Identity and Access Management (IAM) policies.	HIGH	Unauthorized notification of logs is prevented through the restriction of access to the minimum necessary and the required use of robust authentication and authorization.

Policy Control ID	Requirement(s)	Implementation Priority	Standard Requirement(s)
DIS-12	Public access to cloud platform logs shall be strictly prohibited.	HIGH	Activity logging is enabled and monitored on all log storage mechanisms.

		HIGH	Verification that configuration management and tracking is enabled for all regions is required. Programmatic notification of attempted and successful changes to configuration management settings is required.
DIS-13	Configuration management and tracking shall be enabled for all cloud platform regions	HIGH	Access to configuration management changes and data is restricted based on least privilege. (Programmatic notification of attempted and successful changes to permissions of configuration management settings is required.
		HIGH	Access to log storage media and systems is monitored and reviewed to ensure continued prevention of unauthorized access and modification.
DIS-14	Access to cloud platform log storage media and systems shall be strictly controlled to prevent unauthorized access and modification.	MEDIUM	Verification of log file encryption is required.

Policy Control ID	Requirement(s)	Implementation Priority	Standard Requirement(s)
DIS-15	All cloud platform log storage media and systems shall employ encryption at rest.	HIGH	Validation of the rotation of keys is required, including symmetric keys used for authentication, encryption keys, and keys used to secure transport protocols.
DIS-16	Cloud platform customer created Customer Master Keys (CMKs) used to protect sensitive and/or confidential data shall be rotated	HIGH	Processes and procedures are employed to monitor, require, and validate the rotation of keys, depending upon the

	in accordance with applicable policy.		implementation and mechanism(s) used to manage encryption. Product owner ensures that contractually the application must support annual key rotation, at a minimum.
		HIGH	Verification of required logging is required.
DIS-17	Logging of security relevant events in all relevant regions shall be enabled for all cloud platform compute resources and virtual networking capabilities, in accordance with applicable policy.	HIGH	Network traffic, including Virtual Private Cloud (VPC) flow logs, is logged and retained in accordance with DIS policy.
		HIGH	Log metric filters and alarms should be identified, collected, validated, and maintained in the preferred state.
DIS-18	Cloud platform log metric filters and alarms shall be established and maintained for all pertinent services, and events shall be monitored appropriately.	HIGH	Unauthorized Application Programming Interface (API) calls, including both external APIs within the control ("endpoints") and API calls within the cloud service/platform.

Policy Control ID	Requirement(s)	Implementation Priority	Standard Requirement(s)
DIS-18 (Continued)		HIGH	Changes in logging mechanisms and processes, such as suspension or disablement, modification, and unauthorized access attempts.
		HIGH	Changes to compute services, including virtual instances and networking, unauthorized actions, or access requests.
		HIGH	Successful and unsuccessful login attempts to interactive resources such as a web console or portal without Multi-Factor Authentication (MFA) and all unsuccessful attempts.

		HIGH	Use of root account
		HIGH	Disablement, scheduled deletion, modification, or permissions related to encryption keys and key management systems.
		HIGH	Changes to policy, including unauthorized actions or access requests.
		HIGH	Changes to storage services, including unauthorized actions or access requests.
		HIGH	Changes to configuration management services, including unauthorized actions or access requests.
Policy Control ID	Requirement(s)	Implementation Priority	Standard Requirement(s)
DIS-18 (Continued)		HIGH	Changes to network access such as network access control lists, security groups, route tables, and network gateways, including unauthorized actions or access requests.
		MEDIUM	Alerts for the above are generated and delivered to the SCSO. All alarms are routinely validated to ensure they are functioning properly.
		HIGH	Network interfaces and security groups restrict inbound access to all interactive services and ports, such as restricting by IP address, ports, and other means.

DIS-19	Inbound access to ports on the cloud platform shall be restricted to the minimum necessary for remote connectivity and administrative access.	HIGH	Inbound connectivity is restricted to not be overly broad, particularly for services that are used for remote interactive connectivity and administration.
		HIGH	Rules are defined to control network traffic in and out of network interfaces and to implicitly deny all other traffic.
DIS-20	Ingress and egress of cloud platform network traffic shall be strictly controlled.	HIGH	Routing tables for peer-to-peer network services restrict to least access.
DIS-21	Cloud platform routing tables for network interface peering shall be set to "least access."	HIGH	Default should be deny.

3. Inquiries

Direct inquiries about this policy to:
Division of Information Systems
State Cybersecurity Office
Little Rock, Arkansas 72201
Email: SCSO@arkansas.gov

4. Revision History

This standard shall be subject to review according to the Regulatory Spreadsheet to ensure relevancy.

Date	Description of Change	Reviewer
08/01/2022	Annual Review	State Cybersecurity Office
12/19/2024	Annual Review. Update formatting.	Raymond Girdler, State IT Security Specialist