Department of Transformation and Shared Services
State Cybersecurity Office

Policy Title: Identification and Authentication Control 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 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. Related Controls

NIST: AC-2, AC-3, AC-6, AC-7, AC-8, AC-16, AC-17, AU-3, AU-4, AU-5, AU-6, AU-7, AU-11, AU-12, CM-3, CM-5, CM-6, CM-13, IA-3, MA-4, MP-4, PE-3, PM-21, PT-2, PT-7, RA-8, SA-8, SC7, SC-18, SI-3, SI-4, SI-7, SI-10, SI-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

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

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