KAY IVEY
Governor

STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY

JIM PURCELL
Acting Secretary

POLICY 630: Identification & Authentication

VERSION NUMBER	Policy 630-01
VERSION DATE	August 10, 2018
POLICY TITLE	Identification and Authentication
OBJECTIVE	The objective of this policy is to define the end-user and organizational responsibilities, and coordination among organizational entities, required to manage information system identification and authentication including multi-factor authentication (MFA).
AUTHORITY	The authority of the Office of Information Technology (OIT) to create and enforce policies relating to the management and operation of information technology (IT) by state agencies, and exceptions to such authority, are derived from: *Articles 8 and 11 of Chapter 4 of Title 41, and Chapter 28 of Title 41, Code of Alabama 1975 (Acts 2013-68 and 2017-282).* Policies of the OIT are approved and signed by the Governor.
APPLICABILITY	The requirements and responsibilities stated in OIT policies apply to all departments, agencies, offices, boards, commissions, bureaus, and authorities (referred to generally as *agency* or *agencies*) and authorized individuals in the employment of the State of Alabama responsible for the management, operation, or use of state IT.
STATEMENT OF POLICY	Identification and authentication controls ensure that only authorized users access information systems. Without identification and authentication controls, the potential exists that information systems could be accessed illicitly and that the security of those information systems could be compromised.

It is the policy of the OIT that:

a) All devices connecting to state IT shall be uniquely identified, validated, and authorized to connect before establishing a connection.

b) All organizational information system users (state employees or contract employees) or processes acting on behalf of organizational users shall be uniquely identified, validated, and proven.

c) All state information system users and devices shall be assigned a unique identifier (typically a username for users and MAC address, IP address, and/or system name for devices).

d) All state information system users shall use an authenticator for access to state information systems. Examples of an authenticators include passwords, cryptographic devices, one-time password devices, and key cards.

e) Authenticators shall be protected equal to the security category of the information to which use of authenticator permits access. For systems containing multiple security categories of information without reliable physical or logical separation between categories, authenticators used to grant access to the systems shall be protected at the same level as the highest security category of the information system.

f) Replay-resistant authentication mechanisms will be utilized for network access to privileged and non-privileged accounts. For example, replay-resistance techniques include protocols that use arbitrary numbers or challenges such as time synchronous or challenge-response one-time authenticators.

g) Feedback of authentication information will be obscured to protect the information from possible exploitation and use by unauthorized individuals. For example, displaying asterisks when users type passwords into input devices or displaying feedback for a very limited time before fully obscuring it.

h) Multi-factor authentication will be used for all access of privileged accounts. Privileged accounts are defined by NIST Special Publication 800-53 (revision 4) as “an information system account with authorizations of a user that is trusted to perform security-relevant functions that ordinary users are not authorized to perform.”

i) Multi-factor authentication will be used for all accounts accessing state resources from a public network. Public networks are any type of network wherein the public has access; and through it can connect to other networks or the Internet; for example, home Internet connections and public Wi-Fi.

j) In addition to the re-authentication requirements associated with device locks, individuals are required to re-authenticate in certain situations including, for example, when authenticators or roles change, when security categories of systems change, when the execution of privileged function occurs, or after a fixed or periodic (agency-defined) time.

k) All non-organizational information system users, or processes acting on behalf of non-organizational users, must be uniquely identified and authenticated. Non-organizational users include system users other than organizational users previously covered in this document.

OIT RESPONSIBILITIES

Promulgate standards, guidelines, and procedures governing access to state information systems.

Establish policies, procedures, and standards to work in conjunction with manual verification and authentication processes, software driven control polices, and network security tools to enforce this policy on state information systems.

Ensure that all OIT devices and those of agencies hosted by OIT connecting to state information systems are uniquely identified, validated, and authenticated.

Ensure that OIT hosted information systems uniquely identify and authenticate all users or processes acting on behalf of users.

Ensure every user of an OIT hosted information system is assigned a unique identifier and authenticator so all activities on a system or network are traceable to a specific user.

Enforce multi-factor authentication for access to privileged accounts on OIT hosted information systems.

Enforce multi-factor authentication for access to privileged and non-privileged accounts when accessed over an unsecured network.

Document system-specific identification and authentication requirements in system operating procedures.

Ensure OIT information system users are advised on protecting identifiers and corresponding authenticator mechanisms.

AGENCY RESPONSIBILITIES

Enforce this policy within the agency.

Ensure that all agency devices connecting to state information systems are uniquely identified, validated, and authenticated.

Ensure that the identity of all agency organizational users is identified, validated, and proven.

Ensure agency information systems uniquely identify and authenticate all users or processes acting on behalf of users.

Ensure every user is assigned a unique user identifier and authenticator so all activities on a system or network are traceable to a specific user.

Any agency that maintains and administers their own network shall enforce multi-factor authentication for access to privileged accounts.

Any agency that maintains and administers their own network shall enforce multi-factor authentication for access to privileged and non-privileged accounts when accessed over an unsecured network.

Document system-specific identification and authentication requirements in system operating procedures.

Ensure agency information system users are advised on protecting identifiers and corresponding authenticator mechanisms.

USER RESPONSIBILITIES

Users shall protect authenticators (passwords and tokens) from disclosure. Never share, cache, store in any readable form, or keep authenticators in locations where unauthorized persons might discover them.

Users shall employ different authenticators on each of the systems to which they have been granted access. For example, do not use the same password for both RACF and VPN access.

SUPPORTING DOCUMENTS	The following documents support this policy: • Standard 630S1: Authenticator Management • Guideline 630G1: Biometric Authentication
EFFECTIVE DATE	This policy shall be effective upon its approval by the Secretary of Information Technology and the Governor of Alabama as evidenced by the signatures of the Secretary and Governor being affixed hereto.
SUPERSEDES	This is the initial policy and does not supersede a previous version.

The undersigned, as Acting Secretary of Information Technology of the State of Alabama, exercising the power vested in that Office by the laws of this state, declares this policy to be adopted as of the date on which the Governor has approved and signed it.

Jim Purcell
Acting Secretary of Information Technology

ORDERED

Kay Ivey
Governor

This 13 day of September, 2018.

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
630-01	08/10/2018	Initial version