Identification and Authentication

IT SECURITY POLICY

8340

Purpose:

Define the security requirements for establishing and maintaining user accounts for state information systems.

Why it's important:

Establishes and maintains user accounts for state information systems. Identifies and monitors who's logging onto the system. Protects assets and content from unauthorized access, disclosure and modification.

Target audience:

All personnel

Overview:

- Organizational users: Ensure the state information system uniquely identifies and authenticates all organizational users.
- Network access to privileged accounts: ensure that multifactor authentication is implemented for network access to privileged accounts.
- Devices: Ensure the state information system uniquely identifies and authenticates all devices before establishing a local, remote or network connection.
- Manage the state information system authenticators, such as key cards, passwords, tokens and PKI certificates. Change and refresh authenticators as required. Protect authenticator content from unauthorized disclosure and modification.
- Authenticator feedback: ensure the state information system obscures feedback of authentication information during the authentication process to protect against exploitation or use by unauthorized individuals.
- Cryptographic authentication: ensure the state information system implements encryption methods that meet the requirements of applicable federal laws, state laws, executive orders and regulations.

Identify and authenticate all organizational users.

Identify and authenticate all devices.

Establish a password policy for authenticators.

Manage the state information system authenticators.

Establish reuse conditions for passwords, such as prohibiting password reuse for one year.

Employ encryption to protect user authentication.

For more information about this IT Security Policy, contact SecurityPolicies@azdoa.gov.

ADOA-ASET
Arizona Strategic Enterprise Technology

07.07.14