Access Controls

IT SECURITY POLICY
8320

Purpose:
Define the correct use and management of access controls for the protection of state information systems and assets.

Why it's important:
Protects the confidentiality and integrity of information when connecting to state information systems.

Target audience:
IT personnel and system administrators

Overview:

- Enforce approved authorizations for access to information and system resources.
- Develop daily access control operational procedures.
- Enforce approved authorizations for controlling the flow of information within the system and between interconnected systems.
- Employ least-privilege concept, allowing only authorized access for users that is necessary to accomplish assigned tasks.
- Employ a system-use notification to alert users that they are accessing a state information system, that usage is monitored, and that unauthorized use is prohibited and subject to penalties.
- Establish wireless and remote access restrictions and configuration requirements. Monitor and control remote access methods to detect cyber attacks.
- Employ full-device encryption to protect the confidentiality and integrity on mobile devices authorized to connect to state systems or handle confidential information.
- Facilitate information sharing by enabling users to determine awhether access assigned to the sharing partner matches restrictions and circumstances.

Install perimeter firewalls between any wireless network and the protected state information system.

Personal firewall software is required on mobile devices or computers with Internet connectivity used to access the network.

Enforce a limit of consecutive invalid logon attempts by a user and automatically lock the account for a specified period of time.

Employ a session lock to prevent access to the system by initiating a specified limit-of-time inactivity or until the user reestablishes access.

Portable storage devices shall be restricted or prohibited by authorized individuals on external information systems.

service providers acknowledge that they are responsible for the security of confidential data they possess.

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