System and Communication Protections

IT SECURITY POLICY

8350

Purpose:

Establish the baseline controls for the protection of state information systems and their communications.

Why it's important:

Provides the ability to monitor traffic to the network. Protects the authenticity of communication sessions, and protects the confidentiality and integrity of transmitted information.

Target audience:

IT personnel and system administrators

Overview:

- Implement network and network architectural controls: application partitioning, boundary protection, limited access points, deny by default, and network inactivity disconnect.
- Implement firewalls and router configurations to restrict connections between non-protected systems and any system components in the protected state information system.
- Implement controls for servers and components, including: preventing unauthorized data transfers using shared system resources; preventing split-tunneling for remote devices; one primary function per server.
- Ensure the state information system server is configured with security parameters and enables only secure services and protocols.
- Obtain public key certificates from an approved service provider.
- Establish VoIP (voice over Internet protocol) usage restrictions based on the potential to cause malicious damage to the information system.
- Protect communication session authenticity and safeguard against session hijacking.

Employ boundary protection to control communications at the external boundary of the system and at key internal boundaries in the system.

Restrict inbound and outband traffic as needed to protect the state information system.

Implement encryption methods for the protection of confidential information during transmission over open public networks.

Define acceptable and unacceptable mobile code and mobile code technologies.

Remote activation of cameras and microphones are prohibited with the exception of remote conferences and training.

Protect the integrity of audit log data at rest, as well as the confidentiality and integrity of taxpayer information at rest.

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

ADOA-ASET
Arizona Strategic Enterprise Technology

07.07.14