ARIZONA DEPARTMENT OF HOMELAND SECURITY

Statewide Policy: 8350

System and Communications Protections

What?

This policy outlines the security controls required to protect State agency computer systems and the communication networks they use. It covers a wide range of technical measures to safeguard data, prevent unauthorized access, and ensure the reliable operation of agency systems.

When?

This policy is always in effect and applies to all State agency systems and their communication networks.

Why?

To protect agency systems and data from a variety of threats, including unauthorized access, data breaches, denial-of-service attacks, and other malicious activities. This helps ensure the confidentiality, integrity, and availability of sensitive information and critical services.

Who?

Everyone involved in managing or using agency systems.

How?

Network Security:

- Implementing firewalls and other boundary protection devices to control network traffic.
- Creating secure network zones (DMZs) to isolate publicly accessible systems from internal networks.
- Preventing unauthorized network connections and access points.
- Implementing intrusion detection and prevention systems to monitor for suspicious activity.

Server Security:

- Securing servers and other system components with appropriate access controls and security configurations.
- Limiting server functionality to only essential services.
- Preventing unauthorized software and programs from running on servers.

Communication Security:

- Securing various communication channels, like email, web services, and remote access connections.
- Protecting the confidentiality and integrity of data transmitted over networks.
- Implementing secure authentication and authorization mechanisms for remote access.
- Protecting mobile devices that connect to agency systems.

Other Security Measures:

- Implementing denial-of-service protection to prevent disruptions to services.
- Using cryptographic services to protect data and secure communications.
- Managing cryptographic keys securely.
- Securing external telecommunications services.
- Protecting against malicious mobile code.

Remember:

- Agencies must regularly review and update their security controls to address new threats and vulnerabilities.

Where?

You can find more specifics on this policy HERE

If you have ANY questions about this or any other IT policy, **please contact** grc@azdohs.gov.

Effective: January 16, 2024