ARIZONA DEPARTMENT OF HOMELAND SECURITY

Statewide Policy 8340:

Identification and Authentication

What?

This policy outlines the requirements for verifying the identities of users and controlling their access to state agency computer systems and data. It covers a wide range of topics related to user accounts, authentication methods, and password management.

When?

This policy is always in effect and applies to all state agency systems and all users who access those systems.

Why?

To ensure that only authorized individuals can access sensitive information and systems, protecting against unauthorized access, data breaches, and misuse of resources.

Who?

Everyone involved in managing or using agency systems.

How?

- **Unique Identification:** Ensuring that each user has a unique identifier (username).
- **Strong Authentication:** Requiring strong authentication methods, such as passwords, multi-factor authentication, and/or biometrics.
- **Password Management:** Enforcing strong password policies, including password complexity, length, and regular changes.
- **Authenticator Management:** Securely managing authentication methods, including passwords, tokens, and certificates.
- **Device Identification:** Identifying and authenticating devices that connect to agency systems.
- **Identity Proofing:** Verifying the identities of users before granting them access.
- **Re-authentication:** Requiring users to re-authenticate under certain circumstances (e.g., after a period of inactivity).

Remember:

- The policy emphasizes the importance of strong authentication and secure password management.
- Agencies must implement appropriate identification and authentication controls for all types of users and devices.
- Regularly reviewing and updating authentication methods is crucial to stay ahead of evolving threats.

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