ARIZONA DEPARTMENT OF HOMELAND SECURITY

Statewide Policy: 8310 Account Management

What?

This policy outlines how user accounts on state agency computer systems must be managed. This includes things like creating, modifying, and deleting accounts, as well as controlling access and permissions.

When?

This policy is always in effect and applies to all user accounts on state agency systems.

Why?

To ensure that only authorized users have access to agency systems and data, and that their access is appropriate for their role. This helps prevent unauthorized access, data breaches, and misuse of resources.

Who?

Everyone involved in managing or using agency systems, including:

- **Oversight:** AZDOHS and the State CISO
- **Agency-Level:** Directors, CIOs, ISOs, and Account Managers
- **Individuals:** All employees and contractors with system accounts

How?

- **Automated Tools:** Using automated systems for account management.
- **Account Types:** Defining and documenting different types of accounts (e.g., individual, guest, admin).
- **Access Control:** Granting access based on roles and responsibilities.
- **Privileged Accounts:** Special protections for powerful accounts (like administrator accounts).
- **Separation of Duties:** Preventing any one person from having too much control.
- **Account Monitoring:** Tracking account activity and disabling inactive accounts.
- **Termination Procedures:** Promptly disabling accounts when someone leaves the agency.

Remember:

- The policy emphasizes strong security controls for account management.
- It aims to balance ease of use with security by using automated tools and clear procedures.
- Regular reviews and updates are necessary to ensure that accounts are managed effectively.

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