ARIZONA DEPARTMENT OF HOMELAND SECURITY

Statewide Policy: 8210 Security Awareness Training and Education

What?

This policy ensures that all state employees and contractors are appropriately trained and educated on how to protect sensitive information and use state systems securely. This includes ongoing awareness and education to keep everyone's knowledge current.

When?

This policy applies to all end users. Training is required:

- **Prior to system access:** Initial training is required before anyone can use state systems.
- **Annually:** AUP must be signed by all users, and refresher training and awareness activities must occur at least once a year.
- **When changes or revisions occur:** Training is required whenever there are updates to systems, policies, or security threats.

Why?

- **Protect State Data:** Informed employees are the first line of defense against security breaches.
- **Reduce Human Error:** Training helps prevent mistakes that can compromise security.
- **Promote a Security Culture:** Awareness programs create a work environment where everyone prioritizes security.
- **Meet Legal Requirements:** Arizona law mandates security awareness training for state employees.

Who?

This policy applies to:

- **All Employees:** Full-time, part-time, and temporary staff.
- **Contractors:** Anyone who has access to state systems or data.
- **Agency Leadership:** Directors, CIOs, and ISOs are responsible for implementing the policy.
- **Supervisors:** They play a key role in ensuring their team members complete training.

How?

This policy requires agencies to:

- **Develop a Training Program:** Create a comprehensive security awareness program with clear objectives.**
- **Provide Initial and Ongoing Training:** Cover key security topics like insider threat, social engineering, and acceptable use of systems and provide regular updates to those trainings.**
- **Track and Document Training:** Maintain records of who has completed training and when.**
- **Offer Specialized Training:** Provide role-based training for those with elevated security responsibilities. An example is individuals that handle federal tax information or social security information.
- **Timely and Relevant Training:** Leverage State tools, such as *Infosec IQ*, to provide training that reflects real world threats and scenarios.
- **Get Feedback:** Continuously improve training based on feedback from employees.
- **Acceptable Use Policy:** Ensure users understand, consent to, and uphold AUP agreements annually.

Key Reminders:

- **Stay Informed:** Keep up with the latest security threats and best practices.
- **Report Concerns:** Encourage employees to report any suspicious activity or security concerns.
- **Engage Learners:** Use creative and interactive methods to keep employees interested and involved.

***Note: Self-Directed Agencies are obligated to fulfill these requirements. Managed Agencies can leverage ADOA's expertise and resources.*

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