Personnel Security Protections

IT SECURITY POLICY
8270

Purpose:

Increase the ability to protect state information systems and assets containing sensitive data through personnel security protections.

Why it's important:

Pre-employment screening helps to fill sensitive roles involving access to classified or protected data and assets. Security measures for job change or employment separation mitigate potential security breaches.

Target audience:

All personnel

Overview:

- Positions shall be assigned a sensitivity designation based on the individual's exposure to system information or administrative privileges, such as firewall administrators, members of the incident response team, and personnel with vulnerability scanning duties.
- Information security responsibilities shall be defined for those who: establish, document and distribute security policies and procedures; monitor, analyze and distribute security alerts; establish, document and distribute security incident response procedures; administer user accounts; and control access to data.
- Upon termination of employment, access to the state information system will be terminated within 24 hours; all security-related property shall be retrieved; and information system accounts formerly controlled by the individual will be retained.
- Individuals requiring access to state information systems shall acknowledge and accept the access agreement prior to being granted access (Policy 8280: Acceptable Use).
- Third-party contractors shall comply with applicable security requirements.
- A sanctions process shall be employed for personnel failing to comply with security and privacy policies.

Establish screening criteria for individuals filling sensitive and non-sensitive positions.

Define responsibilties for individuals who monitor and analyze security alerts and security incident responses.

Upon any personnel transfer or reassignment, physical access authorization will be reviewed and reissued as needed.

Personnel security requirements, roles and responsibilities shall be established for third-party providers.

Third-party contractors shall report any security incidents, including breaches of unsecured sensitive information.

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