System Security Acquisition and Development

IT SECURITY POLICY
8130

Purpose:
Establish adequate security controls for the acquisition and deployment of state information systems.

Why it's important:
Implementing the right technology best meets the agency's requirements and also follows federal and state regulations for encryption. Mitigates potential risks and vulnerabilities.

Target audience:
IT managers, finance managers, procurement team

Overview:

- Determine security requirements for the state information system.
- Manage the technology life cycle by defining security roles and responsibilities, and integrating the risk management process.
- Follow change control procedures to ensure separate duties for development and test/production areas, and removal of test data before system is active.
- Develop applications based on secure coding guidelines to prevent coding violations.
- The acquisition process must include descriptions and requirements for security function and controls, security strength, security assurance and acceptance criteria.
- Administrator documentation for the state information system must describe user-accessible security functions, methods for user interaction, user responsibility in maintaining system security, and protection documentation in accordance with risk management.
- Perform configuration management during development, implementation and operation and document accordingly.
- Independent agents to verify the correct implementation of the security assessment plan and conduct penetration testing.

Implement software development processes: remove user IDs and passwords; review custom code prior to release.

Documentation must describe the secure configuration, installation, operation of the system and the components.

Information engineering principles must be applied in the specification, design, development, implementation and modification of the system.

Providers of external state information system services must identify the functions, ports, protocols and other services required.

Create and implement a security assessment plan that tests and evaluates security-related functional properties.

Address new threats and vulnerabilities for public Web applications on an ongoing basis. Install Web-application firewalls. Perform threat and vulnerability analyses.

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