Overview:

- Develop, document and implement a configuration management plan that addresses the roles, responsibilities and processes; establish a process for identifying configuration items throughout the software development lifecycle; and protect the configuration management plan from unauthorized disclosure and modification.

- Key components of the configuration management plan include baseline configuration; a change-control board that coordinates and provides oversight for configuration control activities; testing, validating and documenting any changes; a state information system component inventory; and ensuring software usage restrictions.

- Controlled maintenance of state information systems will be performed.

- To ensure system and information integrity, flaw remediation shall be implemented; mechanisms to protect against malicious code shall be employed; and the state information system shall be monitored to detect potential security attacks.

- Integrity verification tools shall be adopted to detect unauthorized changes, and spam protection mechanisms shall be implemented.

- Security alerts shall be disseminated as deemed necessary.

Purpose:
Establish the baseline controls for the management and maintenance of the state information system.

Why it’s important:
Ensures the integrity of systems and data. Protects against vulnerabilities. Ensures control of IT equipment, software and procedures.

Target audience:
IT managers

IT SECURITY POLICY

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