Acceptable Use

IT SECURITY POLICY 8280

Purpose:

Define the acceptable use of state information and system assets to reduce the risks of disclosure, modification or disruption, whether intentional or accidental.

Why it's important:

Protects assets and intellectual property, as well as confidential information in accordance with applicable statutes, policies and procedures. The policy also outlines prohibited behaviors, including computer tampering, unauthorized use of equipment, software or services.

Target audience:

All personnel

Overview:

- Personnel are required to practice safe computing, use caution when opening attachments or links, keep passwords secure, notice unauthorized personnel, report security violations or privacy weaknesses, and wear issued badges.
- Confidential information shall be protected in accordance with applicable statutes, rules, policies and procedures.
- The following behaviors are prohibited: computer tampering, use of unauthorized equipment or software, the introduction of malware, recklessly disrupting the state information system, circumventing security controls, falsifying identification information, and accessing inappropriate material.
- Unauthorized use of electronic messaging is prohibited, including: spam, unprofessional communications, masking your identity, and sending unencrypted confidential information.
- Notifications and acknowledgements shall be used to ensure security, including monitoring and blocking of inappropriate content.
- Personnel who provide and store confidential information and work outside of designated work areas shall employ security controls such as anti-virus protection, firewalls, encryption and security patches.

Personnel shall exercise good security practices and adhere to safe computing to ensure the protection of state systems and data.

Users acknowledge that they consent to the agency's right to conduct monitoring and that there is no expectation of privacy.

Use of email to send spam, chain letters, pyramid schemes or unbusinesslike content is prohibited.

Individuals working in virtual offices or from home shall accept access agreements prior to being granted access.

Appropriate controls such as firewalls and anti-virus protection shall be utilized when working outside of designated work environments.

Individuals utilizing smart phones and tablet computers to access state systems must accept access agreements prior to being granted access.

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