Media Protection

IT SECURITY POLICY
8250

Purpose:

Increase the agency's ability to ensure the secure storage, transport and destruction of sensitive information.

Why it's important:

Proper media storage, protection and encryption mitigates the risk of data breaches for confidential information. Only specific, authorized personnel should handle confidential digital or non-digital media.

Target audience:

IT managers and data owners

Overview:

- Access to digital and non-digital media shall be restricted to authorized individuals.
- Digital and non-digital media containing confidential information shall be marked to indicate distribution limitations, handling caveats and applicable security markings.
- Digital and non-digital media containing confidential information shall be securely stored within controlled areas.
- Digital and non-digital media containing confidential information shall be protected during transport outside of controlled areas. Exact copies of confidential data shall be created prior to transport. A record of movement shall be maintained for any transport of hardware and digital media.
- Encryption mechanisms shall be employed to protect the confidentiality and integrity of information stored on digital media during the transport outside of controlled areas.
- Digital media backups shall be stored in a secure location, with the location's security reviewed annually.
- Prohibition of Use without Known Owner: the use of removable media is prohibited when the media has no identifiable owner.

Inventory logs of all digital media containing confidential information shall be conducted annually.

Encryption shall be utilized to protect the confidentiality and integrity of information.

Confidential digital and non-digital media shall be sent by a secured courier or other secure delivery method.

Digital and non-digital media containing confidential information shall be sanitized prior to disposal, release of control, or release for reuse.

The use of removable media is prohibited when the media has no identifiable owner, such as finding a flash drive in a parking lot.

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