Contingency Planning

IT SECURITY POLICY 8230

Purpose:

Minimize the risk of system and service unavailability due to a variety of disruptions by providing effective and efficient solutions to enhance system availability.

Why it’s important:

Minimizes downtime and unavailability of services. Helps to maintain essential functions despite an information system disruption, compromise or failure. Provides a clear plan for disaster recovery and system restoration.

Target audience:

IT personnel

Overview:

- Develop a contingency plan that outlines recovery objectives, restoration priorities and metrics, addresses roles and responsibilities, and identifies essential missions and business functions.

- Manage the contingency plan by distributing it to key contingency personnel and protect the contingency plan from unathorized disclosure and modification.

- As part of a comprehensive contingency plan, an alternate storage site and alternate processing site shall be established to house the storage and recovery of information system backup. The alternative storage site shall be easily accessible and will be separate from the primary site.

- Priority-of-services provisions shall be established for the alternate processing site to transfer and resume state information system operations. Priority-of-service provisions shall also be established for all telecommunications services used for national or state security emergency preparedness.

- Backup information shall be tested for reliability and integrity at least annually to provide for the recovery and reconsitution of the state information system in the event of a disruption, compromise or failure.

The contingency plan will outline a restoration timeframe based on priorities, regulations and other organizations.

Distribute the contingency plan to key personnel and coordinate contingency planning activities with incident handling activities.

Contingency training shall be provided to state information system users consistent with assigned roles and responsibilities.

A priority-of-service provision shall be developed for the restoration of data, communications and systems.

User-level and system-level information backups shall be conducted for a timely recovery and reconstitution of data and services.

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