Incident Response Planning

IT SECURITY POLICY
8240

Purpose:
Increase the ability to rapidly detect incidents, minimize any loss, mitigate weaknesses that were exploited, and restore computing services.

Why it's important:
Personnel should know how to identify, report and escalate an incident for quick containment, and recovery. Helps to maintain the integrity of the information system and keep the system secure. Outlines the steps to remediate a data breach.

Target audience:
All personnel

Overview:

- Develop, implement and maintain an incident response plan for the detection and analysis, containment, eradication and recovery of security information. The incident response plan shall be tested annually.
- The incident response plan shall provide a roadmap for implementing the agency's incident response capability, define reportable incidents, and provide metrics for measuring the agency's incident response capability.
- The incident response plan shall also describe the roles, responsibilities and communication strategies in the event of a compromise.
- Provide incident response training to state information systems users consistent with assigned roles and responsibilities.
- Potential privacy incidents shall be investigated upon awareness of loss of personally identifiable information (PII). Affected parties will be notified upon breach determination without unreasonable delay.
- Report an incident:
  - Advise your manager or supervisor
  - Open a ticket: ServiceDesk@azdoa.gov
  - Call 602-364-4444, Option 3

Conducted annual tests using checklists, walk-throughs, simulations and exercises to determine incident response effectivenesss.

Information security management personnel shall be available on a 24x7 basis to respond to alerts.

State information system security incidents shall be monitored, tracked, analyzed, documented and distributed to appropriate personnel.

Automated alerts and reporting shall be incorporated in the system for intrusion detection, intrusion prevention and maintaining file integrity of the monitoring systems.

Report security incidents within one hour of knowledge of the suspected incident.

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