System Security Audit

IT SECURITY POLICY
8330

Purpose:
Protect state information systems and data by providing the appropriate controls and configurations to support audit log generation, protection and review.

Why it's important:
Improves the management of the state information system, alerts inappropriate activity, and minimizes potential security vulnerabilities or breaches.

Target audience:
System administrators

Overview:

- Develop and employ security auditing capabilities. Review and update audited events annually or as required.
- Generate audit records detailing what type of event occurred, where and when the event occurred, name of the affected data or system component, the outcome of the event, and any individuals associated with the event.
- Review and analyze state information system audit records periodically for inappropriate or unusual activity and report findings to defined personnel.
- Back up audit trails to a centralized log. Ensure the state information system backs up audit records onto a different system other than the system or component being audited.
- Use file-integrity monitoring or change-detection software on audit logs to ensure that log data cannot be changed without generating alerts.
- Audit records shall be retained for a defined time period to allow for analysis, investigations of security incidents, and to meet regulatory information retention requirements.
- Ensure the state information system provides audit record generation capability for auditable events at servers, firewalls, workstations and other defined system components.

Alert defined personnel in the event of an audit processing failure.

Employ automated mechanisms to integrate audit review, analysis and reporting processes for investigation and response to suspicious activities.

Employ audit report generation capabilities that support on-demand audit review, analysis and reporting requirements.

Generate time stamps for all audit records and synchronize with an authoratative time source.

Protect audit information and audit tools from unauthorized access, modification and deletion.

Ensure that the state information system's anti-virus programs are generating audit logs.

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