Tier 1 Control Standards (State-Wide)

Auditing

Standard ID
IOT-CS-ARC-005

Published Date
6/30/2017

Effective Date
1/1/2018

Last Updated
6/30/2017

Next Review Date
6/30/2018

Policy
11.0 Protective Technology (PR.PT)
   11.1 PR.PT-1
      11.1.1 Audit/Log Records

Purpose
Detail standards for auditing events as related to information systems, devices and components supported by the Indiana Office of Technology.

Scope
All Devices that Connect to the State Network

Statement
The following requirements apply to auditing of confidential information systems and their related components pertaining to systems and infrastructure managed and maintained by the Indiana Office of Technology.

Auditing - General

- Systems shall be configured to log to dedicated, centrally managed servers, where technically feasible
- Event correlation tools shall be used to analyze events from systems and identify potential risk areas or system problems
- Centralized logging servers shall be protected in accordance with State and/or regulatory standards for confidential information
- Systems that cannot be configured to log centrally shall have appropriate access controls for access to log data
- Only dedicated Information Security administrators shall have the authority to archive and delete audit trail records
- Prior to archiving, audit records shall be backed up, retained and protected in accordance with the appropriate State and/or regulatory guidelines (HIPAA, PUB 1075, etc.)
- Auditing functions shall provide a warning when allocated audit volume reaches a pre-defined percentage of maximum capacity
- Confidential systems shall, at a minimum, adhere to the guidelines as described in IOT’s Audit and Accountability control standard

Change Management Auditing

- Records reflecting all physical and logical system and infrastructure changes shall be generated, reviewed and retained
• Audits of information system changes shall be conducted periodically, as well as on an ad hoc basis when warranted, to determine whether unauthorized changes have occurred

Roles
All Personnel
Information Asset Owners/System Owners

Responsibilities
Information Asset Owners/System Owners shall ensure their systems' environments are audited for required events and that those events are logged accordingly.

Management Commitment
Management shall ensure that their staff are aware of ongoing event & activity auditing as detailed in this Standard.

Coordination Among Organizational Entities
Agencies must define and communicate to IOT their required logging events. Further, personnel needing to be notified must be identified by the respective agency.

Compliance
State agencies that are subject to the requirements of this Standard but are not compliant must submit an action plan.

Exceptions
Exceptions will be handled on a case by case basis through the Director of Risk & Compliance, State CISO and the IOT Architect team.