Tier 1 Control Standards (State-Wide)

Logging & Monitoring

Standard ID
IOT-CS-ARC-006

Published Date
6/30/2017

Effective Date
1/1/2018

Last Updated
6/30/2017

Next Review Date
6/30/2018

Policy
13.0 Security Continuous Monitoring (DE.CM)
  13.1 DE.CM-1
    13.1.1 Network Monitoring
  13.2 DE.CM-2
    13.2.1 Physical Environment Monitoring

Purpose
Establish requirements for security logging and monitoring of logs for information systems and components supported by the Indiana Office of Technology.

Scope
All Devices that Connect to the State Network

Statement
The following requirements apply to the collection, retention and monitoring of logs as related to confidential systems and infrastructure managed and maintained by the Indiana Office of Technology.

Logging

- Log files that contain confidential data or that are transmitting over the network shall be encrypted
- Adequate storage capacity shall be maintained to avoid gaps in data gathering
- Log files shall be backed up and disposed of securely
- Log data shall be logged to a separate, isolated location
- Log parameters shall be set to disallow modification of previously written data
- System events that are used to detect a hack attempt shall be logged and stored in order to maintain evidence for incident follow up
- Logs shall be retained in accordance with the appropriate compliance policy (e.g. HIPAA, FISMA, SOX, etc.) as related to the confidentiality of the system and/or function to which they are associated
- All unsuccessful authentications attempts shall be logged

Log and Activity Monitoring

- Monitoring for unauthorized personnel, connections, devices and software shall be performed
- Logs for all systems subject to this Standard shall be reviewed
- Log reviews shall include devices that perform system security functions (e.g. intrusion detection (IDS), authentication,
etc.)

- Information Security shall perform reviews to ensure the State of Indiana's monitoring systems are capable of detecting unauthorized attempts to access State information resources
- Information system audit records shall be reviewed for indications of inappropriate or unusual activity

Roles
All Personnel
Information Asset Owners/System Owners

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

Management Commitment
Management shall ensure that their staff are aware of activity logging and monitoring as described in the Standard.

Coordination Among Organizational Entities
Agency shall work with IOT to determine the events that need to be logged and reported on.

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.