

State of Indiana Policy and Standards

System Isolation

Standard ID

IOT-CS-SEC-002

Published Date

9/1/2016

Effective Date

1/2/2017

Last Updated

8/22/2016

Next Review Date

8/22/2017

Policy

06.0 Access Control (PR.AC)

06.5 PR.AC-5

06.5.1 Network Segmentation

Purpose

Lack of system isolation or segmentation increases the State's breach exposure. Segmenting critical applications and/or systems containing confidential data will reduce the likelihood and impact of a successful attack.

Scope

All Executive Branch State Agencies

Statement

Systems collecting, processing, transferring or storing confidential data, must be physically and/or logically isolated.

Roles

Agency Management

Information Asset Owners/System Owners

IOT Personnel

Users with Elevated Privileges

Responsibilities

Asset Owners/System Owners shall identify confidential systems and isolate them in accordance with State Standards.

Management Commitment

Management shall ensure that all confidential systems are segmented appropriately.

Coordination Among Organizational Entities

Agencies shall coordinate with the IOT Architecture team for proper isolation practices and Standards.

Compliance

Agencies shall review the Information Systems Inventory (ISI), the authoritative source of system information to understand all confidential systems related to their agency. All confidential systems must be isolated per State Standards. Lack of compliance will result in escalations to Agency Heads and the CISO.

Exceptions

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