Tier 1 Control Standards (State-Wide)

**Terminated ID Notification - IBM Mainframe**

**Standard ID**
IOT-CS-SEC-107

**Published Date**
10/1/2013

**Effective Date**
11/1/2013

**Last Updated**
5/19/2017

**Next Review Date**
5/19/2018

**Policy**
06.0 Access Control (PR.AC)  
06.1 PR.AC-1  
06.1.1 Account Management

**Purpose**
Removing access from terminated or changed employment is critical to the protection of data.

**Scope**
IOT Supported Entities

**Statement**
When an employee terminates his or her employment with the State of Indiana (SOI), the agency mainframe security coordinator must submit employee terminations using the automated IBM Mainframe "Account Request" form.

IOT has automated mechanisms in place to ensure IDs do not stay active indefinitely: 1) A scheduled job "ACFREVU" runs and distributes a report to the designated agency mainframe security coordinator every 90 days showing inactive userids that have no been used in over 90+ days. The agency has two weeks to notify their users to logon to the mainframe if they are still active, otherwise, they are terminated 2) Userids that are inactive for over 60+ days are automatically revoked by the system.

The following procedures shall be followed:

- Terminate ID
- Remove user account(s) (termination or deletion of an individual's access privileges to the information, services, and resources for which they currently have clearance, authorization, and need-to-know when such clearance, authorization and need-to-know no longer exists).

**Agency HRD or Designee Notification Process**

Upon termination, the agency's Human Resource Director (HRD) or designee shall submit the IBM Mainframe "Account Request" form for terminated employees.

**IOT’s Functional Process**

Help Desk - IOT’s Help Desk via Help Desk ticket will notify Account Management and Security (if needed)
Security - IOT Security will terminate inactive userids after 90+ days of inactivity

Account Management - Remove userids that are submitted by the mainframe security coordinators using the IBM Mainframe “Account Request” form.

Roles
Agency Personnel
IOT Personnel

Responsibilities
Agency personnel shall provide timely notification of all agency terminations or transfers. IOT staff shall terminate access within SLA required timeframes.

Management Commitment
Management shall confirm appropriate procedures related to terminations or transfers. Management shall periodically audit the process and timeframe of access removal.

Coordination Among Organizational Entities
Agency shall work with IOT to remove access within the agreed upon timeframes.

Compliance
IOT Security generates and reviews quarterly reports on all the agencies.

Exceptions
No exceptions.