Terminated ID Notification

Standard ID
IOT-CS-SEC-106

Published Date
1/1/2007

Effective Date
1/1/2007

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 Human Resource Director (HRD) or designee must submit employee terminations using the automated CAA "Computer Account Administration" form.

IOT has two automated mechanisms in place to ensure IDs do not stay active indefinitely: 1) A PeopleSoft job runs nightly disabling terminated user accounts that were not submitted using the CAA form; 2) Contractors are required to re-certify their accounts on a monthly basis or their accounts will be de-activated.

The following procedures shall be followed:

- Remove ID from access lists (physical eradication of an entity's access privileges).
- Removal of 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).
- Turning in of keys, tokens, or cards that allow access (formal, documented procedure to ensure all physical items that allow a terminated employee to access a property, building, or equipment are retrieved from that employee, preferably before termination).
Agency HRD or Designee Notification Process

Agency Human Resource Director (HRD) or designee shall submit the CAA form for employees on the date the termination process is completed. The CAA form produces a ticket needed to terminate the account.

IOT’s Functional Process

Help Desk - IOT’s Help Desk acts upon the generated ticket

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’s Security Section will verify compliance generating a query on random agencies. Periodic reports are provided to the agency showing the timeliness of account termination versus reliance on the safety net utilizing employee’s termination in PeopleSoft.

Exceptions

No exceptions.