Tier 1 Control Standards (State-Wide)

Active Directory User Account Registration and Deregistration

Standard ID
IOT-CS-SEC-119

Published Date
11/11/2008

Effective Date
11/11/2008

Last Updated
3/30/2017

Next Review Date
3/30/2018

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

Purpose
Establishes a formal process for registering new employees and contractors as well as the timely removal of their access due to changes in employment status

Scope
IOT Supported Entities

Statement

The following are requirements related to account creation with Active Directory:

- Contractor accounts will be set to expire every 30 days. Contractors and their managers will receive email notifications beginning 7 days prior to expiration and daily afterward until action is taken to confirm account is still in use. Lacking an affirmative response indicating continued job duties, the account will expire on the 31st day
- Activating an account that expired in error requires the authorization of the agency security coordinator
- Contractor accounts remain expired for 2 weeks. If the account is not extended at that point a ticket will be generated to disable the account

Registration Procedure (applies to any users needing an Active Directory account):

- PeopleSoft login IDs are obtained by setting up the new employee/contractor in the HR module. Users may be setup in advance of their start date. SPD recommends no more than one week in advance (See the PeopleSoft Work Instructions titled, “Future Dating Work Record Entries into PeopleSoft”, located on the SPD Training Web site.)
- Account registration is initiated by Security Coordinator via completion of the on-line New Computer Account Request form found at http://caa.iot.in.gov/Request/
- A completed form auto-generates a help desk ticket forwarded to IOT Account Management (Employees and non-employees may require slightly different information. Radio buttons are provided for each on the registration form)
- Setting up users
  - Incorporate End User Password Minimums consistent with State standards
  - Configure directory structure, Shares, and NTFS
  - Confirm that each account has an owner
  - The transaction serves as the record of registration
Account creation results in a setup confirmation sent to Security coordinator and Manager, the help desk ticket is closed.

Deregistration procedure:

- Security Coordinators shall request to disable/delete a user account effect as of the last day of employment. Requests can be scheduled in advance to run at a specific date and time. Information on who shall receive copies of email and home directory files can be entered in the comment section of the form. Completion of the form automatically sends a ticket to Account Management for processing (http://caa.iot.in.gov/Request/).
- Account deregistration in Active Directory is automatic with a change in status of employees or contractors to “terminated” or “retired” status in PeopleSoft. This is a safety measure and shall not be relied upon as the primary process for disabling accounts.
- For time sensitive or other special deactivations, agency Security Coordinators shall submit a completed on-line Computer Account Deregistration Request form with the comment section blank. Once the form is submitted the account will be disabled within a few minutes.
- All accounts that have been deregistered and disabled by the CAA process will be automatically deleted from the Active Directory database after 30 days.

Transfers of employment:

- Agency Security Coordinators will use help desk tickets to handle employees moving to a new manager (intra-agency). This ensures Active Directory accounts are updated appropriately. This does not address PeopleSoft (PeopleSoft records may not require updating depending on the change). Employees moving to a new agency will need to have a new account request submitted.
- IOT Account Management, through the help desk ticket process, will require permission from the preceding manager to transfer home directory files and email messages.
- No changes are required for employees promoted but staying in the same chain of command.
- Agencies shall review group memberships for those users remaining in the same agency but moving to a new position to ensure access matches their current role.

Roles
All Personnel

Responsibilities
Agencies shall ensure the timely registration and deregistration of users. IOT Account Management shall implement and maintain registration/deregistration guidelines.

Management Commitment
Management is responsible for ensuring their agency is meeting the requirements written within this standard.

Coordination Among Organizational Entities
Agencies shall coordinate with IOT to confirm account management practices are completed within required timeframes.

Compliance
Management shall periodically recertify accounts for their agency and follow appropriate steps for accounts that fall out of compliance.

Exceptions
No exceptions.

Associated Links
http://caa.iot.in.gov/Request/