Tier 1 Control Standards (State-Wide)

RACF Administrative Privileges Access

Standard ID
IOT-CS-SEC-126

Published Date
9/27/2006

Effective Date
9/27/2006

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
This Standards explains the requirements and regulations for administrative privileges on the State mainframe. The State pushes on all platforms and with all technologies toward a goal of giving the workforce the minimum rights required to perform job functions. With this goal in mind, administrative privileges are not given without appropriate justification. Covered in this Standard are the RACF Special, Auditors, and Operations user attributes. Further, this Standard covers the process for acquiring and revoking rights as well as compliance activities.

Scope
IOT Supported Entities

Statement
The following are the requirements related to RACF Administrative Privileged Access:

- RACF administrative attributes are provided only when a submitted request justifies the need for the attribute against established IOT criteria based on security best practices.
- Staff members authorized to receive the RACF administrative attributes are required to pick up and sign for said RACF Auditors attribute each time the need arises.
- Auditing of the RACF administrative attributes will be reviewed on a periodic basis and are subject to termination if business circumstances have changed.
- Agency managers are obligated to notify IOT if role changes impact the need for the administrative attribute.

Definitions/References

- **Special attribute** – allows the issuance of all RACF commands and gives the user full control over all of RACF profiles in the RACF database.
- **Auditors attribute** - allows the staff member to specify logging options on the RACF commands and list any profile (including its auditing options) using the RACF commands.
- **Operations attribute** - grants the user equivalent of ALTER access to all data sets unless the user or one of the user’s connect groups appears explicitly in the access list of a data set’s profile. (Note: If a user needs to perform maintenance activities on DASD volumes, granting DASDVOL authority to those volumes using the PERMIT command is preferred over assigning the OPERATIONS or group-OPERATIONS attribute.)
Roles
Users with Elevated Privileges

Responsibilities
End users shall properly request and justify need for administrative access. IOT Staff shall review, ensure proper approval and grant access to RACF if proper justification and approval is received.

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

Coordination Among Organizational Entities
Users shall coordinate with IOT Security when RACF access is needed.

Compliance
A review of the RACF administrative attributes will be made on a quarterly basis by IOT Security.

Exceptions
No exceptions.