Tier 1 Control Standards (State-Wide)

RACF RVARY

Standard ID
IOT-CS-SEC-127

Published Date
12/1/2006

Effective Date
12/1/2006

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 Standard provides a set of requirements for the regulation and use of the powerful RVARY command in the mainframe production LPAR. This policy institutes mechanisms for the addition and removal of people authorized to use the RVARY command.

Scope
IOT

Statement
RVARY is used for the following actions:

- Deactivate and reactivate the RACF function.
- Switch from using a specific primary data set to using its corresponding backup data set (possibly because of a failure related to the primary data set).
- Deactivate or reactivate primary or backup RACF data sets. (Deactivating a specific primary data set causes all RACF requests for access to that data set to fail. Deactivating a specific backup data set causes RACF to stop duplicating information on that data set.)
- Deactivate protection for any resources belonging to classes defined in the class descriptor table while RACF is inactive.
- Select the mode of operation when RACF is enabled for sysplex communication.

RVARY command rights are provided only with the approval of the Technical Services Manager and a Security analyst.

- Special access on Indiana Office of Technology (IOT) systems is administered via the IBM Security Server (RACF) and by a Technical Services Security Technician and Security Analysts.
- The RVARY passwords are changed every thirty (30) days.
- Individuals authorized to execute the RVARY command must receive the password from the Technical Services Security Technician.
- Use of the RVARY command is limited to individuals needing said access to perform their job.
- Misuse of the RVARY command must be reported immediately to an IOT Security analyst or the State CISO.
- Contents of the RVARY command is reviewed on a periodic basis.
- Persons who misuse their RVARY command privilege can have said access revoked.
Roles
Users with Elevated Privileges

Responsibilities
End users requiring use of the RVARY command shall justify the need for authorization and follow the appropriate approval process. IOT shall review and approve access to the RVARY command based on least privilege.

Management Commitment
Management shall validate individuals requiring access and periodically review to confirm least privilege.

Coordination Among Organizational Entities
Agencies shall coordinate with IOT where necessary to appropriately secure data in accordance with this standard.

Compliance
The RVARY command will be removed from the password list if the person no longer works at IOT, an individual's duties no longer require use of the RVARY command, the person has violated the use of the RVARY command, other reasons identified by IOT Security. The RVARY password changes when any of these instances occur.

Exceptions
No exceptions.