STATE OF ALABAMA

Information Technology Standard

STANDARD 663S2-02: RACF ARCHITECTURAL STRATEGIES

A concise methodology for the implementation and maintenance of the State's mainframe security software, Resource Access Control Facility (RACF), is essential. Consistent implementation methodology is necessary to achieve efficient and effective protection and operations of state resources while minimizing administrative effort and associated costs. The architecture of the security environment provided by RACF is more understandable and comprehensive when uniform methodologies and strategies are used.

OBJECTIVE:

Define standardized RACF architectural strategies to protect the integrity and ensure interoperability of State of Alabama mainframe resources.

SCOPE:

These requirements apply to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

REQUIREMENTS:

RACF is the authorized primary software used to provide the capability to protect an entity’s resources on the state data center mainframes. RACF implementations within and between entities utilizing the state mainframes shall utilize the RACF architectural strategies outlined herein.

GLOBAL

The RACF record data fields available for user ID, group, dataset and general resource profiles should be utilized to preserve information necessary in the review, maintenance and administration of the State's security structure. The following fields are to be completed:

- Name (User's Full Name or Function Name)
- Installation Data (uniqueness or data needed to be known or description of Function [254 available character spaces])

Generic profiles shall be used for dataset profiles. When generic profiles are not utilized, installation data shall include justification/reason for discrete profile.

The Universal Access (UACC) on profiles should be NONE. Installation data shall include justification /reason for any UACC variance.

RACF Administration capability is provided to a user ID only by the use of SYSTEM SPECIAL, GROUP SPECIAL, CONNECT AUTHORITY or specific general resource profiles.

The OWNER of RACF user ID, group, dataset and general resource profiles shall be a group, never a user ID.

RACF shall contain only active valid profiles.

USER IDENTIFICATION (USER ID)

User IDs are classified as either personal (individual) or functional. A personal user ID is assigned to an individual. A functional user ID is assigned to a started task, function, process, or activity.

User IDs are established to identify individuals or functions (as follows):

> All user IDs (personal and functional) are to be unique.
>
> A user ID established for use by an individual user is for the sole use of the assigned individual. This user ID is used to access information resources (i.e. applications, datasets, data etc.). User IDs are not to be shared, distributed or disseminated in any manner with other functions or individuals.
>
> An individual should have only one user ID. Capabilities (i.e. TSO, ROSCOE, VTAM Switch, etc.) will be assigned to the user ID. If job responsibilities require more than one user ID, justification shall be included in installation data field of both user ID profiles.
>
> The name field for user IDs established for a function (started tasks, batch jobs, applications etc.) will be descriptive. The Installation Data field is to contain further descriptive narrative.
>
> Functional user IDs are assigned the PROTECTED and/or RESTRICTED attribute. Contact State RACF Administration for information and coordination.
>
> User IDs with PROTECTED attribute are never assigned capabilities that require or are used to sign on to the mainframe (i.e. TSO, ROSCOE).
>
> User IDs established for individuals or functions outside the ISD infrastructure (i.e. a bank or non-State agency) shall be assigned the RESTRICTED attribute.
>
> User IDs are not used to establish or identify entities, resources or other activities that does not have the purpose of verification of access to protected resources.
>
> A user ID assigned to a specific individual shall not be used as a functional user ID for any production activity that will continue after a person has left the entity and the user ID shall be deactivated/removed.

Recommended User ID Naming Standard:

The first two characters of a user ID shall be the entity's (agency State Data Center (SDC) primary billing unit) identifier. Additional characters should be assigned as shown in the following table.

Table 1: Recommended User ID Naming Standard

Position	Type	
1st/2nd	Char	SDC Code (required)
3rd	Char	Last digit of year user ID assigned (ex: 2 for 2012)
4th/5th	Char	Month user ID assigned (01 through 12)
6th/7th	Char	Day user ID assigned (01 through 31)
8th	Char	Available to handle multiple assignments if user ID is not to be given TSO capability

If the above naming standard is not used, it is recommended that Agency RACF Administration utilize a spreadsheet or other method to track assigned user IDs.

Additional User ID Requirements:

User IDs are not be reused.

Group Access (GRPACC) is never assigned to a user ID.

Automatic Dataset Protection (ADSP) is never assigned to a user ID.

OPERATIONS attribute is only assigned to the system Disaster Recovery/emergency user ID and to Finance, ISD, mainframe support staff with responsibility for dataset management.

AUDITOR attribute is only assigned to the assigned auditor from Public Examiners Office and the primary State RACF Administrator.

SYSTEM SPECIAL attribute is only assigned to State RACF Administrators and the system Disaster Recovery/emergency user ID.

Only State RACF Administration assigns GROUP SPECIAL attribute to entity staff designated as Agency RACF Administrators.

Do not create user IDs similar to software commands (i.e. rvary, cemt, cssn etc.).

The OWNER of RACF user ID profiles shall be a group. The OWNER is never to be a user ID.

The OWNER Group and DEFAULT Group for a user ID profile shall be the same.

User IDs that have *never* been used for sixty days from date of creation will be deleted.

User IDs that have been inactive for 60 days will be revoked. RACF System Options enforces this requirement.

User IDs that have *not* been used for six months will be deleted.

If an individual moves from one entity (agency/billing unit) to another entity (agency/billing unit), the original user ID should be deleted and a new user ID assigned.

Group user IDs and/or Passwords are not to be established or used. A single user ID used by multiple users or a password knowingly used by more than one individual is called a group user ID or Group Password. Exception: When an application allows only a single user ID and/or Password and multiple users exist.

The unauthorized retrieval of stored user IDs and/or passwords, whether they appear in encrypted or unencrypted form is prohibited. Computer and communication systems should be designed, tested and controlled to prevent such unauthorized retrievals.

Only user IDs with GROUP SPECIAL attribute shall be assigned the Class Authorization (CLAUTH) attribute. Only the appropriate resources for which the user ID is responsible shall be assigned. Example: CLAUTH=USER, CLAUTH=TCICSTRN, etc.

GROUP SPECIAL attribute shall be assigned only to user IDs for staff that have completed the User ID, Group, System Options, and hands-on RACF classes.

PASSWORDS – AUTHENTICATION

RACF Passwords shall consist of eight characters. The composition of a password is a combination of alpha and numeric values. National characters (#,$,@) may also be used. RACF System Options enforces this requirement.

User IDs will be revoked after three (3) consecutive unsuccessful attempts at entering a valid password. RACF System Options enforces this requirement.

The maximum password interval (period between password changes) is 60 days. RACF System Options enforces this requirement. The password interval can be less than 60 days.

A person can change their own password only once a day. A further change of a password on day it is originally changed is completed by Agency RACF Administration or State RACF Administration.

Non-expiring passwords are assigned only to functional user IDs.

Documentation shall exist concerning the necessity of the user ID with a non-expiring password. The necessity includes the function, purpose of the user ID plus why it has a non-expiring password.

User IDs with a non-expiring password shall be assigned the RESTRICTED attribute.

Passwords shall not be reused for at least 24 consecutive changes. RACF System Options enforces this requirement.

All vendor-supplied default passwords shall be changed at the time the software is installed.

GROUPS

Groups are to be established for specific purposes. Examples of the types of valid groups are: users requiring access to a RACF protected resource, OWNER of RACF profiles, and owners of functions (i.e. started tasks, applications etc.).

State RACF Administration establishes on RACF an entity's first group. This first group is the entity's SDC Code.

> This first group shall not be in any access lists.
>
> The only user IDs connected to the group are the user ID(s) of staff established as Agency RACF Administrator.

The OWNER & SUPERIOR group of an entity's first group established by State RACF Administration shall be AGENCIES.

The first two characters of a group shall be the entity's (agency or primary billing unit) identifier (SDC Code).

If two or more user IDs need access to the same information resources, a group should be developed and used in appropriate access lists.

The OWNER of RACF group profiles is to be a group. The OWNER is never to be a user ID.

All groups created for or by an entity are to have the primary entity group or a subgroup of the primary entity group as the SUPERIOR group.

The SUPERIOR Group and OWNER Group of a group are to be the same.

Group established as OWNER of general resource and dataset resource profiles shall not have user IDs connected, nor occur in any access lists.

NOTERMUACC shall be assigned to groups that are high-level qualifiers for datasets. Exception: The agency /entity group whose name is the SDC Code. These groups are the high-level group for the entities users, groups, and datasets.

A group shall exist that contains only the user ID(s) assigned the OPERATION attribute. This group shall be placed in access lists of all resources that contain data from IRS, SSA and other sensitive data. The access level is NONE. The group name containing user IDs with OPERATION attribute is ALOPERTN.

Only user IDs with the SYSTEM SPECIAL or GROUP SPECIAL attributes, and mainframe system software support staff (ISD Tech Support), are connected to group VRAUSERS.

Functional user IDs shall be placed in a group specifically for functional user IDs.

Groups containing functional user IDs shall not be placed in resource access lists.

USER ID GROUP CONNECTION

The data field Universal Access (UACC) for user ID connection to a group shall be NONE.

The data field AUTHORITY for user ID connection to a group shall be USE.

Only State RACF Administration can assign CONNECT AUTHORITY greater than USE.

The OWNER group and CONNECT group shall be the same.

DATASETS

The Universal Access (UACC) of dataset profiles should be NONE.

The OWNER of RACF dataset profiles shall be a group.

The OWNER group shall never be a user ID.

The OWNER group shall not have any connected user IDs

The OWNER group shall not be in any access lists.

The OWNER group shall not be the entity’s first group (the group whose name is the SDC Code).

High-level qualifier/alias shall have a backstop profile.

UACC of backstop profile is NONE.

Access list of backstop profile is empty.

GENERAL RESOURCES

The Universal Access (UACC) of general resource profiles should be NONE. If UACC is greater than NONE, installation data should include justification/reason.

The OWNER of RACF general resource profiles shall be a group.

The OWNER group shall never be a user ID.

The OWNER group shall not have any connected user IDs.

The OWNER group shall not be in any access lists.

The OWNER group shall not be the entity’s first group (the group whose name is the SDC Code).

SURROGAT Profile:

Every user ID with the PROTECTED attribute shall have a SURROGAT profile.

Userids with assigned attributes SPECIAL, OPERATIONS, or AUDITOR shall not have a SURROGAT profile.

The DB2 SYSADM user ID shall not have a SURROGAT profile.

Only user IDs for authorized Help Desk staff shall be connected to the appropriate FACILITY(IRR.PASSWORD) profile.

GROUP TREE FOR DE-CENTRALIZED RACF SECURITY ADMINISTRATION

Level one is the software package installation group (‘SYS1’) for RACF.

Level two is the group (‘AGENCIES’) to which agencies utilizing the state’s mainframes are connected.

Level three consists of the primary group (SDC Code) for entities utilizing the state’s mainframes.

Level four, and subsequent levels, consist of appropriate subgroups, and if used, should be connected to the appropriate owning level.

UNIX

A uid shall be assigned only to user IDs that need to work in the UNIX side of the mainframe and are required to have an OMVS segment.

A gid shall be assigned only to groups that need to work in the UNIX side of the mainframe and are required to have an OMVS segment.

Every user ID with a valid uid shall be connected to an appropriate group with a valid gid.

The OWNER group and DEFAULT group of a user ID with an OMVS segment shall be a group with a gid.

ADDITIONAL INFORMATION:

Information Technology Policy 663: RACF Security
http://cybersecurity.alabama.gov/documents/Policy_663_RACF_Security.pdf

Information Technology Standard 663S1: RACF System Options
Limited Distribution: Email cyber.security@isd.alabama.gov to request a copy of this document

Information Technology Standard 663S3: RACF User Identification and Authentication
http://cybersecurity.alabama.gov/documents/Standard_663S3_RACF_User_IA.pdf

Information Technology Dictionary
http://cybersecurity.alabama.gov/documents/IT_Dictionary.pdf

By Authority of the Office of IT Planning, Standards, and Compliance

DOCUMENT HISTORY:

Version	Release Date	Comments
663S2-00	06/07/2012	Original document
663S2-01	10/24/2012	Changed user ID requirements and functional user ID group assignment
663S2-02	05/29/2014	Updated password history requirement (from 12 to 24); repaired hyperlink