

STATE OF ALABAMA

Information Technology Policy

POLICY 663-01: RACF SECURITY

Access to State of Alabama information systems must be authorized, authenticated, and audited to ensure that only authorized users gain access to State resources and data. Access, in a computer-based environment, means the ability to do something with a computer resource (for example, use, change, or view something). Access control is the method by which this ability is explicitly enabled or restricted. The access control principle says that access to resources is controlled in such a way that permission to use them is restricted to just those people whose normal duties require their use.

Resource Access Control Facility (RACF®) is an add-on software product that provides basic security for a mainframe system. RACF protects resources by granting access only to authorized users of the protected resources. Major software products such as CICS®, VTAM®, and DB2® also use the facilities of RACF to protect transactions and files.

OBJECTIVE:

Manage user access to critical resources while maintaining a flexible and responsive access control strategy and ensuring the security principles of least privilege and separation of duties through the careful administration of RACF security policies and standards.

SCOPE:

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

RESPONSIBILITIES:

Information Services Division (ISD) and State RACF Administration:

Implement the security assessment process, security activities and security policies for the Department of Finance; Information System Division (ISD).

Provide de-centralized RACF Administration that is effective and easily maintained.

Establish an entity's Agency RACF Administrator(s) on the State Data Center (SDC) mainframe.

Advise and guide Agency RACF Administration.

Work with the entity's Agency RACF Security Contact in matters relating to the implementation of RACF for the entity.

Provide RACF training to Agency RACF Administrators.

Perform RACF administration functions for agencies without a trained RACF Administrator. Includes establishing user IDs, setting of initial passwords, resetting of passwords for the entity, creating dataset and general resource profiles and establishing access rights to entity owned dataset and general resource profiles.

State RACF Administration may complete RACF administrative actions for an entity with an Agency RACF Administrator only with acknowledgement from that Agency RACF Administrator.

Determine and administer access rights for shared mainframe resources (such as TSO).

Create and document RACF policies, procedures, standards, and guidelines.

Monitor the implementation and compliance of adopted RACF policies and standards.

Support State and system-level audits and assist with agency-level audits.

Monitor the RACF database. Based upon findings, recommend and/or take appropriate actions.

Identify the appropriate individual(s), within the entity(ies) directly supported by them, who can appropriately request and/or authorize permissions, profiles, privileges, accesses and other entrustments for such entity-related applications and data.

Agency Management, Information Technology Organization:

All organizations that utilize mainframe-based resources shall designate at least one individual to be responsible for RACF activities within the organization.

- The individual(s) designated to implement the security assessment process, security activities, and security standards/policies for the organization is referred to as "*Agency RACF Administration.*"
- The individual(s) designated to act as liaison to the State RACF Administrator for the purpose of performing RACF administration functions on the entity's behalf is referred to as "*Agency RACF Security Contact.*"

An entity that does not have an Agency RACF Administrator shall designate an Agency RACF Security Contact.

Ensure Agency RACF Administrators attend classroom training (provided by the State RACF Administrator). This training is required before the Agency Administrator will be granted the rights necessary in order to perform RACF administration functions (maintenance of RACF profiles and determination of access rights). Contact the State RACF Administrator to schedule training.

Agency-level audits of RACF and related resources are the responsibility of the agency and the Agency RACF Administrator. The State RACF Administrator can provide limited audit assistance on a case-by-case basis when requested by Agency Management.

Agency RACF Administration:

The person(s) designated by an agency/department/entity to implement RACF for their entity is identified as Agency RACF Administration. Depending on the nature of the entity and the individual, this may be a part-time or full-time activity.

Agency RACF Administration is designated to implement the security assessment process, security activities and security policies for their entity.

Agency RACF Administration implements and maintains the entity's use of the RACF package. This includes, but is not limited to, the establishment of user IDs; setting of initial passwords, resetting of passwords for the entity and establishing access rights to entity owned dataset and general resource profiles.

Agency RACF Administration is responsible for identifying the appropriate individual(s), within the entity(ies) directly supported by them, who can appropriately request and / or authorize permissions, profiles, privileges, accesses and other entrustments for such entity-related applications and data.

Agency RACF Security Contact:

Agency RACF Security Contact is designated to implement the security assessment process, security activities and security policies for their entity.

Agency RACF Security Contact is the liaison with State RACF Administration relating to RACF implementation and maintenance for their entity.

Notify and provide appropriate documentation to State RACF Administration for establishment of appropriate user ID, group, dataset and general resource profile and access requirements.

Notify State RACF Administration upon termination of an employee.

The Agency RACF Security Contact should know and understand the entity's RACF implementation.

Agency RACF Security Contact is responsible for identifying the appropriate individual(s), within the entity(ies) directly supported by them, who can appropriately request and / or authorize permissions, profiles, privileges, accesses and other entrustments for such entity-related applications and data.

ADDITIONAL REQUIREMENTS:

Ownership – Custodian:

Each major information resource (application, dataset, data, or other information resource) possessed by or used by an entity shall have a designated owner. Owners or their delegate shall determine appropriate sensitivity classification as well as criticality ratings. Owners or their delegate shall make decisions about access permissions to the information resource, and the uses to which the information resource will be put. Owners shall additionally take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, regular usage and protection of information resources.

Department of Finance, Information Services Division (ISD) is the custodian of an entity's data and other information resources. With the exception of operational computer and network information resources, ISD is not the owner of any entity's information resources. ISD will follow / adhere to the standards / policies and instructions concerning security of an entity's information resources residing on the Department of Finance, ISD mainframe.

Monitoring Requirements:

Once a year each entity shall review their RACF implementation for user ID, group, dataset and general resource profiles. The review checks for compliance with all security standards & policies. The entity shall take or approve appropriate actions concerning information or implementation features not meeting standard and/or policy.

Each entity (Resource Owner) shall review for accuracy access lists of dataset and general resource profiles they manage.

Security Assessment:

Resource Access Control Facility (RACF) is designed to provide security protection for an entity's information resources (i.e. datasets, files, programs, applications etc.). To implement security and utilize RACF to provide the security for an entity's information resources, an entity should complete the following activities of a security assessment:

Identify an entity's information resources (e.g. data files, programs) residing in the Department of Finance mainframe (State Data Center)

Establish:

- The unique ownership of each resource
- Who the owner considers to be the authorized individual to determine access rights to those resources
- Who and/or what, both within the entity and outside the entity, has access rights to which information resource
- The types of access rights (i.e. create, read, update, delete etc.) for each individual or function requesting access

Determine roles and relationships between the information resources and the holders of access rights to those information resources

Implement the security mechanisms identified (i.e. unique user identification [user ID], group, dataset and general resource profiles) for each of the entity's relationships, keeping the implementation current as the resources / who's / what's and authorizations change.

ADDITIONAL INFORMATION:

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 663S2: RACF Architectural Strategies
http://cybersecurity.alabama.gov/documents/Standard_663S2_RACF_Architectural_Strategies.pdf

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 Director, Information Services Division, Department of Finance

DOCUMENT HISTORY:

Version	Release Date	Comments
663-00	12/06/2011	Original document
663-01	06/07/2012	Added responsibilities (to all entities) and Additional Requirements