STATE OF ALABAMA

Information Technology Standard

STANDARD 663S3-01: RACF USER IDENTIFICATION AND AUTHENTICATION

To ensure individual accountability, State IT Policy 621 requires every State information system user to have an individual system access account (i.e., a unique user identifier); therefore, every mainframe system user shall have an individual Resource Access Control Facility (RACF) profile with a unique user ID.

OBJECTIVE:

Manage mainframe user authorization, identification, and authentication.

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:

USER IDENTIFICATION (USER ID)

State RACF Administration, or appropriate Agency RACF Administration, are responsible for the creation of a user ID for an individual or function. An Agency RACF Security Contact may authorize State RACF Administration to create a user ID for their agency personnel.

An individual is issued a user ID only when their supervisor or manager provides a written request for the issuance of a user ID. Positive identification of users and required information resources shall occur prior to access or usage. The Department of Finance utilizes the MAINFRAME ACCESS AUTHORIZATION FORM (which can be found at http://cybersecurity.alabama.gov/forms.aspx) to assign user IDs. Other entities are encouraged to utilize this form or a similar form provided all appropriate signatures are affixed.

An individual's role, job responsibilities and duties determine the access privileges granted to their user ID. An individual's supervisor or manager shall identify, as appropriate, access privileges required (i.e. CICS, TSO, and ROSCOE etc.). Mainframe permissions, privileges, accesses and other entrustments are to be granted to an individual based solely on the needs of that individual to accomplish their assigned job duties and responsibilities.

Individuals needing access to any ISD mainframe data processing resources, applications and/or data must request and receive written permission from the individuals authorized to grant the required permissions, profiles, privileges, accesses or other entrustments. The MAINFRAME ACCESS AUTHORIZATION FORM is used to authorize permission to datasets and general resources. Some resource authorizations do not require written permissions (contact State RACF Administration to determine).

Each mainframe information resource Administration (a.k.a. Software or Application Administration) is authorized to approve permissions, profiles, privileges, accesses and other entrustments for ISD data processing resources over which they have direct functional responsibility. Programmers, operators, technicians, supervisors, managers or mainframe resource administrators lacking direct functional responsibility for a resource are not authorized to approve, grant or permit access to such information resource(s).

When an individual is terminated (voluntarily or involuntarily) from employment, the employee's supervisor shall notify, as appropriate, the State RACF Administration or Agency RACF Administration / Agency RACF Security Contact. Department of Finance ISD supervisors will use the Departure Notification procedures to notify the State RACF Administration to have the user ID and access privileges revoked.

When an individual is voluntarily or involuntarily assigned different duties or to a different position, the employee's supervisor, prior to the reassignment, shall notify, as appropriate, the State RACF Administration or Agency RACF Administration / Agency RACF Security Contact. ISD supervisors will notify the State RACF Administration to have the user's access privileges revoked or modified as appropriate.

When the reason for a user ID assigned to a function no longer exists, the entity responsible for use of the user ID is responsible for notifying the State RACF Administration or appropriate Agency RACF Administration / Agency RACF Security Contact to have the user ID and access privileges revoked.

The person to whom a user ID is assigned is responsible for all activities affected through all sessions established through such user ID.

The user ID and its corresponding password are established for an individual or function, to access-authorized systems and data and are only for the sole use of the assigned individual or function. The user ID and password are not to be used by any individual other than the assigned user. They are not to be distributed or disseminated in any manner to other individuals or shared with another individual.

A user ID / password shall not remain logged on to an unattended workstation (terminal or personal computer (PC)).

User IDs shall be revoked after three (3) consecutive unsuccessful attempts at entering a valid password. RACF System Options enforces this requirement. After three unsuccessful attempts, the system will revoke the user ID, thus requiring the user ID be resumed. A RESUME should only be accomplished after verification of the identity of the person assigned the revoked user ID. If dial-up or other external network connections are involved, the session should be terminated.

A user ID assigned to a specific individual shall not be used as a functional user ID.

AUTHENTICATION - PASSWORDS

Password Construction:

Passwords shall consist of eight (8) characters. The password shall be comprised of both alpha and numeric characters. National characters (#, @ $) may also be used. Passwords should be non-associative. Non-associative passwords cannot be easily guessed, are not related to the user's job, personality or personal life and are not found in the dictionary or some other part of speech. Passwords are not constructed that use a basic sequence of characters that is then partially changed based on the date or some other predictable factor. Passwords should not be constructed which are identical or substantially similar to previously used passwords. Passwords should not be a repetition, realignment or restatement of the user ID. Passwords similar to software commands (i.e. rvary, cemt, close, open etc) are not to be used. Derivatives of user IDs and common character sequences (i.e. 123456", "abcdef") should not be used.

Password Management:

Passwords must be changed every sixty- (60) days. RACF System Options enforces this requirement. The first time an attempt to use a user ID that has not had the password changed within sixty (60) days will be automatically revoked. The password interval can be less than 60 days. Users are expected to change their passwords periodically, depending on the sensitivity of the system(s) or data, application or package implementation, and federal, state or local requirements.

Passwords for a specific user ID shall not be reused for 24 consecutive changes. RACF System Options enforces this requirement.

The initial password is valid only for the first logon of the user ID. The individual assigned the user ID is expected to change the initial password within 96 hours of their receipt of the initial password.

Passwords should not be written down! Passwords should be committed to memory.

Passwords shall not be contained in macros or scripts. Passwords shall not be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorized individuals might discover them. Passwords should not be hard-coded into application or system software.

Only the individual to whom the password associated user ID is assigned is to know the password.

Passwords shall be protected from unauthorized disclosure or misuse by appropriate administrative, technical and physical controls. Systems using passwords for access control shall not display or print the actual password (masking or stilled cursor are acceptable practices).

A password shall be changed whenever it has been compromised or it is suspected that the password has been compromised. If an employee suspects their password has been compromised, they are to report the incident and circumstances to their supervisor immediately. The supervisor shall immediately report the incident to the appropriate State or Agency RACF Administration / Agency RACF Security Contact.

When applications on the mainframe that do not utilize RACF for user identification and authentication require separate logon (in addition to logon to mainframe), users shall employ different passwords on each of the applications/systems to which they have been granted access.

Password Resets:

The appropriate Agency RACF Administration, Agency Help Desk, Finance ISD Help Desk or State RACF Administration resets passwords.

Agency RACF Security Contact requests password resets for their entity from Finance ISD Help Desk.

The Finance ISD Help Desk or State RACF Administration will reset passwords for individuals whose entity does not have Agency RACF Administration. Requests for resumption of revoked user IDs are made by the entity's Agency RACF Security Contact.

Resuming a Revoked User ID:

The appropriate Agency RACF Administration, Agency Help Desk, Finance ISD Help Desk or State RACF Administration resumes user IDs that are revoked.

Agency RACF Security Contact requests resume of user IDs for their entity from Finance ISD Help Desk.

The Finance ISD Help Desk or State RACF Administration will resumed revoked user IDs for individuals whose entity does not have Agency RACF Administration. Requests for resumption of revoked user IDs are made by the entity's Agency RACF Security Contact.

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

Information Technology Policy 621: Network and System Access
http://cybersecurity.alabama.gov/documents/Policy_621_Network_System_Access.pdf

Mainframe Access Authorization Form
http://cybersecurity.alabama.gov/documents/RACF/Mainframe_Access_Authorization_Form.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
663S3-00	06/07/2012	Original document
663S3-01	05/29/2014	Updated password history requirement (from 12 to 24)