

Title: Mainframe Account Authorization, Review, and Revocation Procedures
Effective Date: September 13, 2006
Review Date: November 22, 2011
Issuing Authority: Chief Information Security Officer

SCOPE

These procedures apply to individuals accessing the Financial Management System (FMS), the Human Resources System (HRS) and the Student System (ISIS). It gives direction to all mainframe Data Stewards, Data Steward Designees, Account Administrators, and those involved with determining access authorization for users of the University's mainframe applications.

PURPOSE

The purpose of this document is to establish procedures for the authorization, review, and revocation of an individual's access to mainframe applications, such as the Financial Management System (FMS), the Human Resources System (HRS) and the ISIS student system. The procedures also describe the process for revoking access to these applications

ASSUMPTIONS

The procedures below discuss the process whereby a RACF Administrator, Data Steward, and an Account Administrator perform certain functions to add and remove users from the mainframe. Detailed procedures are on file as to how access is added and revoked by the RACF/Account Administrators.

DEFINITIONS

1. Authorized User – A person who has been authorized to access electronic media and services and who invokes or accesses an electronic media and service for the purpose of performing his or her job duties or other functions directly related to his or her affiliation with Temple University. The authorization granted is for a specific level of access to the electronic media and service as designated, unless otherwise defined by University policy.
2. RACF – The Resource Access Control Facility (RACF) is the security component of the mainframe operating system. It controls all user access to the mainframe.
3. RACF Administrator – A Computer Services Office of Information Security individual who controls access to all mainframe resources and is responsible for the creation and maintenance of mainframe user accounts, user ID's, and initial passwords.
4. Account Administrator – An Administrative Computer Services individual who is responsible for the maintenance of user accounts.
5. Data Steward – The budget head or senior management individual who is ultimately responsible for the information belonging to an application.
6. Data Steward Designees – Managers or supervisors of personnel who have access to the mainframe application systems. The Data Steward Designees relay user requests for account creation, maintenance, deletion, and other issues to the Account Administrator

7. ISIS Coordinators – School and college and/or central administration personnel who coordinates all access to ISIS for users under their jurisdiction. The ISIS Coordinators may also be referred to by policy as ISIS Data Steward Designees. The ISIS Coordinators relay user requests for ISIS account creation, maintenance, deletion, and other issues to the ISIS Account Administrator.

ACCESS AUTHORIZATION PROCEDURES

Access to mainframe applications will be granted based on legitimate business need as determined by the individual's supervisor and the data steward

Access will be granted by the account administrator after receiving approval from the user's supervisor and the data steward

ACCESS REVIEW PROCEDURES

Access to mainframe applications will be reviewed periodically in accordance with the following procedures:

1. Schedule for Access Review

- a. ISIS Review – the Student System will be reviewed for authorized access during the Fall, Spring, and Summer semesters for a total of three times per annum. The ISIS coordinators (Data Steward Designees) are required to verify that each account on the list should remain active. **ISIS coordinators must sign, date, and return the account listings to the ISIS Account Administrator within 10 business days of distribution. If the coordinator fails to return the list within 10 business days, then all accounts on the list will be suspended until the list is received.**
- b. FMS Review – the Financial Management System will be reviewed annually by the Data Stewards and Designees to re-approve all users and their access. This review presupposes that all access is explicitly denied unless re-authorized through this process. Additionally, another review will take place within 6 months following the annual review whereby Data Stewards and Designees will perform an exception based review, reporting all access to the Account Administrator which is no longer valid or authorized.
- c. HRS Review – The Human Resources System will be reviewed annually by the Data Stewards and Designees to re-approve all users and their access. This review presupposes that all access is explicitly denied unless re-authorized through this process. Additionally, another review will take place within 6 months following the annual review whereby Data Stewards and Designees will perform an exception based review, reporting all access to the Account Administrator which is no longer valid or authorized.

2. Generation of Access Reports

To facilitate the review schedule listed above, the Account Administrator will generate a report of all accounts which have access to the mainframe application systems under the scope of this document. This report will detail the level of access each account maintains. The report will be distributed to the Data Steward Designees for review.

3. Data Steward Designee Review

- a. Each Data Steward Designee will review each account under their responsibility for appropriateness. An individual user must only have access to the screens and data fields

necessary to perform his or her job responsibilities. All access above and beyond that which is required for the person's job function is considered unauthorized.

- b. If a Data Steward Designee determines that an inappropriate level of access is granted to an individual, the Data Steward Designee will inform the Account Administrator and all noted access will be removed.
- 4. Data Steward Authorization**

After the Data Steward Designee review, three times annually for ISIS and annually for HRS and FMS a final report will be generated that contains all accounts along with the access they have to the application system. The Data Steward will review the report and will sign the report as authorized, only if access is appropriate. The authorized report will be sent to the office of the Chief Information Security Officer and kept on file until the next authorized report is released.
 - 5. Office of the Chief Information Security Officer**
 - a. Internal Audits will perform spot checks to determine the appropriateness of access. The Office of the CISO will correct all access determined to be inappropriate.
 - b. All user accounts to the mainframe application systems must be owned by an individual. Any account that is shared by more than one person or that is used for a system function must be documented and approved by the Chief Information Security Officer.
 - 6. Returning a SecurId Token**

A SecurId Token that is returned to the RACF Administrator (other than for replacement) is an indication that access to the administrative mainframe is no longer needed by the cardholder. If the cardholder has FMS, HRS, or ISIS access, the RACF Administrator will remove the cardholder's RACF account and will notify the Account Administrator to deactivate the user's account(s).

ACCESS REVOCATION PROCEDURES

When an individual resigns, is terminated, transfers, or for any reason no longer needs access to mainframe applications, the account holder's access will be immediately revoked.

- 1. Notification From Management**

The Budget Unit Heads, supervisors, or the Data Steward Designees must notify either the Account Administrator or to the RACF Administrator, indicating that a subordinate employee should no longer have access to mainframe application(s). When the Account Administrator receives this notice, the administrator will immediately deactivate the user's application account and will notify the RACF Administrator to remove the employee's access to the application(s) through RACF and Netview Access Services.
- 2. Notification From User**

Application account holders may send written notice to the RACF and Account Administrators stating that access to the application is no longer needed. The RACF Administrator will remove access to RACF and Netview Access Services and the Account Administrator will remove access to the application.

3. **Periodic Revocation of RACF Accounts**

On a quarterly basis, the RACF Administrator will compare RACF accounts to an extract from the Human Resource System to ensure that accounts are deactivated for terminated employees. If application access is involved, the RACF Administrator will notify the Account Administrator to deactivate the user's application account(s).

4. **Periodic Review of Application Accounts**

On a quarterly basis, the Account Administrator (where applicable) will review all deactivated application accounts, will produce a backup of all security records associated with the deactivated application account users, and will then remove the accounts from the system.

5. If the notice is first received by the RACF Administrator, the RACF Administrator will remove the employee's access to the application(s) through RACF and Netview Access Services. The RACF Administrator will then notify the Account Administrator to deactivate the user's application account(s).