Security Standard: Account Management

Scope

This standard applies to all RIT Information and Information Resources.

Requirements for All accounts

The following security controls are required to be implemented on all accounts:

1. **Account Authentication**
   - 1.1. End user account authentication should use the enterprise identity and access management service when the system or application processes Private, Confidential, or Critical Process information.
   - 1.2. The use of the enterprise authentication service by an application should be authorized by the Authentication Service Provider and the security reviewed by ITS.
   - 1.3. Password Management
     - 1.3.1. Access to passwords and their hashes should be restricted, Therefore, public terminals and kiosks should not cache user passwords/passphrases
     - 1.3.2. All password changes should be logged, but the password itself should not be logged.

2. **Account Authorization**
   - 2.1. Account authorization should use the enterprise identity and access management service or role-based account authorization native to the application when the system or application processes Private, Confidential, or Critical Process information.
   - 2.2. Data Owners should authorize:
     - 2.2.1. A process for approving and documenting authorization. Authorization granted to an account should be commensurate with the level of identity validation performed
     - 2.2.2. The parties who may approve user access to roles
     - 2.2.3. Roles and their privileges following the security principles of Least Required Access and Segregation of Duties.

3. **Account Provisioning**
   - 3.1. Account Establishment: Each account should be for the individual use of a specific person with an academic or business need for this access.
     - 3.1.1. Employees who have multiple roles with the University should have role-based access provided such that when one of the roles is changed, the access for that role can be changed without impacting the other role. In the event this cannot be achieved technically, then separate accounts are required to fulfill the requirements of each role.
     - 3.1.2. Student employees should have separate accounts from their student accounts. The student accounts may not have student employee-related access.
     - 3.1.3. Physical access granted by student IDs should have a termination date pre-populated at the time of hire.
   - 3.2. Account Duration: Accounts are valid when the individual account holder has authorized access to the account or until the account is suspended by the University.

3.3. Authorized Administrators should
  3.3.1. Review approvals and provision account/access
  3.3.2. Track authorizations, including:
    - Date of authorization
    - Identification of individual approving access
    - Identification of the role assigned (where applicable) or description of the access privileges granted. The access privileges granted should only be used to fulfill assigned job duties.
    - These authorizations should be retained in accordance with the Records Management Policy (C22.0).

4. Account Management and Maintenance

4.1. Access Review:
  4.1.1. Managers are responsible for reviewing account and access privileges with the employee upon notification of job changes (e.g., termination, job changes).
  4.1.2. Data owners of Private information identified by ITS should review all accounts and access privileges at least annually to ensure that they are commensurate with job function, need-to-know, and employment status.

4.2. Account Change Communication: Managers are responsible for communicating to account administrators when an account or access privileges may require modification or deactivation.

4.3. Account Modification: Upon notification, the account administrators will review account and access privileges with the data owner or designee. All changes to accounts and access privileges should be approved and formally documented.

4.4. Account Deactivation: Upon notification, account administrators are responsible for the immediate deactivation of accounts and access privileges when continued access is no longer required (e.g., terminated). All deactivation of accounts and access privileges should be formally documented.

4.5. Account Lockout /Reset
  4.5.1. Authentication systems should disable user accounts after a set number of failed logon attempts.
  4.5.2. Administrators should follow established procedures for re-enabling or resetting user accounts once they have been disabled or upon request by the user. They should verify user identity prior to re-enabling or resetting user accounts. These procedures should take into consideration the potential risk to determine if automated procedures and the lockout time duration are appropriate.
  4.5.3. Administrators may not use the University Identification Number as the sole verification for resetting passwords.

Requirements for Special Accounts

The following security controls are required to be implemented on special accounts:

5. **Provisioning Administrator and Service Accounts:** Requirements for issuing Administrator and Service Accounts are the same as other accounts with the following additions and changes:
   - 5.1. Account Establishment
     - 5.1.1. Ownership of an administrator account or group should be assigned to an individual.
     - 5.1.2. Service accounts should be assigned to a system or application and are not for individual use.
   - 5.2. Account Usage: Administrator and Service Accounts are specifically for system or application use only and should not be used for any purpose other than the administration or operation of the system or application. However, service accounts should be assigned to an account administrator.
   - 5.3. Group Access: Administrator and Service Accounts may be shared by a limited group of individuals for the purpose of operation and administration of the application or system, and only where required by the system or application. (In these cases, when possible, access to system accounts should be by methods that allow the individual to authenticate using a username and password.)
   - 5.4. **Default Administrative or Service Accounts**: Accounts that are part of the default setup of a system (including, but not limited to configuration access, database accounts, etc.) should be removed, disabled, or changed (in that order) whenever possible.
   - 5.5. **Service Accounts**: Service accounts should be reassigned and passwords of the service accounts changed when the account administrator is no longer in that role.

6. **Sponsored Accounts**: Requirements for sponsored accounts are the same as other accounts with the following additions and changes:
   - 6.1. All sponsored accounts (for those who do not receive an account based on their role at RIT) with access to RIT information resources should contain an expiration date of no more than one year or the work completion date, whichever occurs first. Only authorized RIT account holders can approve sponsored accounts.
   - 6.2. Upon termination of the Sponsor's account, the Sponsored account should be transferred to another appropriate RIT account holder or be deactivated.

7. **Generic/Shared Accounts:** Requirements for Generic/Shared Accounts are the same as other accounts with the following additions and changes
   - 7.1. Each generic or shared account should have a designated owner who is responsible for the management of access to that account. The owner should log access to the generic or shared account.
   - 7.2. **Shared Generic Accounts:** Generic accounts may only be shared in those situations where a system (server), device (switches or routers) or application cannot support the use of individual accounts technically.

Effective Date: January 23, 2015

Standard History:
November 11, 2013
October 19, 2015