Policy Title: Account Management

Policy Type: Administrative


Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Account Management defines the steps necessary to protect the confidentiality, integrity, and availability of IT systems and information against compromise. Account Management requirements identify the measures needed to verify that all system users are who they say they are and that they are permitted to use the systems and information they are attempting to access.

TABLE OF CONTENTS

| Contacts | 1 |
| Stakeholder(s) | 1 |
| Purpose | 2 |
| Requirements | 2 |
| Violations | 5 |
| Interpretation | 6 |
| Publication | 6 |
| Review Schedule | 6 |
| Related Documents | 6 |

CONTACT(S)

Office of Information Technology – (757)823-2869

STAKEHOLDER(S)

University Faculty & Staff
Office of Information Technology
PURPOSE

This control is intended to establish the steps necessary to formalize the process of requesting, granting, administering, and terminating accounts. The University should apply these Account Management practices to all accounts on IT systems, including accounts used by vendors and third parties.

REQUIREMENTS

NSU manages information system accounts, including:

1. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);

2. Establishing conditions for group membership;

3. Identifying authorized users of the information system and specifying access privileges;

4. Requiring appropriate approvals for requests to establish accounts;

5. Establishing, activating, modifying, disabling, and removing accounts;

6. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;

7. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;

8. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users;

9. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and

10. Reviewing accounts and privileges at least annually.

Supplemental Guidance: These requirements distinguish between internal and external IT systems. Internal IT systems are designed and intended for use only by University employees, contractors, and business partners. External IT systems are designed and intended for use by University customers and by members of the public. University employees, contractors, and business partners may also use external IT systems. Users requiring administrative privileges on information system
accounts receive additional scrutiny by Information Security Officers responsible for approving such accounts and privileged access.

Control Enhancements for Sensitive Systems:

1. The information system automatically terminates temporary and emergency accounts after a predetermined period based on sensitivity and risk.

2. The information system automatically disables inactive accounts if not used for a predefined period. Note* Agencies should strongly consider locking accounts that go unused for 90 consecutive days.

3. NSU:
   a. Monitors for atypical usage of information system accounts; and
   b. Reports atypical usage to designated organizational officials.

4. NSU tracks and monitors privileged role assignments.

   Enhancement Supplemental Guidance: Privileged roles include, for example, key management, network and system administration, database administration, web administration.

NSU shall or shall require that its service provider document and implement account management practices for requesting, granting, administering, and terminating accounts. At a minimum, these practices shall include the following components:

1. For all internal and external IT systems:
   a. Prohibit the use of shared accounts on all IT systems. Those systems residing on a guest network are exempt from this requirement.
   b. Disable unneeded accounts.
   c. Retain unneeded accounts in a disabled state in accordance with the agency’s records retention policy.
   d. Associate access levels with group membership, where practical, and require that every system user account be a member of at least one user group.
   e. Require that the System Owner and the System Administrator investigate any unusual system access activities and approve changes to access level authorizations.
f. Require that System Administrators have both an administrative account and at least one user account and require that administrators use their administrative accounts only when performing tasks that require administrative privileges.

g. Prohibit the granting of local administrator rights to users. An Agency Head may grant exceptions to this requirement for those employees whose documented job duties are primarily the development and/or support of IT applications and infrastructure. These exception approvals must be documented annually and include the Agency Head’s explicit acceptance of defined residual risks.

h. Require that at least two individuals have administrative accounts to each IT system, to provide continuity of operations.

i. The information system automatically audits account creation, disabling, and termination actions and notifies, as required, appropriate individuals.

j. Temporarily disable logical access rights when personnel do not need such access for a prolonged period in excess of 30 days because they are not working due to leave, disability or other authorized purpose.

k. Disable logical access rights upon suspension of personnel for greater than 1 day for disciplinary purposes.

2. For all internal IT systems:

a. Require a documented request from the user to establish an account on any internal IT system.

b. Complete any agency-required background check before establishing accounts, or as soon as practicable thereafter.

c. Require confirmation of the account request and approval by the IT system user’s supervisor and approval by the Data Owner or designee to establish accounts for all sensitive IT systems.

d. Require secure delivery of access credentials to the user based on information already on file.

e. Notify supervisors, Human Resources, and the System Administrator in a timely manner about termination, transfer of employees and contractors with access rights to internal IT systems and data.
f. Promptly remove access when no longer required.

3. For all external IT systems, require secure delivery of access credentials to users of all external IT systems.

4. For all service and hardware accounts:

Document account management practices for all University created service accounts, including, but not limited to granting, administering and terminating accounts. If the service or hardware account is not used for interactive login with the system, the service or hardware account is exempt from the requirement to change the password at the interval defined in the Password Management section of this Standard.

Control Enhancements for Sensitive Systems:

1. If the IT system is classified as sensitive, prohibit the use of guest accounts.

2. If the IT system is classified as sensitive, require requests for and approvals of emergency or temporary access that:
   a. Are documented according to standard practice and maintained on file;
   b. Include access attributes for the account.
   c. Are approved by the System Owner and communicated to the ISO; and
   d. Expire after a predetermined period, based on sensitivity and risk.

3. For all external IT systems:
   a. Require confirmation of the user’s request for access credentials based on information already on file prior to delivery of the access credentials to users of all sensitive external IT systems.

Require delivery of access credentials to users of all sensitive external IT systems by means of an alternate channel (i.e., U.S. Mail).

VIOLATION

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 32-01 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an
individual case basis by the appropriate executive or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

INTERPRETATION

The Information Security Officer is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to the Office of Information Technology. The Information Security Officer reserves the right to revise or eliminate this policy.

PUBLICATION

This policy shall be widely published and distributed to the University community. To ensure timely publication and distribution thereof, the Responsible Office will make every effort to:

1. Communicate the policy in writing, electronic or otherwise, to the University community within 14 days of approval;

2. Submit the policy for inclusion in the online Policy Library within 14 days of approval;

3. Post the policy on the appropriate SharePoint Site and/or Website; and

4. Educate and train all stakeholders and appropriate audiences on the policy’s content, as necessary. Failure to meet the publication requirements does not invalidate this policy.

REVIEW SCHEDULE

- Next Scheduled Review: 05/28/2015

- Approval by, date: Office of Information Technology and 05/28/2014

- Revision History:

- Supersedes (previous policy): OIT 62.8.102 Account Management

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard