



OIT 62.502: Account Management

Responsible Executive: Information Security Officer
Responsible Office: Office of Information Technology
Related Policy: 60.201
Approved-On Date: 2/28/2011
Effective Date: 7/1/2011
Revision Date: 2/1/2011

I. 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.

II. Purpose

The Account Management policy identifies those 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.

The requirements below 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.

III. Scope

This policy applies to all NSU Faculty, staff, students, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties with access to NSU technological resources protected by authentication.

IV. Requirements

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:

Note: It is strongly recommended technical controls be implemented wherever possible to fulfill the following requirements, understanding that manual processes must sometimes be implemented to compensate for technical controls that might not be feasible.

For all internal and external IT systems

1. Grant IT system users' access to IT systems and data based on the principle of least privilege.
2. Define authentication and authorization requirements.
3. Establish policies and procedures for approving and terminating authorization to IT systems.
4. 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.
5. Based on risk, consider use of second-factor authentication, such as tokens and biometrics, for access to sensitive IT systems.
6. Review all user accounts for the user's continued need to access all IT systems.
7. Notify the System Administrator when IT system user accounts are no longer required, or when an IT system user's access level requirements change.
8. If the IT system is classified as sensitive, prohibit the use of guest accounts.
9. Prohibit the use of shared accounts on all IT systems. Those systems residing on a guest network are exempt from this requirement.
10. Prohibit the display of the last logon user ID on multi-user systems. Desktop and laptop systems assigned to a specific user are exempt from this requirement.
11. Lock an account automatically if it is not used for a predefined period.

Note: The University should strongly consider locking accounts that go unused for 90 consecutive days.

12. Disable unneeded accounts.
13. Retain unneeded accounts in a disabled state in accordance with the University's records retention policy.
14. Associate access levels with group membership, where practical, and require that every system user account be a member of at least one user group.
15. Require that the System Owner and the System Administrator investigate any unusual system access activities and approve changes to access level authorizations.
16. 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.
17. Prohibit the granting of local administrator rights to users. The ISO 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 ISO's explicit acceptance of defined residual risks.
18. Require that at least two individuals have administrative accounts to each IT system, to provide continuity of operations.

For all internal IT systems

19. Require a documented request to establish an account on any internal IT system.
20. Complete any agency-required background checks before establishing accounts, or as soon as practical thereafter.
21. Require confirmation of the account request and approval by the IT system user's supervisor and approval by the System Owner or designee to establish accounts for all sensitive IT systems.
22. Require secure delivery of access credentials to the user based on information already on file.

23. 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.

24. Promptly remove access when no longer required.

For all external IT systems

25. Require secure delivery of access credentials to users of all external IT systems.

26. 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.

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

For all service and hardware accounts

28. Document account management practices for all University created service accounts, including, but not limited to granting, administering and terminating accounts.

V. Violations

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 60.201 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.

VI. 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.