



OIT 62.503: Password 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

Faculty, staff, and students with access to computer systems are required to use passwords to protect the integrity of the systems as well as the confidentiality of information stored therein.

II. Purpose

Password Management requirements specify the means for password use to protect IT systems and data.

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 password management practices. At a minimum, these practices shall include the following components:

1. Require the use of a non-shared and a unique password on each account on IT systems, including local, remote access and temporary accounts.
2. Require passwords on mobile devices issued by the agency such as PDAs and smart phones. For mobile phones, use a pin number with a minimum of 4 digits.
3. Require password complexity:
 - a. At least eight characters in length; and
 - b. Utilize at least three of the following four:

- 1) Special characters,
- 2) Alphabetical characters,
- 3) Numerical characters,
- 4) Combination of upper case and lower case letters.

Note: It is considered best practice not to base passwords on a single dictionary word in any language, slang dialect, jargon, and in information such as names, places or things. It is strongly recommended that system users be educated not to base passwords on the above criteria.

Create passwords that can be easily remembered but difficult to decipher by other individuals. One way to do this is to create passwords based on a song title, affirmation, or other phrases. For example, the phrase might be: "This May Be One Way to Remember!" and the password could be: TmB1w2R! (Do not use this example as an actual password.)

4. Require that default passwords be changed immediately after installation.
5. Prohibit the transmission of identification and authentication data (e.g., passwords) without the use of industry accepted encryption standards (see Encryption).
6. Require IT system users to maintain exclusive control and use of their passwords, to protect them from inadvertent disclosure to others.

Note: Avoid writing down passwords in places where they might be unknowingly revealed to someone else. Do not store passwords on-line or in a file or directory unless the file is encrypted.

7. Configure all sensitive IT systems to allow users to change their password at most, once per 24 hour period.
8. Require users of all sensitive IT systems, to include network systems, to change their passwords after a period of 90 days.
9. Require that IT system users immediately change their passwords and notify the ISO if they suspect their passwords have been compromised.
10. Configure all sensitive IT systems to maintain at least the last 24 passwords used in the password history files to prevent the reuse of the same or similar passwords.
11. Provide a unique initial password for each new account of sensitive IT systems and require that the IT system user changes the initial password upon the first login attempt.

12. For sensitive IT systems, deliver the initial password to the IT system user in a secure and confidential manner.
13. Require that forgotten initial passwords be replaced rather than reissued.
14. Shared passwords shall not be used on any IT systems.
15. Prohibit the storage of passwords in clear text.
16. Limit access to files containing passwords to the IT system and its administrators.
17. Suppress the display of passwords on the screen as they are entered.
18. Implement a screen saver lockout period after a maximum of 30 minutes of inactivity for NSU devices. NSU devices with access to sensitive systems or those devices in less physically secure environments must have a lower time out interval documented and enforced.
19. Require passwords to be set on device management user interfaces for all network connected devices.
20. Document and store hardware passwords securely.
21. Implement procedures to handle lost or compromised passwords and/or tokens.
22. Set an account lockout threshold of not greater than 10 invalid attempts and the lockout duration for at least 15 minutes.
23. Do not use University computer system password on any Non-NSU system such as America Online, Yahoo, eBay, etc
24. Do not share NSU passwords with anyone else - including supervisors, administrative assistants, secretaries, department colleagues, or family members.
25. Passwords are to be treated as sensitive and confidential information of the University.
26. Do not mention passwords where they may be overheard by others.
27. Do not hint at the format of a password (e.g., "it rhymes with my family name").
28. Do not reveal a password on questionnaires or security forms.

29. Users are discouraged from using the "Remember Password" feature of applications (e.g., MS Outlook, Netscape Messenger, Eudora, etc.)
30. If someone demands to know your password, refer them to this document or have them contact the Office of Information Technology.
31. If you suspect that a password has been compromised, report this to NSU authorities and change the password immediately.
32. Unauthorized attempts to collect, guess, or crack passwords is a violation of **University Policy 60.201: Acceptable Use of Technological Resources.**

Additional Information for Computer System Administrators

33. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed not later than every 90 days; sooner is preferable.
34. Default vendor passwords must be changed immediately after the installation of vendor software or hardware equipment.
35. Whenever possible, account lockout and automatic notification after a number of incorrect password attempts has been reached must be enforced. The incorrect password threshold must not exceed ten attempts, at which point the account must be locked for a period of time not less than three minutes.
36. Whenever possible, the use of password enabled session lockout must be enforced (e.g., password protected automatic screen savers)
37. Personal computers maintained by OIT must be part of the OIT administered network security database.
38. Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to login interactively. A keyed hash must be used where available (e.g., SNMPv3).

Additional Information for Application Developers

39. Ensure support authentication of individual users, not groups.
40. Do not store passwords in clear text or in any easily reversible form.

41. Provide for some sort of role management such that one person can take over the functions of another without having to know the person's password.
42. Provide support for TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

Password Security Assessment

Password security assessments will be performed on a periodic as well as random basis by NSU system security authorities. If a password is guessed or cracked during one of these security assessments, the user will be required to change it.

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.