

Password Guidelines

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Northern Kentucky University's, NKU's, entire university network. As such, all NKU employees, students, contractors, consultants, temporaries, and vendors, with access to NKU systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any NKU facility, has access to the NKU network, or stores any non-public NKU information.

4.0 Policy

4.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the NKUIT administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.
- All user-level passwords (e.g., email, web, desktop computer, etc.) minimum time to be changed is 1 day.
- All new user-level passwords (e.g., email, web, desktop computer, etc.) will be disabled if not logged into with in 90 days.
- Passwords must be unique from prior passwords.
- Concurrent logins will be restricted to 5.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where 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 log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

4.1 Guidelines

A. General Password Construction Guidelines

Current password construction guidelines are maintained on the NKUIT website.

B. Password Protection Standards

Do not use the same password for NKU accounts as for other non-Northern Kentucky University access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various NKU access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share NKU passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential NKU information.

Password cracking or guessing may be performed on a periodic or random basis by NKUIT or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users

Access to the Northern Kentucky University Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

5.0 Enforcement

Any user found to have violated this policy will be subject to universities disciplinary policies and law enforcement action.

6.0 Definitions

| Terms | Definitions |
|------------------------------------|---|
| Application Administration Account | Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator). |
| TACACS+ | Terminal Access Controller Access Control System is an authentication protocol. |
| Radius | Remote Authentication Dial-In User Service, an authentication and accounting system. |
| X.509 | This is a specification for digital certificates. |
| LDAP | Lightweight Directory Access Protocol. A protocol used to access a directory listing for authentication. |

7.0 Revision History

2/10/2006 - Added additional requirements to section 4.1, to cover unique, minimum password time, concurrent logins, and new accounts with no activity.