PASSWORDS

RESPONSIBLE OFFICIAL TITLE: CHIEF INFORMATION OFFICER
EFFECTIVE DATE: 02/15/2022
NEXT REVIEW DATE: PREVIOUS REVIEW PLUS FOUR (4) YEARS – 03/2029
BOARD OF REGENTS REPORTING (CHECK ONE): PRESIDENTIAL REPORT

I. POLICY STATEMENT

Passwords are an important aspect of computer security and a critical protection mechanism for securing digital identities and user access. All individuals with Northern Kentucky University (NKU) account credentials are responsible for taking the appropriate steps for protecting system and data access.

The purpose of this policy is to establish secure practices for password management.

A. OVERVIEW

NKU accounts, passwords, and other types of authorization (e.g., NKU keys, access cards) are owned by the University. Account operations such as passwords and alternative authorization are the responsibility of the individual assigned to the account. Credential information is not to be disclosed to non-authorized parties.

B. STANDARD USER ACCOUNTS

Standard accounts are provided to users for basic NKU system and data access and generally applied to all faculty, staff, and students to conduct University business. Standard accounts provide access to core services such as domain computer login, email services, myNKU functionality, and other online services that use the standard NKU domain login credentials.

Standard user account passwords must have the following characteristics:

- Be eight (8) to sixteen (16) characters long
- Contain at least three (3) of the following: uppercase letter, lowercase letter, number, special character (~!@#$%^&*)
- Not contain the user's username or any part of the user's name
- Expire and must be reset on an annual basis and must be actively using NKU-provided multifactor authentication (see the "Multifactor Authentication" section below)
- Not be identical to previous passwords
- Not be transmitted in clear or plain text (e.g., passwords shall not be emailed or transmitted via insecure web authorization)

C. PRIVILEGED USER ACCOUNTS

Privileged accounts are provided to a limited selection of users for access to central servers, networks, and other infrastructure that support the technical systems of the University. Privileged access is assigned based on job duty requirements on a need-to-know basis. Privileged accounts provide access

to data, services, and functionality necessary to operate and maintain the technical systems that support the University. Privileged accounts may be either bound to the NKU domain service or to a local account created on the device.

Privileged user accounts are assigned to individuals and not user-interactive, generic/services accounts shared between system administrator users. For user-interactive shared administrative accounts, see the “Special Accounts” section below.

A privileged user account shall be a separate account from the user’s standard account.

Privileged user account passwords must have the following characteristics:

- Not be the same as the user’s standard account password (when applicable)
- Be eight (8) or more characters, or the maximum allowed length within the system’s limitations
- When possible, contain complex characters (e.g., numbers, special characters)
- Not contain an NKU username or part of the user’s name
- Be unique to the system, not common amongst many systems
- Not be transmitted in clear or plain text (e.g., passwords shall not be emailed or transmitted via insecure web authorization)
- Be periodically evaluated by system administrators for expiration and reset; passwords must expire and be reset annually and must be actively using NKU-provided multifactor authentication (see “Multifactor Authentication” section below).

D. SERVICE ACCOUNTS (NON-INTERACTIVE)

Service accounts are special and provisioned for use only by computers or similar electronic devices, requiring no direct user interaction to access, store, or process data or system functions. Non-interactive service accounts are used by applications or services to interact with the operating system, another application, or service. These accounts are commonly implemented as local system accounts and use local administrator privileges.

Non-interactive service account passwords must have the following characteristics:

- Be eight (8) or more characters, or the maximum allowed length within the system’s limitations
- When possible, contain complex characters (e.g. numbers, special characters)
- Not contain an NKU username or part of a user’s name
- Be unique to the system, not common amongst many systems
- When possible, not be transmitted in clear or plain text (e.g., passwords shall not be emailed or transmitted insecure web authorization)
- Be periodically evaluated by system administrators and information security for potential expiration and reset

E. SPECIAL ACCOUNTS

The following accounts provide unique and specific access, provisioned to meet needs outside of the categories listed above.

GENERIC ACCOUNTS/INTERACTIVE SERVICE ACCOUNTS

Passwords for generic accounts and interactive service accounts must have the following characteristics:

- Be eight (8) or more characters, or the maximum allowed length within the system's limitations
- When possible, contain complex characters (e.g. numbers, special characters)
- Not contain an NKU username or part of a user's name
- When possible, be stored in a password vault or other secured password management system

TEMPORARY/GUEST/TEST ACCOUNT PASSWORDS

Passwords for temporary/guest/test accounts must have the following characteristics:

- Be eight (8) or more characters, or the maximum allowed length within the system's limitations
- When possible, contain complex characters (e.g., numbers, special characters)
- Not contain an NKU username or part of a user's name
- Be unique to the system, not common amongst many systems

NOTE: These accounts are temporary only and must be disabled/deleted when access is no longer needed.

STUDENT WORKER ACCOUNT PASSWORDS

Passwords for student worker accounts must have the following characteristics:

- Not be the same as the user's standard account password (when applicable)
- Be eight (8) or more characters, or the maximum allowed length within the system's limitations
- When possible, contain complex characters (e.g. numbers, special characters)
- Not contain an NKU username or part of the user's name
- Be unique to the system, not common amongst many systems
- Not be transmitted in clear or plain text
- Must utilize NKU's multifactor authentication

NOTE: Student worker account access is assigned based on job duty requirements and the need-to-know principle. When applicable, in a limited scope, student worker access should be a separate account from the user's standard account

F. MULTIFACTOR AUTHENTICATION

NKU provides multifactor authentication services to students, faculty, and staff. Multifactor authentication (MFA) is an additional layer of security applied to a digital identity. When using MFA, additional steps are required during the user login process to validate the user's identity.

MFA-protected accounts will be required to change passwords at annual (365 day) intervals. Unenrollment from MFA is not permissible.

G. PENALTIES

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

H. HANDLING COMPROMISED PASSWORDS

Users suspecting their password has been stolen should take the following actions:

- Change the password immediately.
- Check for malicious account activity, including email and network drives to assess potential impact to University data confidentiality, integrity, and accessibility.
- Contact the NKU Office of Information Technology through the IT Help Desk, client support specialist, or a service request to Information Security if compromised.

NOTE: Attempts to discover and identify accounts that do not meet the password policy requirements may be performed periodically and/or randomly by the NKU IT Security Department. If a compliance issue is found, the responsible party will be required to address the issue in a timely manner.

II. ENTITIES AFFECTED

This policy applies to:

- Anyone using an NKU computer account, or with responsibility for an NKU account that supports or requires a password credential on any system accessing NKU business, research, or academic data—this includes, but is not limited to, faculty, staff, students, vendors, service providers, retirees, graduates, and University guests.
- Service accounts, computer accounts, or similar accounts that are non-user interactive for the purpose of executing computer services, automated processes, or scheduled jobs/tasks.

III. EXCEPTIONS

Exceptions to this policy must be approved by the Chief Information Officer (CIO) and the appropriate Vice President.

IV. REFERENCES AND RELATED MATERIALS

REFERENCES & FORMS

Password Requirements

RELATED POLICIES

Acceptable Use Policy

Account Lifecycle Maintenance Policy

Information Security Policy

REVISION HISTORY

REVISION TYPE	MONTH/YEAR APPROVED
Revision to update for MFA's applicability to students; changed password reset requirements from 90 days to annually because of MFA use; minor editing	March 18, 2025
New Policy	February 15, 2022

PASSWORDS

PRESIDENTIAL APPROVAL

PRESIDENT

Signature Cady Short Thompson *Date* 3·18·2025

Cady Short-Thompson

BOARD OF REGENTS APPROVAL

BOARD OF REGENTS (IF FORWARDED BY PRESIDENT)

☐ This policy was forwarded to the Board of Regents on the ***Presidential Report (information only)***.
Date of Board of Regents meeting at which this policy was reported: _____/_____/_____.

☐ This policy was forwarded to the Board of Regents as a ***Presidential Recommendation (consent agenda/voting item)***.

- ☐ The Board of Regents approved this policy on _____/_____/_____.
  (Attach a copy of Board of Regents meeting minutes showing approval of policy.)
- ☐ The Board of Regents rejected this policy on _____/_____/_____.
  (Attach a copy of Board of Regents meeting minutes showing rejection of policy.)

BOARD OF REGENTS REPORTING

Board of Regents Meeting Date

Board of Regents Materials Page #