UNIVERSITY OF NEBRASKA
UNK™
KEARNEY

Effective: *February 1, 2017*
Last Revised: *November 27, 2017*

Responsible University Office:
Information Technology Services

Responsible University Administrator:
Chief Information Officer

Policy Contact:
Deb Schroeder
schroederd@unk.edu

Password Policy

POLICY CONTENTS

Scope

The policy applies to all employees, temporary employees, retirees, contractors, consultants, and students who are responsible for an account or any form of access that supports or requires a password or PIN on any system that resides at any UNK or NU campus or facility, has access to the UNK network, or stores any non-public UNK information.

Policy Statement

All user-level and system-level passwords must conform to the following:

- Passwords cannot be shared or revealed to anyone, regardless of the circumstances.
- Passwords cannot be written down and stored near computers.
- Passwords cannot be emailed or revealed in other electronic communications.
- Passwords may be stored using a password manager, such as KeePass, LastPass, or Dashlane, as long as the master password meets or exceeds UNK password management criteria.
- Passwords cannot be revealed on questionnaires or forms.

- Default passwords of applications or systems must be changed immediately after installation.
- Initial passwords or reset passwords must conform to UNK password criteria.
- Users are responsible for all activity performed with their usernames and passwords.
- Usernames and passwords may not be utilized by anyone but the individuals to whom they have been issued.
- Users must not allow others to perform any activity with their username and passwords.
- Users must not perform any activity with usernames and passwords belonging to other users.
- The same password should not be used for UNK accounts and for non-UNK access (i.e. personal ISP account, option trading, benefits, etc.). When possible, different passwords should be used for different NU access needs (i.e. TrueYou and EASI.)
- The "Remember Password" feature of applications must be utilized cautiously and only on a device dedicated to an individual's use.
- If an account or password is suspected to have been compromised, the Technology Helpdesk must be notified and all passwords must be changed.

When technically feasible, this password criteria will be implemented in current systems and applications to secure IT resources. As new systems and applications are purchased and/or licensed, password capability should meet this password criteria:

- Each system requires that passwords be changed at least every 90 days.
- Each system requires that all passwords have at least ten (10) characters consisting of a combination of upper and lower case alphabetic characters, numeric digits, and special/punctuation characters.
- Each system checks the length of passwords automatically at the time that users construct or select them.
- After five unsuccessful attempts to enter a password, each system will suspend the involved username until reset by a system administrator.
- The password file maintained by the application should be encrypted.
- At a minimum, the previous ten passwords cannot be reused.

User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

System administrators will utilize two-factor authentication.

VPN access will utilize two-factor authentication.

Systems and application administrators will ensure that vendor supplied accounts are secure. Such account should be enabled only when necessary for vendor access. This applies to operating system and application software.

Requests for single-sign-on using EASI credentials must be evaluated and approved by the UNK Security Team.

Enforcement

This policy is enforced by the Information Technology Services Security Team in coordination with Human Resources (staff) and/or Academic Affairs (Faculty). Failure to comply with this policy may result in disciplinary actions.

Reason for Policy

This policy provides guidance for the proper use of passwords and establishes a standard for creation of strong passwords, the protection of those passwords and the frequency of change.

Definitions

Employee refers to faculty, staff, students, independent contractors and other persons whose conduct in the performance of work at UNK is under the direct control of UNK, whether or not they are paid by UNK.

Network is defined to be all UNK owned or managed internal infrastructure for converged services, including but not limited to, data, video and voice, to facilitate resource sharing and communication.

Two Factor Authentication is a process that requires a user to provide two methods of identification, typically something the user knows, such as a password or code, and something the user possesses, such as a card or a token.

Virtual Private Network (VPN) refers to an encrypted communication link between the campus network and the public Internet. Since all data passing through the communication link is encrypted, it is referred to as being virtually private.

Additional Contacts

Subject	***Contact***	***Phone***	***Email***
Passwords	Andrea Childress		Childressa@unk.edu

Related Information

Guidelines for the Use of Information Technology Resources at the University of Nebraska at Kearney

Responsible Use of University Computers and Information Systems (Executive Memorandum No. 16)

University of Nebraska Password Policy

University of Nebraska Enterprise Password Policy Technical Implementation Guide

University of Nebraska Enterprise Password Policy User Implementation Guide

Guidelines for General Password Construction

Traveling with Electronic Devices

History

Initial Draft – November 3, 2016
Updated November, 2017 – Responsible University Administrator changed from Assistant Vice Chancellor-IT to Chief Information Officer and corrected links to University of Nebraska Password Policy documents in Related Information