# University of Nebraska Password Policy User Implementation Guide

Effective: December 31, 2013

**Purpose:** This policy governs the standards that will be used to define and enforce password requirements for any University systems that use a password-based authentication method. It is constructed within the framework of Executive Memorandum 26, under the direction of the University Information Security Council. It applies to any individual, in any capacity, interacting with University managed information systems to create or access University or Nebraska State College System information assets. It does not apply to the Affiliated Covered Entity Agreement between the University of Nebraska Medical Center and its healthcare partners.

**Policy:** The campus or UNCA Security Information Security offices, in cooperation with the information owners of any affected system, will establish and communicate specific password construction requirements for any password-based authentication systems for which they are responsible. In the case of distributed (federated) authentication systems, those requirements will be established by the individual campus Information Security office, and in the case of enterprise wide authentication systems those requirements will be established by the University-Wide Information Security council.

All password construction requirements will be defined in a manner that provides compliance with the applicable InCommon Level of Assurance (LOA): 1-Bronze, 2-Silver. The required LOA for a given system or user role will be determined by the information owner of that system, in cooperation with their entity Information Security Officer.

The password construction requirements will include definition of required password length, complexity, duration, reusability, number of failed attempts allowed and the lockout period after reaching that number of attempts. The desired combination of password construction factors must yield a level of entropy (complexity)sufficient to meet the minimum requirement for a given InCommon LOA, and be validated by InCommon endorsed tools for calculating password entropy.

It is essential to understand that an acceptable entropy level may be achieved by various combinations of requirements (length, expiration, etc.) and that individual authentication systems may have differing password requirements while still meeting the required InCommon LOA.

**System Administration Responsibilities:**

- Administrators will ensure that vendor supplied accounts are secure and will change any default passwords upon deployment.
- Temporary passwords that are issued to users must be changed on first use.
- The password field in a login panel will be configured to obfuscate the password entered by a user.
- New authentication or information systems must be capable of enforcing this policy.

- Help Desks will establish policies to authoritatively establish the identity of any individual requesting a password reset and will communicate any such information in a secure manner.

**User Responsibilities:**

Users are responsible for all activity performed with their user-IDs and passwords, and must use the following standards to manage their password related activities. Any detected violation of these standards will be forwarded to the appropriate Information Security Officer and their associated Human Resources office for appropriate action.

- Users will create passwords that comply with the structural requirements (length, characters, etc.) enforced by the application or authentication system.
- Passwords should not be based on well-known or easily accessible personal information.
- Users should not keep an unsecured written record of passwords, either on paper or in an electronic file.
- Passwords should be treated as confidential information and as such should not be shared.
- Users must protect against “accidental disclosure” of credentials when working in groups or on teams.
- Passwords should not be transmitted electronically over the unprotected Internet, such as via e-mail, without verified SSL protection.
- Users should not disclose passwords to any other individual, for any reason, with the exception of authorized personnel performing computer maintenance.
- Passwords used to gain access to university systems should not be used as passwords to access non-university accounts or information.
- If an employee either knows or suspects their password has been compromised, it must be reported to the appropriate Information Security Office and the password must be changed immediately.