Password Policy Technical Implementation Guide University of Nebraska

Effective: December 31, 2013

1 Table of Contents

2 Password Construction Procedures

2.1 Overview

All password construction requirements will be defined in a manner that provides compliance with the applicable InCommon Level of Assurance (LOA): 1-Bronze or 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.

2.2 Construction

Passwords should have the correct amount of randomness or entropy in their creation so that they cannot be easily guessed in the event they are lost or stolen. The following guidelines assist in ensuring this.

- Passwords should not be based on well-known or easily accessible personal information.
- Passwords should not be based on a user's personal information or that of his or her friends, family members, or pets. Personal information includes NU I.D., name, birthday, address, phone number, social security number, or any combinations thereof.
- Passwords should contain a combination of uppercase letters (e.g. N), lowercase letters (e.g. t), numbers and special characters.
- Passwords should not be words that can be found in a standard dictionary (English or foreign) or are publicly known slang or jargon.
- The use of so-called "first-character" passwords makes it easy to comply with these guidelines. To do this, compose an easily-remembered sentence (for example, "I have worked here for 2 years") then use the first character of each word to form the password; with adding a symbol for added security, that is "Ih.whf2y$z" [1].

2.3 Protection

- Passwords should be treated as confidential information and as such should not be shared.
- If someone demands your password (except in the cases necessary to facilitate computer maintenance and repairs by authorized personnel), refer them to this policy and have them contact the Information Security Office. Section 5[6] in xecutive Memorandum 16 specifies that this is not allowed.
- Passwords should not be transmitted electronically over the unprotected Internet, such as via e-mail, without verified SSL protection. Each campus Information

Security Plan (if exists) will detail the method for verification. Otherwise the responsible IT office will outline this method.

- You should not keep an unsecured written record of your passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access safe if in hardcopy form or in an encrypted file if in electronic form. Contact your Information Security Office for a recommendation of password vault tools.

- It is recommended that users do not use the "Remember Password" feature of applications.

- Passwords used to gain access to university systems should not be used as passwords to access non-university accounts or information. For example, you should not use the same password for your online banking tool as your university email account.

  In addition you should not use the same password to access multiple authentication stores unless those stores are in a SSO or synchronized environment. Keeping work passwords separated from personal passwords is recommended.

- If an employee either knows or suspects that his/her password has been compromised, it must be reported to the Information Security Office and the password must be changed immediately.

2.4 Tips for choosing a strong password

The length and complexity requirements may appear to make it hard to choose a password that is easy to remember, but it is straightforward to do so. A password that meets the minimum length requirement must be rather complex.

You can readily construct such a password from the initial letters of a favorite quotation, song lyric, poem and so on, capitalizing some letters and substituting a number or special character in an appropriate place. For example, consider the sentence "I have worked here for 2 years" then use the first character of each word to form the password; adding a symbol for additional security, resulting in "Ih.whf2y$z" Other examples of strong passwords are:

- IXdKKAs8pdd — In Xanadu did Kublai Khan A stately pleasure-dome decree

- Iitco@bshf — It is the color of a bleached skull, his flesh

Recommended: A long passphrase can be relatively simpler. Choose three simple words, capitalizing some letters, and link them with a number or special character. For example:

- gorilla8banana@SanDiego

2.4.1 Example Verification Data

The following list (in order of applicability) may be used to verify or proof an individual when they are attempting to recover their password.

- Full Name
- Date of Birth
- Country of origin
- State of residence
- Zip code
- Your alternate e-mail address
- Your IP address (if known)
- Your Internet service provider (if known)
- Last successful signed in date/time (if known)

Examples

These are examples only and each respective Information Security Office or designated office is responsible for identifying further examples and education on the standards for their campus or unit.

2.5 User-chosen Passphrase

15 characters in length requiring upper, lower, non-alpha characters

365 day expiration

10 concurrent failures

60 minute lockout (1 hour)

NIST Level 1 (InCommon Bronze)

User-chosen password
8 characters in length requiring upper, lower, and non-alpha characters
365 day expiration
5 concurrent failures
180 minute lockout (3 hours)

NIST Level 2 (InCommon Silver)

User-chosen password
8 characters in length requiring upper, lower, and non-alpha characters
90 day expiration
3 concurrent failures
420 minute lockout (7 hours)

2.6 Recommendations

- To minimize the window of opportunity for an attacker who has discovered a user's password, users will be forced to change their passwords periodically.
- Users must promptly change any password that is either suspected or known to have been disclosed to unauthorized parties.
- A user's new password (or passphrase) will be completely different from any recently used password (or passphrase).

- A user will be free to choose a new password at anytime, but a user will not perform multiple changes in quick succession in order to enable continued use of a recently used password.
- A user will be prompted to change his or her password in accordance with section 2.2 and/or 2.4 above.
- A user's new password will be different from his or her previous four (4) passwords.

2.7 Recovery Procedures

2.7.1 Self Service Recovery

For added security it is recommended that a two factor approach be employed. This may utilize either security questions or a One-Time-Password (OTP) delivered as a text message or to an alternate email address.

1. The users navigates to the recovery page.
2. The users answers a minimum of three security questions

2.7.2 Alternate Method

1. The user inputs a One-Time-Password (OTP) that was sent to a device or account under their control.

2.7.3 Help Desk Password Recovery

1. User calls in to Help Desk
2. User is proofed/verified using associated assurance level requirements. By asking specific demographic and security questions
3. Help Desk Technician issues a password reset email containing a OTP to be used to reset their account
4. User obtains instructions begin password reset process.

2.7.4 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.

2.7.5 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.

3. Users will create passwords that comply with the structural requirements (length, characters, etc.) enforced by the application or authentication system.
4. Passwords should not be based on well-known or easily accessible personal information.
5. Users should not keep an unsecured written record of your passwords, either on paper or in an electronic file.
6. Passwords should be treated as confidential information and as such should not be shared.
7. Users must protect against "accidental disclosure" of credentials when working in groups or on teams.
8. Passwords should not be transmitted electronically over the unprotected Internet, such as via e-mail, withoutSSL protection valid SSL certificates.
9. Users should not disclose passwords to any other individual, for any reason, with the exception of authorized personnel performing computer maintenance.
10. 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 changed immediately.

3 Entropy

3.1 Entropy, Defined

In cryptanalysis, entropy is a measure of the unpredictability of a key. In this case a user password or credential used to authenticate is the key. By increasing unpredictability (entropy), greater security can be achieved.

3.2 Measuring Password & Credential Entropy

There are various metrics used to measure password/credential strength, including:

- Credential length (8, 10, 15, 20+ characters)
- Available characters (upper, lower, numeric, special characters)
- Expiration (how long before the password must be changed or renewed)

3.2.1 The expiration period can be measured in many different ways.

1. Time-based
    1. Days
    2. Months

        3. Years
    2. Event-based
        1. Number of failed attempts
        2. Frequency of failed password attempts

Credentials should be valid until their unpredictability diminishes beyond acceptable risk. *Requiring passwords to change too frequently can cause other security implications, so caution should be taken when determining the expiration period.*

By adjusting each metric, a password with greater entropy can be achieved.

3.3 Calculators

Entropy calculators can be found on the InCommon Assurance wiki [6]. The calculators assist in measuring against specific government and higher education entropy standards.

4 References

[1] InCommon Identity Assurance Profiles: Bronze & Silver
http://www.incommon.org/docs/assurance/IAP.pdf

[2] NIST 800-63-1 http://csrc.nist.gov/publications/nistpubs/800-63-2/SP-800-63-2.pdf
[3] M-04-04
http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

[4] Entropy Calculators
https://spaces.internet2.edu/display/InCAssurance/Password+Entropy+Calculators

[5] PCI Security Standards Council - https://www.pcisecuritystandards.org/