Policies and Standards

SECTION: Security

CHAPTER: General

POLICY: Strong Password Construction Standard

PURPOSE

This standard establishes the minimum requirements for generating passwords used by operating systems, DBMS, or applications within Creighton University.

Passwords authenticate that a user accessing a system or application is an authorized individual. A consistent, global standard of password requirements is needed to ensure a minimum level of security is maintained across all operating systems and applications in Creighton.

In the future, the move to Single Sign On (SSO) may require a minimum common password standard across systems and applications administered by a single login point. Implementation of this standard will help ensure consistent access controls to the various information systems.

SCOPE

This standard applies to all applications, operating systems, and network operating systems requiring a user ID and password, unless an exception is noted.

STANDARD

Protection of Passwords

Passwords must never be written down or recorded

No Creighton employees or students should ever share or divulge their password to anyone. Each user is accountable and responsible for any action taken with that user's UserID or Username and password. No Creighton employee or administrator should ever ask a user for their password, and even if they do, the user should not reveal it to anyone, no matter how plausible the reason. Any password that is know or suspected to be compromised must be changed immediately.

Password Selections

Users must select passwords that do not contain words generally found in a dictionary. Easy to guess words, such as the university name, product names, the user's name or the user's UserID or Username, must not be used at any time. Strong passwords should include at least three of the four following characteristics:

At least one numeric character
At least one special character (/, [ - , =, +, !, #, $, etc.),
At least one lower case character
At least one upper case character.
## Strong Password Construction Standard

Passwords issued for temporary IDs, password resets, and locked out IDs, must also conform to this standard.

### Password Lengths

Each password must be a minimum of eight (8) characters.

### Password Expiration

All passwords generated within the Creighton system, must be set to expire a **maximum of every 90 days**. Passwords issued for temporary IDs, password resets, and locked out IDs must all be reset to expire immediately. The recipients of temporary passwords will then be forced to change their passwords at their first login opportunity.

### Password Encryption

For security purposes, passwords will not be sent across the network in 'clear text' format. Passwords must also not be listed in clear text for the purpose of automating a login sequence. All passwords must be stored in an encrypted format by the OS, DBMS, or application.

**NOTE**: All encryption methods and technology must comply with any international regulations governing this technology.

### Account Lockouts

An account will be set to 'lock out' a user after a **maximum of 3 bad password or login attempts**.

### Password Uniqueness

Where technically feasible, a history of at least two (2) passwords must be kept within the system for each password generated. This uniqueness forces users to select a password (when generating a new password) that has not been used as the two previous passwords.

### Password Hacking

Workers must not attempt to "break" "hack" "crack" or otherwise determine another users’ password. This applies to passwords for Creighton employees and students, Creighton business associations, and accounts on systems reached through the Internet.

### Password Display and Printing

The display and printing of passwords must be masked suppressed, or otherwise obscured such that unauthorized parties will not be able to observe or subsequently recover them.
Password Retrieval

Computer and communication systems must be designed, tested, and controlled to prevent the retrieval of stored passwords -- whether they appear in encrypted or plain text form. Electronic or automated means must not be used to record and retrieve a password instead of keying it in through a keyboard when logging on or authenticating a user.

Breach of Password Security

All passwords must be promptly changed if they are suspected of being disclosed or known to have been disclosed to unauthorized parties.

RESPONSIBILITIES

Network Users are responsible for creating and maintaining their password in accordance with this standard.

Help Desk is responsible for applying the standard (when establishing password rules on systems and applications) and issuing passwords to users.

Information Security has sole authorization to review all minimum password standards established (within any system using an OS, dB, or Applications) under the scope of this standard. Upon review, Information Security has the authority to distribute a written report identifying non-compliance and then directly overseeing the implementation of the standard on all non-complying systems, DBs, or applications.

ADMINISTRATION AND INTERPRETATIONS

This standard shall be administered by Information Security. Questions regarding this policy should be directed to the Information Security Officer.

AMENDMENT/TERMINATION OF THIS POLICY

The University reserves the right to modify, amend or terminate this standard at any time. This standard does not constitute a contract between the University and its faculty or employees.

REFERENCES TO APPLICABLE STANDARDS

Information Security Philosophy
Information Security Governance Policy
Access Control Policy
User ID Policy
Policies and Standards

SECTION: Security
CHAPTER: General
POLICY: Strong Password Construction Standard

EXCEPTIONS

Requests for an exception to this standard must be submitted via the Policy Exception Request Form. All exception requests will be handled in accordance with the Information Security Exception Policy and Standard.

VIOLATIONS/ENFORCEMENT

Any known violations of this standard should be reported to the University's Information Security Officer at 402-280-2386 or via e-mail to infosec@creighton.edu.

Violations of this standard can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with University procedures.

The University may advise law enforcement agencies when a criminal offense may have been committed.