Policies and Procedures

SECTION: **Administration**	*NO.* **2.4.13.**		
CHAPTER: **Information Technology**	*ISSUED:* 4/7/06	*REV. A* 3/13/13	*REV. B*
POLICY: **Password Management Policy**	*PAGE 1 OF 2*		

PURPOSE

To ensure that passwords are handled in a secure manner and to provide assurance that they are a trusted factor for authentication to access University assets.

SCOPE

This policy applies to all individuals who are granted an electronic identity at Creighton University or systems that store or process electronic identities.

POLICY

Passwords are the minimum factor that can be used for authenticating an individual and tying him or her to an electronic identity for the purpose of accessing information systems at Creighton. As they are often the primary and sole factor in ensuring accurate identity information, they must be treated as Confidential data as outlined in the **Data Classification Policy** and the **Data Handling Policy.** Specifically, passwords:

- MUST be changed at least every 180 days.
- MUST meet the following complexity requirements, when technically possible:
    - Be at least 8 characters in length
    - Contain at least 3 of 4 types of characters
        - Uppercase Latin letters [A-Z]
        - Lowercase Latin letters [a-z]
        - Digits [0-9]
        - Non-alphanumeric printable characters (e.g.: !@#$%^&)
    - MUST NOT contain any significant portion of the username/NetID
    - MUST NOT contain any part of an individual's first or last name.
- MUST not be shared with any individual at any time for any purpose.
    - The only exception is one time use passwords or passwords with a limited lifetime for the purposes of activating or establishing an account.
- MUST NOT be written down or stored in any manner that would allow them to be viewed by other individuals.

DEFINITIONS

System Administrator - An individual responsible for maintaining an information technology system.

System User - An individual who has been granted an account to access any Creighton system.

SECTION: **Administration**	*NO.* **2.4.13.**		
CHAPTER: **Information Technology**	*ISSUED:* 4/7/06	*REV. A* 3/13/13	*REV. B*
POLICY: **Password Management Policy**	*PAGE 2 OF 2*		

RESPONSIBILITIES

System Administrators are responsible for ensuring, where possible, that password parameters on systems they administer meet a minimum level of complexity, length, and age.

System Users are responsible for safeguarding their passwords.

Information Security Office is responsible for validating that all systems adhere to this policy.

ADMINISTRATION AND INTERPRETATIONS

This policy 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 policy at any time. This policy does not constitute a contract between the University and its faculty or employees.

REFERENCES TO APPLICABLE POLICIES

Classification Policy
Data Handling Policy

EXCEPTIONS

Exceptions to this policy must be approved by the Information Security Office.

VIOLATIONS/ENFORCEMENT

Any known violations of this policy 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 policy 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.