Policies and Standards

SECTION: Security
CHAPTER: General

PURPOSE

This document describes the Creighton University policy on user identification (user ID).

Due to the nature of the information contained within Creighton's applications, it is essential to have user IDs associated with an individual and not shared among users. The capabilities within applications and systems have become robust enough to allow us to track user activity. Without unique user IDs, logs cannot be used to definitively indicate the activities of a particular user. Unique user IDs allow for better administration of access control as well. The amount of information contained within our applications requires that access rights be tailored to a user's requirements. Unique user IDs places the responsibility on the individual user as well. Since the individual should be the only person using that logon, they are held accountable for all activity performed as that user ID. This responsibility requires that all users keep their user ID and password confidential and protect their computer from use by an unauthorized user.

SCOPE

This policy applies to all members of the Creighton University community (staff, faculty, students, contractors, consultants, temporaries, visitors, etc.) while using Creighton's computing or networking resources. All users are expected to be familiar with and comply with this policy.

POLICY

All users will be assigned a unique user identification (user ID).

DEFINITIONS

None.

RESPONSIBILITIES

**Authorized Account Creators** are responsible for communicating the User ID Policy to anyone requesting a generic user ID. If the requestor deems it necessary to appeal for an exception, the account requestor is responsible for escalating the appeal to the Information Security Officer. If the appeal is granted, the account creator is responsible for creating generic user IDs that meet or exceed the security requirements stated in this policy.

**Information Security** is responsible for maintaining and enforcing the policy.

Information Security has the authorization to review all generic user IDs being requested (within any system using an OS, DB or Application) within the scope of 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/TERRMINATION 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 STANDARDS

- Information Security Philosophy
- Information Security Governance Policy
- Authentication Standard
- Information Security Exception Policy

EXCEPTIONS

Requests for an exception to this Policy 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 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.