Policies and Standards

SECTION: Security

CHAPTER: General

POLICY: Authentication Standard

PURPOSE

This standard outlines the acceptable means of implementing authentication into applications and/or websites at Creighton. It includes the type of authentication to be used. This standard is in support of the Access Control Policy.

SCOPE

This standard applies to all applications and websites that are connected to Creighton’s network or that control access to Creighton proprietary, patient, student, supplier or employee information.

STANDARD

The following common authentication solutions are approved for use whenever user authentication is required under the Access Control Policy.

- Application ID/Password Authentication - for internal client/server applications
- Active Directory - for internal or external client/server applications
- NT Authentication - for internal client/server applications
- X.509v3 user certificates - for internal or external applications to authenticate internal Creighton users (NOTE: full support of x.509-enabled applications is not yet in place.)
- Novell Directory Service - for internal or external client/server applications

The solutions listed above may not be available for all applications. Any other means of authenticating users must be approved by the Information Security Officer. The level of authentication required will be directly related to the sensitivity of the information contained within the application. In the case of systems that contain Creighton CONFIDENTIAL data or sensitive, personal data, there may be additional layers of authentication required.

DEFINITIONS

**Authentication**
Verification that the presenter of user credentials is the individual to which the credentials are assigned. ("Proof that they are who they say the are")

**Authorization**
Verification that the authenticated user has privileges to complete the task requested. ("Rights to do what they are trying to do")

**Public Application**
An application or website that does not present user-specific information to the end user.

**Non-Public Application or Site**
An application or website that presents user-specific information to the end user, such as patient information.

RESPONSIBILITIES

**Systems Administrators** are responsible for carrying out the activities associated with the compliance of this standard for the applications under their control. Such compliance includes implementing authentication that meets or exceeds the requirements in this standard.

**Information Security Office** is responsible to review all authentication controls established under the scope of this standard. Upon review, Information Security has the authority to overseeing the implementation of the standard on all non-complying systems.

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

EXCEPTIONS

Requests for an exception to this standard must be submitted via the [Policy Exception Request Form](mailto:infosec@creighton.edu). 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](mailto: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.