Identity and Accounts Policy

Identity and Accounts Policy

Effective Date:

Revised:

Status:

_X_  Draft
__  Under Review
__  Approved
__  Obsolete

Responsible University Officer:

Vice President, Information Services, CIO

Responsible Coordinating Office:

Office of Information Services

Version 1.0

REVISION HISTORY

November 22, 2013 - Initial draft

OVERVIEW

Cardinal Stritch University requires that all individuals who are accessing protected or private information or University systems and resources provide a unique username and password which has been assigned to that individual and which will act as their electronic identity.

PURPOSE

The purpose of this policy is to establish a unique, traceable electronic identity for every individual using Cardinal Stritch University electronic resources to ensure that access to information can be limited to only those who need access and to ensure that the individual accessing the resources is the intended party.

SCOPE

This policy applies to all individuals who use, access or control University electronic resources. This includes but is not limited to students, faculty, staff, contractors, vendors, guests, visitors and any other user who uses University owned or controlled electronic resources.

POLICY
Identity and Accounts Policy

Wherever possible, all access to electronic systems, information or resources will be authenticated against the University Active Directory database. Accounts for all students, faculty, staff, vendors and visitors are created utilizing an automated process which pulls data from our SIS/ERP system, Jenzabar EX, based on a set of rules defined around the relationship that the individual has with the University. This includes but is not limited to: creating accounts for students only after they have been accepted to the University; creating accounts for employees only after they have been fully hired by the University; creating accounts for vendors as employees only if they have a specific need for access and then only during the time that they are actively working on University business.

Active Directory accounts are tied back to the individual by their SIS/ERP ID number, are unique to the individual, and after initial setup only the individual has access to their password.

When it is not possible to directly tie authentication back to Active Directory, an intermediary system such as ADFS utilizing SAML, custom SAML code, AD LDS or other systems may be used. When this occurs, every effort must be made to tie the account back to a specific individual.

All University owned, controlled, operated, rented, leased or otherwise engaged systems which a student uses to submit course work or which represent the student in any academic endeavor in relation to the University must have an account which ties back to the student using either their SIS ID number or their Active Directory login.