



## Single Sign-On Policy

---



## Single Sign-On Policy

Version 2

02/24/2020



## Single Sign-On Policy

---

### 1. Overview:

- 1.1. Single Sign-On (SSO) technology allows for the reduction in the number of passwords required by users in order to conduct business on university systems across multiple platforms without having multiple username/password combinations. These systems make use of multiple or robust means of authenticating a user and granting access to university systems based on that one-time authentication.

### 2. Purpose:

- 2.1. The purpose of this policy is to establish minimum standards of administration and operation of a Single Sign-On system for accessing university information systems.

### 3. Scope:

- 3.1. The scope of this policy covers university information systems except as designated by the Chief Information Officer as critical to maintaining or securing vital university assets and designated sensitive information.

### 4. Policy:

- 4.1. The University of Dallas implements Single Sign-On capability in order to:
  - 4.1.1. Simplify user access to university systems;  
and,
  - 4.1.2. Ensure strong protections for designated sensitive information and assets.
- 4.2. This is achieved through the use of the university's approved system solution, Ethos Identity – also known as "MyUD".
  - 4.2.1. Network Requirements:
    - 4.2.1.1. Network connections are established on the campus network or remotely via VPN.
  - 4.2.2. Software Requirements:
    - 4.2.2.1. As part of the SSO operation, user credentials are maintained via Microsoft Active Directory.
  - 4.2.3. SSO Server Access Requirements:
    - 4.2.3.1. Automatic computer lockout is to occur after not more than ten minutes of inactivity, with re-entry to the system requiring only the user password that initiated the session.
  - 4.2.4. SSO Administration:
    - 4.2.4.1. Managers and administrators of the SSO system are appointed by the head of information technology with internal documentation detailing data ownership and administrators.
    - 4.2.4.2. Access credentials to SSO expire automatically with the expiration of the Active Directory password.



## Single Sign-On Policy

---

- 4.2.4.3. System administrators reserve the right to revoke access(es) if an individual poses a risk to the secure operation of SSO.

## 5. Related Standards, Policies and Processes

- 5.1.1. University of Dallas Virtual Private Network (VPN) Policy

## 6. Definitions:

Definitions of terms used in this policy can be found in the SANS Glossary located at: <https://www.sans.org/security-resources/glossary-of-terms/>



## Single Sign-On Policy

---

### 7. Revision History

Date of Revision	Responsible	Summary of Change
2/2/2020	UD Policy Team	Updated and converted to new format
2/24/2020	Blake Palmer	Updated phrasing and policy guidelines