



<b>Multi-Factor Authentication Policy (MFA)</b>		<i>Department:</i> <b>Information Technology Services</b>	
		<i>APP No.</i>	
<i>Department Vice President:</i> <b>Vice President for Finance &amp; Administration/CFO</b>	<i>Revised:</i>	<i>Original Effective Date:</i> November, 2020	<b>Page 1</b>
<i>Subject:</i> The Linfield University Multi-Factor Authentication Policy defines the requirements for users to ensure an extra layer of security when connecting to hardware, software or University network systems.		<i>Applicable Divisions:</i> <b>All</b>	

## **PURPOSE**

The purpose of this policy is to define when the additional security provided by multi-factor authentication will be required to access Linfield University systems.

## **SCOPE**

This policy applies to all users who access restricted or confidential data (or the systems that contain this data) outlined in the Data Classification Policy maintained by the Data Governance Team.

This policy applies to both on-campus and off-campus access to university resources whether the access is through university-owned or personally owned devices.

This policy applies to any system that contains confidential or restricted data or that requires an additional layer of protection as determined by the Chief Information Office or designated Information Security Officer in collaboration with university Data Stewards. Since Microsoft 365 services may hold restricted data these systems will be part of MFA.

## **DEFINITIONS**

- User

Any person or entity accessing, logging into, or attempting to access or log into, a University hardware or software system; or connecting to, or attempting to connect to or traverse a University network, whether by hardware or software or both, from any location. The term "User" includes faculty, staff, students, visitors, vendors, contractors, service providers, automated software programs/agents (and their developers), and any other individuals or agents who access and use University information technology.

- Data Governance Team

Members of the Data Governance Team collaborate to manage data as a Linfield resource to be used to support student success and advance Linfield's mission. The team will set standards and clarify or create policies and practices around data ownership, data quality, data security, and data access and availability. The team is largely made up of data stewards.

- Data Steward

Data stewards are University officials having direct operational-level responsibility for information management - usually department directors. Data stewards are responsible for data access and policy implementation issues. Procedures for performing data validation should be developed and implemented by data stewards in responsible departments.

- Multi-Factor Authentication (MFA)

MFA is an extra layer of security for your Linfield accounts designed to ensure that you are the only person who can access your account, even if someone knows your password.

- Microsoft 365

Microsoft 365 is a suite of cloud-based solutions that includes Outlook email, SharePoint, and Teams.

## **POLICY**

All users who have access to confidential and/or restricted data will be required to use Multi-Factor Authentication on their Linfield University system accounts.

- User Requirement

Users will be required to enroll a device to serve as the second authentication method as part of multi-factor authentication. This second device can be an office phone, cell phone, or supported authenticator app. Multiple authentication methods can be added to a single account.

- Users will set a default sign-in method from the methods added to their account.
- Users must contact Information Technology Services to report suspicious activity or a compromised account.

- Personal Cell Phone Usage

Linfield University will not require the use of a personal cell phone for multi-factor authentication. It is a user's choice if they wish to enroll a personal device as a method for multi-factor authentication.

## **EXCEPTIONS**

Any exceptions to this policy must be approved by the Chief Information Officer.

## **RELATED POLICIES**

- [Acceptable Use Policy](#)
- [Catnet Account Policy](#)
- [Information Security Awareness Policy](#)
- [Data Classification Policy](#)
- [Additional ITS Policies](#)

## **PERIODIC REVIEW and RECERTIFICATION**

Due to the rapid change in technology and increase in cyber security threats all exemptions will be reviewed periodically at the discretion of Chief Information Office in collaboration with the Data Governance Team and Data Stewards.

## **POLICY COMPLIANCE**

When a user is found to be in violation of this policy, access to University-owned information technology resources may be revoked and the University's disciplinary process will be followed as outlined in the personnel handbooks. If the matter involves illegal action, law enforcement agencies may also become involved, as would occur for matters that do not involve information technologies or the Internet.

Date Issued: November, 2020

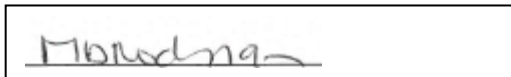
Date Last Revised:

Responsible Executive:

Vice President for Finance and Administration

Responsible Office:

CIO/Information Technology Services



Vice President, Finance and Administration

Date: November, 2020

This policy is effective immediately and supersedes all previous editions.