LUTHER COLLEGE

POLICIES AND PROCEDURES

Department:	Information Technology Services
Subject:	Mobile Device Policy
Date Issued:	April 20, 2023
Updated and Reviewed By:	Information Security Council - April 20, 2023
Approved By:	Reviewed by Cabinet, Approved by President, September 13, 2023

I. Policy

This document outlines the policy for secure usage of mobile devices that have access to Luther College data, systems, and services.

II. Purpose

The purpose of this policy is to define procedures and guidelines for end users who use a personally-owned or Luther-owned mobile device to access Luther College data, systems, and services.

III. Scope

This policy applies to all faculty, staff, volunteers, contracted workers, and student employees who use personally-owned or Luther-owned mobile devices to access Luther College data, systems, and services.

IV. Terms and Definitions

A. Mobile Device - A mobile device is a computer small enough to hold and operate in the hand. Examples include smartphones, tablets, and E-readers.

B. Encryption - Process for transforming information to make it unreadable to anyone except those possessing appropriate credentials for access, in accordance with NIST standards.

C. Secure Wireless Network - A wireless network that secures data transmission between a mobile device and the internet connection point with a password and a secure encryption method.

V. Procedures and Guidelines

A. Support

1. Information Technology Services (ITS) will provide limited technical support on personally-owned mobile devices to all faculty, staff, volunteers, contracted workers, and student employees. Access to this support is available by contacting the Technology Help Desk.

2. ITS will provide technical support on Luther-owned mobile devices to all faculty, staff, volunteers, contracted workers, and student employees. Access to this support is available by contacting the Technology Help Desk.

B. Security Requirements
   1. Login access to mobile devices must be protected with a password, PIN, pattern, or biometric scan.
   2. The automatic locking feature on mobile devices must be set to lock, preferably after one minute of inactivity.

C. Security Recommendations
   1. Missing or stolen mobile devices that have been used to access Luther data, systems and services should be reported to the Technology Help Desk immediately and users should change their Norse Key password.
   2. Operating system updates should be applied to mobile devices in a timely manner. Devices that are no longer supported by their manufacturer should not be used to access Luther College data, systems, and services.
   3. Encryption should be enabled on mobile devices. Enabling a password, PIN, pattern, or biometric scan to access a device will automatically enable encryption on the vast majority of mobile devices. If a device does not support encryption, it should not be used to access Luther College data, systems, and services.
   4. Consider enabling location services and remote "find my device" in order to assist with locating, locking, or erasing a missing or stolen mobile device.
   5. Whenever possible, Luther College data, systems, and services should be accessed via a secured wireless network or your cellular data connection.
   6. Additional Safe Computing recommendations are available at www.luther.edu/offices/its/help-desk/guides/safecomputing.

D. Enforcement

   Failure to comply with the requirements of this policy may result in loss of access to systems and services.