

# Messiah College Data Protection Procedures

## I. Purpose

The purpose of this procedures document is to notify the Messiah Community about the appropriate processes for handling sensitive college data. Sensitive college data is defined as data that must be protected because its unauthorized disclosure, alteration, loss or destruction may cause damage to the college or one of its entities. Data in electronic or paper formats can be stored and handled in a variety of ways. This policy will articulate the standards expected of all college employees when handling sensitive college data. This policy is to be used in reference to the Data Security Policy. This policy is also part of the Messiah College IT Security Plan.


## II. Procedure

### A. Securing your workstation

Users must do the following:

1. Lock the door where your PC is located (if available), whenever room is unoccupied.
2. Setup a screen saver to require a password on resume.

Users are expected to do one of the following:

1. Lock the PC, by holding down the Windows key  + L
2. Logoff the PC, by going to the Start Menu, then clicking “Shut Down” then selecting “Log off” and clicking “OK”.

### B. Securing Data

ITS will identify mechanisms that can be used to encrypt sensitive data. All employees who handle sensitive data are required to use the prescribed encryption method to protect the college’s data assets.

1. Digital (Electronic) Data
  - a. Any data downloaded or exported to a college-owned computer from college systems (i.e. Banner spreadsheets, Discoverer reports, Grade Book Manager and other academic data, etc.) must be saved to the encrypted folder on your computer (specified folder location will go here).
  - b. If data needs to be transported off campus, users must have the data in an encrypted state before copying to external media (i.e. Flash Drive, CD, External Hard Drive, etc).
  - c. No sensitive college data will be stored on a non-college owned machine.
2. Printed Data

- a. Any printed copies that contain sensitive data must be protected. Printed copies of sensitive data can not be left in plain sight on desks or shelves.
- b. Filing cabinets containing sensitive data are required to be closed and locked when not in use.
- c. Lock doors in rooms that contain filing cabinets or document storage areas (if available), whenever room is unoccupied.