Policy Title: Employee Computer Data Protection / Screen Locking (Protecting Student Data)

**Purpose:**
The purpose of this document is to set a minimum standard for protecting data on college-owned computers with password protected screen savers. The screen saver locks the desktop after a set amount of time with no activity. By requiring a user to sign in when they return, it minimizes the risk of an unauthorized person using an active session while the authorized user is away. A password-enabled screen saver helps to protect the information displayed on your screen, stored on your computer’s hard drive, and other data that is accessible from your computer when you walk away from the computer.

**Definitions:**
None

**Policy:**
All College-owned computers should be configured to have a password-enabled screen saver. This data security feature should automatically initiate after the computer remains idle from user interaction after a predefined time period. The user must then re-enter their password to gain access to the computer. The general best practice for enabling automatic lockout of a screen saver is to set the timeout so that it can provide adequate security.

The policy requires that all employees manually lock their computer when not in use, or exiting the room, leaving their computer behind, and that all computers have a screen saver lock out set at 30 minutes. After 30 minutes of no activity, the screen saver will be invoked automatically, with a one-minute delay before actually locking. If no activity occurs, a password will be required before any activity can resume. No transparent screensavers are allowed.

The screen saver lockout is not a replacement for manually locking your machine to ensure its security.

**Associated Policies:**
M State Acceptable Use of Computers and Information Technology Resources Policy
M State Student Directory Data Policy
Family Educational Rights and Privacy Act (FERPA)
Minnesota Government Data Practices Act (MGDPA), Chapter 13 of Minnesota Statutes
Minnesota State System Board Policy 1.C.2-Fraudulent and Other Dishonest Acts

**Associated Procedures:**
M State Employee Computer Data Protection/Screen Locking Procedure
Policy History:
Policy Owner: Chief Information Officer
Policy Author: Dan Knudson
Date of Adoption: 4/21/2017
Date of Implementation: 4/21/2017
Date and Subject of Revision: 4.21.17 newly written policy;

Policy Group Assignment: Technology

Procedure Written: New/Draft