Minnesota State Community and Technical College
Institutional Procedure

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

Policy Purpose Statement:

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:

Click here to enter Procedure associated Definitions. If there are none, enter "None".

Procedure:

Part 1. Responsibilities:

Information Technology Department Employees (IT):

a. Implement a domain wide policy to enforce the standard. This sets the standard globally on the network for everyone.
b. Provide support for machines that do not get the screen locking standard automatically enforced. (example: Mac machines)
c. Identify and review exception requests.
d. Leadership: Supervisors
    1. Support the concept of a screen locking standard.
    2. Advise of and follow the exception policy when needed.

All Faculty and Staff:

a. Follow this policy, making sure that your screen lock is enabled and functioning.
b. Always lock your computer manually if you intend to be away from it when it is on and logged in. Make this a habit. (Manual locking instructions are below)
c. Always ensure that the data on your devices is kept safe and backed up.

Part 2. Standards

A domain wide standard screen lock of 30 minutes.

Exceptions:

Digital signage, lab & library systems, and kiosk systems. (These systems must remain unlocked for viewing and contain no important or private data)

The lock out time for machines that contain highly sensitive information and or in high traffic areas should be evaluated as some situations may warrant a lock out time that is well below the 30-minute standard.

Other exceptions are very rarely granted as screen locking timeouts are a standard security measure. Perceived inconvenience is not sufficient grounds for removal. M State is able to exempt computers from the timeout policy only in circumstances where: physical security for the space in which the computer is located is of such high quality as to make access by unauthorized users effectively impossible; or application of the timeout policy to the particular computer is materially detrimental to work activities and makes work processes effectively impossible.

Exceptions can be requested by creating a screen locking exemption ticket in the Computer Help Center ticketing system.

Part 3. Frequently Asked Questions

a. How will IT centrally apply a screensaver time out to workstation?
   A: IT will apply a centralized group policy via active directory where all domain joined workstations screensaver timeout is changed to 30 minutes. Once the screensaver is activated, there is a one-minute delay before locking, and a password will be required before activity resumes.
b. Will Classroom instructor PCs have the policy enforced also?
   A: Yes. The operating systems for these machines receive a different configuration that is maintained by the Information Technology Department, but also require the locking feature to be enabled.
c. How can I stop my screen from locking in the classroom or during presentations?
   A: There are remote devices and software/mobile apps that can allow you to control your mouse/keyboard from anywhere in the room. Proximity devices could also be used. Please contact your local Computer Help Center for information on what might be available.
d. If I have a machine that has an operating system other than windows or is not connected to the domain, is the screen lockout standard still required?
   A: Yes. Machines that are not connected to the domain are still bound by the standard and must have the screen saver lock enabled and set to lock automatically. For instructions on how to set the screen saver lockout please see instructions below. (Part 3. Instructions)

Part 4. How to Enable the Data Protection Locking Screen Saver?

Windows 7

a. From the Start menu, select Control Panel. In the "Control Panel" window, select Appearance and Personalization and then select Change screen saver (under "Personalization").
b. In the Wait box, choose 30 minutes.
c. Check the On resume, display logon screen check box and then click OK.

Windows Vista & Windows XP

a. From the Start menu, select Control Panel. In the "Control Panel" window, select Display and then select Screen Saver.
b. In the Wait box, choose 30 minutes.
c. Check the On resume, password protect check box and then click OK.

Mac OS X

a. From the Apple menu, choose System Preferences.
b. Click Desktop & Screen Saver.
c. Click Screen Saver, and then use the slider to choose 10 minutes.
d. Optionally, set up a hot corner to let you invoke the screen saver manually:
    1. Click the Hot Corners button
    2. Click the list next to the corner of the screen you want to use as a hot corner and select "Start Screen Saver," and then click OK.
e. Click Show All to go back to the main "System Preferences" window.
f. Click Security, and then click “Require password” to wake this computer from sleep or screen saver.
g. Close the "System Preferences" window.

Manually Invoking the Screen Saver to Lock Computer

On Windows, you can manually invoke the screen saver (thereby locking your computer) any time you leave your work area by pressing the Windows logo key (near the space bar) and typing 'L'. You can also press the Ctrl-Alt-Del keys at the same time and choose to “Lock this Computer”.

On the Mac, you can invoke the screen saver manually by moving the mouse to the hot corner you set up for that purpose (see instructions above).

Associated M State Policy:

M State Employee Computer Data Protection/Screen Locking Policy

---

Procedure History:

Procedure Author: Dan Knudson

Date of Implementation: 4/21/2017

Date and Subject of Revision: 4.21.17 newly written;