This paper provides explanation and guidelines for the mandatory password protected screensaver to each University-owned computer in the College of LSA. On computer systems, Password Protected Screen Savers serve as a necessary security measure especially for systems for which physical security is not limited or those systems that are mobile (including laptops, iPads, smartphones, etc). While full disk encryption protects the data on the system while powered off, password protected screensavers prevent access to the system in the event of it being lost while powered on and/or the user is logged on.
General Information

Many UM College of LSA students, faculty and staff are provided a computer to carry out daily tasks and a network password to protect access to UM/LSA information. Paramount to all usage is the need to keep information, especially sensitive information secure. Only the employee who has been assigned a password should have use and knowledge of that password. It may be helpful at this point to remind the reader that the practice of sharing a password with a coworker or student is prohibited due to the accountability associated with the account/password. To further protect the employee, the integrity of the system and the security of any sensitive data, LSAIT has initiated the use of the mandatory password protected screen savers.

In response to questions and comments relating to the automatic password protected screen saver policy, the University Audit report on Research computing in LSA states:

“Physical Security Discussion: The easiest way to create a problem with a computer is to have physical access to it. Having physical access removes all of the challenges of connecting to a system through the network. It also eliminates any protections provided by network controls. The level of physical security over research systems reviewed varied widely. Some departments cited policies requiring staff to lock office doors when they left to prevent physical tampering. Some departments stated no such requirements. Many departments stated that some of their systems were housed in various data centers, and were therefore assumed to be secure.

Control Recommendation: Each department should decide what physical security is appropriate for their research computers and the data they store. Departmental IT should also review the security policies and practices for the data centers that house their research servers. In each instance, physical access to hardware containing research data should be restricted as much as possible while still allowing appropriate use.”

In evaluating this specific recommendation, LSA determined that to improve the physical security of our computer systems, a password protected screensaver is necessary. Furthermore, this policy specifies that, for inactive computers, the computer must be automatically locked to prevent access to the computer after 15 minutes of inactivity. The Screensaver must be configured so that only entry of the current user’s password will unlock the computer.

Since the computer resources at U of M have significant value (and not just within the research community here) and our students and the citizens of Michigan expect us to be good stewards of these resources, we strive to take all reasonable precautions to protect them. The University's security guidelines call for you to lock the workstation whenever it will be left unattended. Consider the 15 minute screen saver and password requirement to be a safety-net to help prevent inappropriate access to your account and the files/data you are permitted to use.

We recognize that the auto-lock feature introduces a certain level of inconvenience as we interact with computing resources on a daily basis. It is hard to make a case that the additional time to type a few keystrokes is an unreasonable burden. However, U of M has a very clear policy in this regard. Under
the Log-in Process section of the Information Security Standards on the SecureUM website it states: "It is expected that any user of one of these devices will activate a screen lock prior to leaving the computer unattended"

Furthermore, a best practice policy has been established by the LSA.Security group here on campus that recommends that the system be forced to lock after a given time of inactivity and states: "default is 15 minutes, but it is advisable to set it less than 15 minutes". This includes University-owned cell phones, smart phone or iPads as well. These hand held devices should be configured with an access code (PIN#) so that if the device is lost or stolen, the owner’s account and data is inaccessible to unauthorized persons.

In addition, there are energy saving benefits to using a locked screen saver with power management parameters in place. The University's recommendations for these parameters can be found here on the UM Climate Saver website (or go to www.climatesavers.umich.edu).

It is prudent that we therefore continue the implementation of the 15-minute automatic password-protected screen saver mechanism if we are to be in compliance with U of M security standards recommendations, and best practices. LSAIT initially set this policy on Windows systems in 2001, – see #29:

http://webapps-stage.lsa.umich.edu/lsait/admin/implemented.asp

Guidelines

The LSAIT Systems team established a procedure in their automated Windows installation that configures all LSA computers and most applications to lock after fifteen minutes of inactivity. This step is necessary to protect the critical integrity of the operating system, application programs, and data files. ITS/MAIS have implemented similar lockout configurations on Human Resources applications such as PeopleSoft, and Wolverine Access, as these applications must operate as expected and the data they use must be complete, correct and secure. Otherwise, users lose productivity and may report false information – identity theft and fraud crimes, even stolen research can result from unsecured computers. The guidelines for maintaining the integrity of the system are as follows:

A. Password. Passwords are used to maintain privacy and to secure sensitive information. Passwords may consist of letters, numbers, and other characters and must be changed every 450 days. The user is prompted by the computer when it is necessary to change the password. UM Password Policy - http://www.itcs.umich.edu/itcsdocs/r1162/

B. Screen Saver. A password protected screen saver is automatically activated after fifteen minutes of inactivity which locks the user’s computer workstation.
C. Login. The user must login to the Local computer, the UM kerberos or Active Directory domain with his or her network password to unlock the computer workstation thus disabling the password protected screen saver.

D. Application Programs. The University’s Human Resource applications, PeopleSoft, and Wolverine Access have built-in timeout features that will log out the user after fifteen minutes of inactivity in these applications, even though the user may be working in other applications on his or her computer. Any unsaved data will be lost.

All computers at the College of LSA should be configured such that a password protected screen saver locks the computer screen after 15 minutes or less of idle time. A password protected screen saver has been set on LSAIT maintained Windows computers before June 20, 2007. LSAIT will begin enforcing this on supported PCs running Windows Operating Systems on January 1, 2011. The Red Hat Linux deployments in LSA also configure the screensaver by default. People that administer their own computers (especially laptops) are expected to comply with these guidelines. Some useful examples are listed below: This default setting should not be reconfigured unless properly vetted.

Platform specific examples

A. Windows XP
   1. Screensaver Configuration
      a. Open Display in Control Panel (or right-click on the Desktop and select Properties…)
      b. On the Screen Saver tab under Screen Saver, select a screen saver
      c. Select the On resume, password protect check box and the time to 15 minutes or less. (If Fast User Switching is turned on, select the On resume, display Welcome screen check box. Fast User Switching is not allowed if the computer is a member of a domain.)
   2. Locking the screen manually
      a. Hold down the Windows key (has the Windows logo on it) and press “L” for lockscreen.

B. Windows Vista and Windows 7
   1. Screensaver Configuration
      a. Right click on the Desktop and select Personalize
      b. Click on Screen Saver
      c. Select a screen saver from the pull-down menu
      d. Some screensavers have additional options which can be configured using the Settings… button.
      e. Configure the wait time to be 15 minutes or less and check the box On resume, display logon screen. (Note: Computers that are members of the Active Directory domain will have the wait time automatically set to 15 minutes)
      f. For additional power saving features click on Change power settings
   2. Locking the screen manually
      a. Hold down the Windows key (has the Windows logo on it) and press “L” for lockscreen.
C. Mac OS X
   1. Screensaver Configuration
      a. Open System Preferences either by clicking on the dock icon or selecting System
      b. Preferences from the Apple menu
      c. Select Desktop & Screensaver
      d. Click on the Screen Saver button and select a screensaver, or check Use random screensaver
      e. Set the Start screen saver: timer to 15 minutes or less
      f. Some screen savers have additional options that can be configured using the Options button
   2. Locking the screen manually
      a. Open a Finder window and navigate to Applications -> Keychain Access
      b. Double click on Keychain Access to run the application
      c. On the Mac’s menu bar select Preferences...
      d. On the General tab, check the box Show Status in Menu Bar and close Keychain Access
      e. A lock icon is now on the right side of the Mac's Menu Bar.
      f. To manually lock the desktop, click the lock icon and select Lock Screen

D. RedHat Linux (Gnome Desktop)
   1. Screensaver Configuration
      a. From the menu bar select System, Administration and Screensaver.
      b. This will open a new window from which you can select a screen saver.
      c. Check the box that says to require a password to unlock the screen saver and set the time to 15 minutes or less.
   2. Locking the screen manually
      a. In the menu bar select System and Lock System.

Possible Exceptions
Digital signage and kiosk systems.

Questions Regarding this Document
May be referred to the IT Security Manager for LSA;
Christopher Brenner (cbrenner@umich.edu) 734-647-8213
Email: LSA.Security@umich.edu
LSA.Security’s web site: http://www.lsa.umich.edu/lsait/lsasec-itam/security