

This Guideline is provided to assist system administrators and end-users to configure networked devices to comply with the Minimum Security for Networked Devices Standard (IS-S701). The Guideline includes clarifying information about the Standard and configuration details for many situations. It does not include step-by-step instructions for every existing device or operating system, but does provide the information necessary for the majority of Windows, Macintosh, and Linux/UNIX operating systems. The absence of details in this Guideline on any particular environment does not exempt a device from compliance with the Standard.

If your networked device is professionally managed by information technology support staff members, please consult with them before making any changes based on information in this document.

The numbered headings below match those in the Standards.

1. Operating system and software patch updates

Software Patch Guideline

<http://security.arizona.edu/files/ISG704.pdf>

Microsoft Operating System

- Office of Student Computing Resources (OSCR) Guide to Configuring Automatic Updates in Microsoft Windows
http://www.oscr.arizona.edu/security_intro%23patches
- How to Set Up Microsoft Auto Updates
<http://www.microsoft.com/protect/computer/updates/automatic.msp>
- UA Computer Science Guide for Patch Installation for Windows
<http://www.cs.arizona.edu/computing/help/winpatch.html>

Updating a Linux/UNIX Operating System

- FreeBSD
http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/cutting-edge.html
- Red Hat Linux
<http://www.redhat.com/apps/support/errata/>

- Debian GNU/Linux
<http://www.debian.org/security/>
- Solaris
<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

Macintosh Operating System

- Updating the Macintosh Operating System
http://www.xvsexp.com/system/os_updates.php

2. Anti-virus software

Anti-Virus Software Guideline

<http://security.arizona.edu/files/ISG702.pdf>

OSCR's Guide to Installing and Configuring Sophos Anti-Virus

http://www.oscr.arizona.edu/security_intro%23antivirus

3. Anti-spyware software

Spyware & Adware Prevention Guideline

<http://security.arizona.edu/files/ISG705.pdf>

OSCR's Guide to Installing and Using Spybot Search & Destroy and AdAware

http://www.oscr.arizona.edu/security_intro%23spyware

4. Host-based firewall software

Firewall Software Guideline

<http://security.arizona.edu/files/ISG703.pdf>

OSCR's Guide to Enabling the Windows Firewall

http://www.oscr.arizona.edu/security_intro%23firewall

5. Passwords

Password/Passphrase Construction and Management Guideline

<http://security.arizona.edu/files/ISG701.pdf>

Password Security Tips

<http://security.arizona.edu/files/passwordsecurity.pdf>

6. Account management

Common daily tasks such as email, web browsing, and instant messaging do not require administrative privileges and are common avenues for malicious code to attack and compromise end users' computers and data . To be more secure, users should log on with a Limited (or "Least-privileged") User account (LUA), and use elevated privileges only for specific tasks that require them such as downloading or upgrading software.

- More information on this can be found at <http://www.microsoft.com/protect/computer/advanced/useraccount.mspx>

If somebody 'must' run as full administrators regularly, using 'Drop My Rights' from Microsoft can be very helpful to limit the damage that can be done through certain applications such as web browsers or email clients.

- Microsoft's Drop My Rights application can be found at <http://msdn2.microsoft.com/en-us/library/ms972827.aspx>

7. Encrypted authentication

You must configure your email client to securely access your University email account. SSL (Secure Socket Layer) and TLS (Transport Layer Security) are security protocols used to protect your information when you send and receive email. When you activate SSL/TLS in your email client (Thunderbird, Eudora, Outlook), your UA NetID and password cannot be read by an outside party. In email clients without SSL/TLS enabled, passwords appear in "clear text." This means that someone hacking into the system can read and access your UA NetID and password. With your NetID and password, a hacker can access your Student/Employee Link and all your personal information including your Social Security Number, address, and birthdate. They can also read your email messages. Instructions for configuring your email client to use SSL are available at <http://uits.arizona.edu/index.php?id=ssl>.

SSH is the required way to connect with the U-System. SSH uses encryption to prevent eavesdroppers from reading information, such as your password, from the network. All SSH-type software allows for secure communication, replacing the vulnerable utilities like telnet, rlogin, ftp and rcp. More information on SSH tools can be found at <http://ccit.web.arizona.edu/index.php?id=752>.

8. Email relays and proxy servers (Applicable to System Administrators).

Email Relays

- More information and test tools can be found at <http://www.spamhelp.org/shopenrelay/>

Proxy Servers

- More information can be found at <http://www.technerd.net/proxy.html>

9. Session controls

Devices must be configured to "lock" or logoff and require a user to re-authenticate if user leaves device unattended.

To lock your computer screen:

For Windows XP and VISTA hold down the **Windows Logo** key and simultaneously press the **L** key.

-OR-

Press **Ctrl-Alt-Del**, then click **Lock Computer** (or press the enter key).

For Mac OS X your screen saver must be turned on in order to use this method. To find out how to turn on your screen saver, look for Turning a screen saver on or off under Help > Mac Help on your computer. Once you have turned on your screen saver:

1. Go to **Apple Menu > System Preferences**.
2. In the System Preferences window, click the **Security** icon.
3. In the Security window, check the **Require password to wake this computer from sleep or screen saver** box.
4. You will now need your User Account password to unlock your computer and resume your work.

To enable screen saver passwords

To set up your screen saver for Windows XP to prompt you for your User Account password when you return to your computer:

1. Minimize all open windows.
2. On your desktop, right-click any empty area, then select **Properties**. The Display Properties window will open.
3. In the Display Properties window, click the **Screen Saver** tab.
4. On the Screen Saver tab:
 - Select the **On resume, password protect** check box for your current screen saver.
 - Click **Apply**, then **OK**. Your screen saver will now prompt you for your User Account password when you resume your computer work.

For Mac OS X, locking the screen also locks your screen saver! You're all set!

10. Physical security

Remember security threats that can occur at your keyboard as well as remotely, which is especially true if your computer is in a publicly accessible area. Even if your computer is in a locked office, remember that more people than you would think have access to your office (co-workers, facilities crew, janitorial staff etc). Hard copies and other media such as CDs, memory sticks, etc., should be locked in a file cabinet.

11. Unnecessary services (Applicable to System Administrators).

Reduce your surface area for vulnerabilities by turning off services which you don't need to be running. A service that isn't running is usually a service that can't be exploited. Do this very carefully, however, as some services which many not have an immediately obvious purpose could have critical backend functionality.

Related Guidance

Information Security Policy (IS-100)
Minimum Security for Networked Devices Standard (IS-S701)

All italicized terms used in this standard are defined in the Information Security Terms Guideline.

Revision History

Initial Draft	3/11/08
Effective Date	5/27/08