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-S602). 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 Minimum Security for Networked Devices Standard (IS-S602).

1. **OPERATING SYSTEM AND SOFTWARE PATCH UPDATES**
   - Software Patching Guideline (IS-G602B)
   - **Microsoft Operating System**
     - Office of Student Computing Resources (OSCR) Security Guide
     - Microsoft Safety and Security Center
     - UA Computer Science Guide for Patch Installation for Windows
   - Updating a Linux/UNIX Operating System
     - FreeBSD
     - Red Hat Linux
     - Debian GNU/Linux
     - Solaris
   - Macintosh Operating System
     - Updating the Macintosh Operating System - OS Updates pg. 214

2. **ANTIVIRUS SOFTWARE**
   - Antivirus Software Guideline (IS-G602C)
   - Sophos Endpoint Security and Control
   - Sophos Endpoint Security and Control Documentation

3. **ANTI-SPYWARE SOFTWARE**
   - Spyware and Adware Prevention Guideline (IS-G602D)
   - Sophos Endpoint Security and Control
HOST-BASED FIREWALL SOFTWARE
- Firewall Software Guideline (IS-G602E)
- OSCR’s Guide to Enabling the Windows Firewall

4. PASSWORDS
- Password/Passphrase Construction and Management Guideline (IS-G703)

5. 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.
- Microsoft’s Demo for Understanding User Accounts

If somebody ‘must’ run as full administrator on a regular basis, using 'Drop My Rights' from Microsoft can be very helpful in limiting the damage that can be done through certain applications, such as web browsers or email clients.
- Microsoft’s Drop My Rights

6. 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.
- UITS SSL Instructions for Email Programs

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.
- UITS SSH (Secure Shell) Access Clients

7. EMAIL RELAYS AND PROXY SERVERS (APPLICABLE TO SYSTEM ADMINISTRATORS)
- SpamHelp’s Email Open Relay Information and Testing Tools
- Technerd’s Insecure Proxy Scanning Information Center
8. **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:**
  - *Windows XP, Vista, and 7:* 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).
  
  - *Max 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.

9. **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 (coworkers, facilities crew, janitorial staff, etc.). Hard copies and other media, such as CDs, memory sticks, etc., should be locked in a file cabinet.

10. **UNNECESSARY SERVICES (APPLICABLE TO SYSTEM ADMINISTRATORS)**

Reduce your surface area for vulnerabilities by turning off services that you do not need to be running. A service that is not running is usually a service that cannot be exploited. However, do this very carefully, as some services that many not have an immediately obvious purpose could have critical backend functionality.

**Related Guidance**

Information Security Policy (IS-100)
Information Security Terms Guideline (IS-G100)
Minimum Security for Networked Devices Standard (IS-S602)
Software Patching Guideline (IS-G602B)
Antivirus Software Guideline (IS-G602C)
Spyware and Adware Prevention Guideline (IS-G602D)
Firewall Software Guideline (IS-G602E)
Password Construction and Management Guideline (IS-G703)

All italicized terms used in this standard are defined in the Information Security Terms Guideline (IS-G100).

**Revision History**

<table>
<thead>
<tr>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Draft</td>
<td>3/11/08</td>
</tr>
<tr>
<td>Effective Date</td>
<td>5/27/08</td>
</tr>
<tr>
<td>Revision</td>
<td>11/5/12</td>
</tr>
<tr>
<td>Effective Date:</td>
<td>11/5/12</td>
</tr>
</tbody>
</table>