BSD Securing a Windows Device

Guideline	GDE-02	Effective Date	10/30/15	Modified Date	10/27/15	Version	1.0

Table of Contents

PURPOSE

The purpose of these guidelines is to ensure greater security on individual assets, specifically for the security of a Windows device.

SCOPE

These guidelines apply to all Windows computers managed by a user.

GUIDELINES

1.0 Computer Settings

Section	Guideline	Guideline Description	Effort Level
1.1	Use a Password	Require a password to access your computer. See Microsoft Support - Strong Passwords for recommended guidelines for password construction. See Windows: Change your Windows password for instructions (Windows 7). For other versions of Windows, check the Windows Support website.	Low
1.2	Set a Screensaver	Set a screensaver that re-prompts your password to activate after 15 minutes or less of inactivity. See Windows: Use your Windows password for your screen saver password for instructions (Windows 7). For other versions of Windows, check the Windows Support website.	Low
1.3	Install and Use Anti-virus Software	Download Symantec Endpoint Protection for Windows. Log in using your CNetID and password and download the file. Extract the zip file, open the extracted file(s), and click on the installer file. If the Windows firewall is disabled	Medium

		during the Symantec Endpoint Protection install, re-enable the Windows firewall.	
1.4	Turn on the Built-in Firewall	Enable the built-in Windows Firewall. In **Control Panel**, choose **System and Security**. Click on **Windows Firewall**. Click **Turn Windows Firewall on or off**. Choose **Turn on Windows Firewall** for both settings and click OK.	Low
1.5	Encrypt your Hard Drive	Use the Windows built-in encryption tool, BitLocker, to encrypt your computer's hard drive. BitLocker is available for Ultimate and Enterprise editions of Windows Vista and Windows 7 and the Pro and Enterprise editions of Windows 8 and later. Check Microsoft Support for instructions for your version of Windows or see the BSD ISO Website at http://security.bsd.uchicago.edu/encryptwindows/ for more information on encrypting Windows computers.	Medium
1.6	Install UChicago VPN (Virtual Private Network)	Install cVPN software if you expect to use untrusted networks (such as guest wireless in a hotel or coffee shop). UChicago students, researchers, faculty, and staff can download and install cVPN by visiting cvpn.uchicago.edu.	Medium

2.0 Connections

Section	Guideline	Guideline Description	Effort Level
2.1	Use a Secure Internet Connection	Use a secure internet connection. Secure networks include wired connections and uchicago-secure.	Low
2.2	Turn on the UChicago VPN	Turn on UChicago cVPN if using untrusted wireless networks (ie: coffee shops, guest wifi, most publicly accessible non-password protected wifi). Utilizing the UChicago cVPN or any VPN – Virtual Private Network- provides a secure computing experience when accessing a UChicago network or PHI from a remote location or when using Wi-Fi.	Medium
2.3	Turn Off Optional Network Connections	Turn off optional network connections (ie: Wifi, Bluetooth) when not in use. This prevents unauthorized access to your computer through these connections.	Low

3.0 Management and Keeping Up-to-date

Section	Guideline	Guideline Description	Effort Level
3.1	Subscribe to the BSD ISO Security Awareness Newsletter List	Bsd_iso-cybersecurity_newsletter@lists.uchicago.edu at lists.uchicago.edu.	Low

3.2	Report Security Incidents	If you use your computer to maintain or access sensitive institutional data and it is lost or stolen, inform your Manager, IT custodian and send an email to the BSD Information Security Office at security@bsd.uchicago.edu.	Low
3.3	Keep your Windows OS updated	Turn on automatic updating to keep your Windows operating system updated to the latest version of the release. This provides you with security updates and other improvements. See Windows: Turn automatic updating on or off for instructions (Windows 7). For other versions of Windows, check the Windows Support website. Contact your IT custodian if you have questions about an update and the impact on your operation system.	Low
3.4	Keep your Applications Updated	Keep your applications updated take advantage of security updates and other improvements. Contact your IT custodian if you have questions about an update and the impact on your applications.	Low
3.5	Only Install Trusted Applications	Only install applications from reputable software providers.	Low
3.6	Be Aware of the Treatment of Confidential Information	Be aware that the University is bound by law or contract to protect some types of confidential information and in other instances the University requires protection of confidential information beyond legal or contractual requirements as an additional safeguard. Refer to http://humanresources.uchicago.edu/fpg/policies/600/p601.shtml.	Low
3.7	Erase Hard Drive Securely	Before you sell or give away your computer be sure to erase the hard drive securely. There are many tools available for erasing a Hard Drive effectively. https://www.microsoft.com/security/online-privacy/safely-dispose-computers-and-devices.aspx	High

4.0 Additional Best Practices

Section	Guideline	Guideline Description	Effort Level
4.1	Backup your Data	Always keep a backup copy of files you do not wish to lose.	Low
4.2	Enable Web Browser Security Settings	Choose web browser security settings that protect your privacy and enhance security. Learn more about security features in Internet Explorer, Firefox, Safari, and Chrome.	Medium

Resources

- BSD Information Security Office Services
- 601 - Treatment of Confidential Information Policy

Approval and Ownership

Responsible Office: BSD Information Security Office
Guideline Owner: BSD Security Liaison Group

Revision History

Version	Description	Revision Date	Review Date	Reviewer/Approver Name
1.0	Initial Version	10/27/2015	11/01/2016	BSD SLG Members