BSD Securing a Windows Device

Guideline	GDE-02	Effective Date	10/30/15	Modified Date	03/23/2022	Version	2.0

Table of Contents

Purpose 1
Scope 1
Guidelines 1
1.0 Computer Settings 1
2.0 Connections 2
3.0 Management and Keeping Up-to-date 3
4.0 Additional Best Practices 4
Resources 4
Approval and Ownership 5
Revision History 5

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	Requires a password or passphrase to access your computer. Passwords should follow the standards outline here (requires VPN for access). For Windows systems managed and maintained by BSD IT Support please click on the following link to change your password on the domain. For windows systems not managed or maintained by BSD IT Support follow Microsoft recommended procedures which can be found here.	Low

1.2	Set a screensaver and password lock	For windows systems managed and maintained by an IT Support, this setting is already in place. The screensaver should re-prompt for your password after it activate after 15 minutes or fewer of inactivity. For windows systems not managed or maintained by an IT Support follow Microsoft recommended procedure which can be found here.	Low
1.3	Install and Use Antivirus Software	For systems managed and maintained by an IT Support, this setting is already in place. For systems not managed or maintained by an IT Support you can download CrowdStrike here and contact security@bsd.uchicago.edu Another option would be to follow microsoft recommended guidelines for using windows defender which can be found here.	Medium
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	For systems managed and maintained by an IT Support your system is required to be encrypted by your IT Support. Policy for this guideline can be found here and here (Must be on VPN to access these links). For systems not managed or maintained by an IT Support please review your vendors hardware for encryption methods or follow Microsoft guidelines for using BitLocker	Medium
1.6	Install UChicago VPN (Virtual Private Network)	For windows systems managed and maintained by an IT Support please consult your IT Support for the need to install the VPN Client. For windows systems not managed or maintained by an IT Support, 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 VPN by visiting cvpn.uchicago.edu.	Medium

2.0 Connections

Section	Guideline	Guideline Description	Effort Level

2.1	Use a Secure Internet Connection	When off campus use the Uchicago VPN to create a secure connection. When on campus use a wired connection or uchicago-secure for wireless when applicable.	Low
2.2	Turn on the UChicago VPN	Turn off optional network connections (ie: Wifi, Bluetooth) when not in use. This prevents potential unauthorized access to your computer through these connections	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	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 Support and send an email to the BSD Information Security Office at security@bsd.uchicago.edu.	Low
3.2	Keep your Windows OS updated	For windows systems managed and maintained by an IT Support this is already in place for your operating system. Third party applications should be reviewed with your IT Support for updates. For windows systems not managed or maintained by an IT Support 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 microsoft support page for instructions	Low
3.3	Install only trusted applications.	Only install applications from reputable software providers.	

3.4	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
3.5	Erase Hard Drive Securely	Before an asset is disposed of the hard drive must be securely erased or destroyed. For assets purchased and managed by a BSD Custodian, the hard drive will be removed and destroyed. If the asset will be repurposed for another user we recommend that the machine is completely wiped before being repurposed. For assets not managed or maintained by BSD we recommend removal and destruction of the hard drive.	High

4.0 Additional Best Practices

Section Guideline Guideline Description Level

			Level
4.1	Backup your Data	Sensitive information such as PHI requires backups. Please consult your IT department support for the type of data that will be generated and where to save your data.	Low
4.2	Enable Web Browser Security	Choose web browser security settings that protect your privacy and enhance security. Learn more about security features in Microsoft Edge, Firefox, Safari, and Chrome. Note: Microsoft Edge has Internet Explorer backward compatibility so there should be no need for Internet Explorer.	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
2.0	Updated Version	3/23/2022	3/23/2022	BSD ISO