|  |  |
| --- | --- |
| University of Washington Human Subjects DIvision | **WORKSHEET Device Configuration** |

|  |  |
| --- | --- |
|  |  |

|  |
| --- |
| **PURPOSE AND APPLICABILITY** |

This Worksheet was developed to support researchers in meeting the expectations outlined under requirement D1 (“Configure the device”) of the Human Subject’s Division (HSD) [WEBPAGE Data Security Requirements Guidance](https://www.washington.edu/research/hsd/guidance/data-security/). This worksheet provides practical, actionable guidance for configuring research devices to ensure secure operation and to limit access to authorized users only.

Proper device configuration is a foundational step in protecting human subjects data from unauthorized access, loss, or misuse. Whether using institutionally managed or personally owned devices, researchers are responsible for ensuring that devices used in research are secured in accordance with institutional standards and best practices. Similar to many other data security requirements, institutionally managed devices and services frequently meet or exceed the specifications in this checklist without requiring any further action by researchers or other users. As a result, **researchers are encouraged to use institutionally managed devices** as much as possible.

|  |
| --- |
| **RESOURCES** |

Researchers are strongly encouraged to consult with their department Information Technology (IT) and/or UW IT for general guidance, technical support, and access to institutionally approved tools and services. UW IT offers a range of resources to help researchers securely manage their data and devices, including:

* The [Researcher Quick-Start Guide](https://it.uw.edu/get-started/researcher-quick-start-guide/), which provides an overview of essential IT services and tools for research.
* The [UW IT Knowledge Base](https://uwconnect.uw.edu/it?id=it), a searchable repository of articles, how-to’s, and support documentation.

|  |
| --- |
| **REQUIREMENTS** |

1. **Authentication & Access Control**

|  |  |
| --- | --- |
| **Requirement** | **Met** |
| Use strong, unique passwords for each device and account.  | [ ]  |
| **+ Guidance**Passwords should be at least 12-16 characters long and include a mix of uppercase and lowercase letters, numbers, and special characters. Avoid reusing passwords or using easily guessable information such as birthdays, names, or dictionary words.  |  |
| Lock your device when not in use; enable automatic timeouts.  | [ ]  |
| **+ Guidance**Set your computer and mobile devices to auto-lock after a short period of inactivity (e.g., 5 minutes).* [Windows reference](https://answers.microsoft.com/en-us/windows/forum/all/how-to-auto-lock-the-device-after-a-set-time-of/d29758c0-784d-4266-807d-05c7b5c3331a)
* MacOS [reference one](https://support.apple.com/guide/mac-help/set-sleep-and-wake-settings-mchle41a6ccd/mac), [reference two](https://support.apple.com/guide/mac-help/require-a-password-after-waking-your-mac-mchlp2270/mac)
* [iPad OS and iOS reference](https://support.apple.com/guide/iphone/keep-the-iphone-display-on-longer-iph7117338a8/ios)
* [Android reference](https://support.google.com/android/answer/9079129?hl=en)

Set your computer and mobile devices to not display notifications or message content (e.g., text messages, emails) on the lock screen.* [Windows reference](https://answers.microsoft.com/en-us/windows/forum/all/lock-screen-notifications-in-windows-10/44586668-8057-40db-a2bd-2c64bd5834a8)
* [MacOS reference](https://support.apple.com/guide/mac-help/notifications-settings-mh40583/mac)
* [iPad OS and iOS reference](https://support.apple.com/en-us/108781)
* [Android reference](https://support.google.com/android/answer/9079661?hl=en)

Manually lock your screen (Windows: Win + L, Mac: Ctrl + Command + Q) whenever stepping away.  |  |
| Use a password manager (e.g., [LastPass Enterprise via UW-IT](https://it.uw.edu/uware/lastpass-password-manager/)). | [ ]  |
| **+ Guidance**A password manager generates and securely stores complex passwords so you don’t have to remember them. Do not save passwords in web browsers.  |  |
| Enable Multi-Factor Authentication (MFA) wherever possible.  | [ ]  |
| **+ Guidance**MFA adds an extra layer of security by requiring something you have (e.g., an authenticator app) in addition to something you know (password).Use official authenticator apps like Microsoft Authenticator, DUO, or Google Authenticator instead of SMS or email-based codes, which can be intercepted.  |  |
| Consider enabling biometric authentication wherever possible (e.g., Windows Hello, Face ID, Touch ID) for added security.  | [ ]  |
| **+ Guidance**Biometric authentication can enhance security but should not replace strong passwords.  |  |

1. **Software & System Updates**

|  |  |
| --- | --- |
| **Requirement** | **Met** |
| Enable automatic updates for your operating systems (OS), applications, and security software.  | [ ]  |
| **+ Guidance**Keeping your OS (Windows/macOS/Linux/iOS/Android) and software up to date protects against known vulnerabilities and ensures you receive the latest security patches. * [Windows reference](https://support.microsoft.com/en-us/windows/install-windows-updates-3c5ae7fc-9fb6-9af1-1984-b5e0412c556a#windowsversion=windows_11)
* [macOS reference](https://support.apple.com/guide/mac-help/keep-your-mac-up-to-date-mchlpx1065/mac)
* [iPadOS and iOS reference](https://support.apple.com/guide/iphone/update-ios-iph3e504502/ios)
* [Android reference](https://support.google.com/android/answer/7680439?hl=en&sjid=1817921126976266116-NC)

Enable automatic updates for web browsers, research tools, applications, and any software, especially those handling confidential data. * [iPadOS and iOS reference](https://support.apple.com/en-us/102629)
* [Android reference](https://support.google.com/googleplay/answer/113412?hl=en)
 |  |

1. **Antivirus & Firewall**

|  |  |
| --- | --- |
| **Requirement** | **Met** |
| Install and enable antivirus software on your devices. | [ ]  |
| **+ Guidance**Microsoft Defender is built into Windows and offers real-time protection.Utilize XProtect, which is integrated into the MAC operating system and no additional action is required. For Linux distributions, install and use ClamAV for antivirus protection.Ensure that the antivirus software has automatic updates enabled to protect against the latest threats and vulnerabilities.  |  |
| Enable a host-based firewall (deny-all by default) to prevent unauthorized network access.  | [ ]  |
| **+ Guidance**A firewall helps block unauthorized incoming and outgoing connections from your device.Configure your firewall to allow only trusted applications to communicate over the network. * [Windows reference](https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/)
* [macOS reference](https://support.apple.com/guide/mac-help/block-connections-to-your-mac-with-a-firewall-mh34041/15.0/mac/15.0)
 |  |

1. **Encryption**

|  |  |
| --- | --- |
| **Requirement** | **Met** |
| Enable whole-disk encryption for built-in storage.  | [ ]  |
| **+ Guidance*** Windows: Use [BitLocker](https://support.microsoft.com/en-us/windows/bitlocker-drive-encryption-76b92ac9-1040-48d6-9f5f-d14b3c5fa178)
* macOS: Use [FileVault2](https://support.apple.com/guide/mac-help/protect-data-on-your-mac-with-filevault-mh11785/mac)
* Linux: Use LUKS (Linux Unified Key Setup) or an equivalent solution.
 |  |
| Ensure mobile devices are encrypted to protect data in case of loss or theft.  | [ ]  |
| **+ Guidance**iOS and Android devices both support full-disk encryption. * iOS has this enabled by default as long as a device PIN or biometric authenticator has been enabled.
* Ensure that Android devices have this enabled. [Android reference](https://learn.microsoft.com/en-us/intune/intune-service/user-help/encrypt-your-device-android)
 |  |

1. **Data Backup**

|  |  |
| --- | --- |
| **Requirement** | **Met** |
| Regularly back up data to a secure, encrypted location (e.g., UW-approved cloud storage). | [ ]  |
| **+ Guidance**Store data and backups in UW IT-approved could services like your UW.edu [OneDrive (O365)](https://uwconnect.uw.edu/it?id=sc_entry&sys_id=60a95c36db8af38437ae9ec6db961956) account or a UW-managed instance of REDCap. Avoid backing up data on external drives such as USB drives. If data must be stored or backed up on external drives, ensure the drive is fully encrypted.  |  |

1. **Network Security**

|  |  |
| --- | --- |
| **Requirement** | **Met** |
| Avoid public Wi-Fi and ad-hoc network sharing. Use a personal hotspot if necessary.  | [ ]  |
| **+ Guidance**Public Wi-Fi networks are vulnerable to communication interception. If unavoidable, use a VPN provided or approved by UW IT. |  |
| Do not use commercial VPNs unless explicitly approved by the IRB.  | [ ]  |
| **+ Guidance**Many VPN services log (and sometimes sell) your data or have security flaws. Avoid services promoted in online ads. The [Husky OnNetVPN](https://it.uw.edu/summary/husky-onnet/) provided by UW-IT for UW students, faculty, and staff may be used to access university resources remotely.  |  |

1. **Secure Behavior & Human Practices**

|  |  |
| --- | --- |
| **Requirement** | **Met** |
| Be cautious of phishing attempts. Always verify emails, links, and text messages before clicking or responding.  | [ ]  |
| **+ Guidance**Hover over links and the sender email address. Look for misspelled URLs, domains, unexpected results, and generic greetings (e.g., “Dear User”).Never enter credentials or confidential information on sites linked in emails unless you are certain of their legitimacy.  |  |
| Be wary of tech support scams and avoid unofficial tech repair services.  | [ ]  |
| **+ Guidance**Scammers may claim to be from Microsoft, Apple, or IT support. Always verify before allowing remote access. Use only trusted, vendor certified repair shops (e.g., Apple Store, manufacturer-certified centers). Do not take UW equipment to external or third-party tech repair services unless explicitly authorized.  |  |
| Do not share devices with others, especially those used for research. | [ ]  |
| **+ Guidance**If a shared computer must be used, have separate accounts with restricted access.  |  |
| Use separate user accounts for different activities (e.g., research vs. personal use). | [ ]  |
| **+ Guidance**Avoid using the same account for personal use and research use. Using your UW.edu account is usually best for IRB-governed research.  |  |
| Always lock your device when stepping away and never leave it unattended in public places.  | [ ]  |
| **+ Guidance**This includes libraries, coffee shops, and cars. Opportunistic theft can lead to serious data breaches.  |  |
| Immediately report lost or stolen devices per IRB and institutional guidelines.  | [ ]  |
| **+ Guidance**Report incidents to UW IT or the IRB as required.  |  |
| Sanitize devices before disposing of it to ensure all data stored on the device cannot be recovered.  | [ ]  |
| **+ Guidance**“Sanitizing” devices usually includes securely erasing and factory resetting the device and/or removing storage media like hard drives. Many common methods for laptops, desktops, phones, and tablets are more effective at securely erasing data when the device’s storage media have been encrypted since the device was first used or set up. Examples include:* [Windows reference](https://support.microsoft.com/en-us/windows/reset-your-pc-0ef73740-b927-549b-b7c9-e6f2b48d275e)
* [macOS reference](https://support.apple.com/en-us/102664)
* [iPadOS and iOS reference](https://support.apple.com/guide/iphone/erase-iphone-iph7a2a9399b/ios)
* [Android reference](https://support.google.com/android/answer/6088915?hl=en)
 |  |
| Enable remote lock/wipe features where available (e.g., iOS, Android).  | [ ]  |
| **+ Guidance**Ensure that “Find My Device” style features are enabled for lost device recovery.* [Windows reference](https://support.microsoft.com/en-us/account-billing/find-and-lock-a-lost-windows-pc-f21327d3-282e-9269-fffb-bc16e198dcac)
* [iOS, iPadOS, and macOS reference](https://support.apple.com/en-us/102648)
* [Android reference](https://support.google.com/android/answer/6160491?hl=en)
 |  |

1. **Secure Storage & Physical Security**

|  |  |
| --- | --- |
| **Requirement** | **Met** |
| Minimize or avoid storing confidential data on personal devices.  | [ ]  |
| **+ Guidance**If data must be stored, ensure it is encrypted and backed up securely.  |  |
| Avoid using portable storage media (e.g., USB devices) whenever possible.  | [ ]  |
| **+ Guidance**USB drives are easily lost and can be infected with malware. If necessary, use encrypted drives.  |  |
| Physically secure your devices when not in use (e.g. locked cabinets, security cables).  | [ ]  |
| **+ Guidance**Use laptop locks, secured drawers, or safes for storing research devices. |  |
| Minimize physical printing. Use a cross-cut shredder for disposal of sensitive materials. | [ ]  |
| **+ Guidance**Avoid printing confidential research data unless absolutely necessary. |  |

1. **Secure Web & Application Configurations**

|  |  |
| --- | --- |
| **Requirement** | **Met** |
| Use encrypted protocols where feasible.  | [ ]  |
| **+ Guidance**Unencrypted protocols expose login credentials and data. Always use secure, encrypted alternatives (e.g., SFTP instead of FTP, SSH instead of Telnet, HTTPS instead of HTTP).  |  |
| Consider using a separate web browser or browser profile for research activities.  | [ ]  |
| **+ Guidance**See also #7 above – use separate devices or user profiles where feasible.  |  |
| Tie research account to your UW.edu or institutional email account whenever possible.  | [ ]  |
| Use UW-provided solutions for research data storage, email, and data collection (e.g., UW Office 365, REDCap). | [ ]  |
| **+ Guidance**Institutional solutions meet compliance requirements for handling ePHI and PII. * [Microsoft Office 365](https://it.uw.edu/uware/microsoft-office-for-desktop/)
 |  |
| Disable or avoid AI features unless reviewed and explicitly approved for use in research.  | [ ]  |
| **+ Guidance**AI-generated content, summaries, transcription, or analysis tools may store or process data externally, creating potential compliance and security risks. See these additional guidance documents:* [UW Medicine Interim Guidance for Generative AI in the Healthcare Setting](https://uwnetid.sharepoint.com/sites/og_uwm_internal_comms/vitals_document_repository/Generative%20AI%20at%20UW%20Medicine/Forms/AllItems.aspx?id=%2Fsites%2Fog%5Fuwm%5Finternal%5Fcomms%2Fvitals%5Fdocument%5Frepository%2FGenerative%20AI%20at%20UW%20Medicine%2FUW%2DMedicine%2DLLM%2DInterim%2DGuidance%2DGenerative%2DAI%2Epdf&parent=%2Fsites%2Fog%5Fuwm%5Finternal%5Fcomms%2Fvitals%5Fdocument%5Frepository%2FGenerative%20AI%20at%20UW%20Medicine)
* [UW IT Generative Artificial Intelligence General Use Guidelines](https://it.uw.edu/guides/security-authentication/artificial-intelligence-guidelines/)
 |  |

|  |
| --- |
| **RELATED MATERIALS** |

Refer to additional resources on the UW IT website, including:

* [<https://it.uw.edu/guides/security-authentication/securing-computer/>](https://it.uw.edu/guides/security-authentication/securing-computer/)
* <https://it.uw.edu/guides/security-authentication/securing-computer/computer-management/>
* <https://it.uw.edu/get-started/researcher-quick-start-guide/>

|  |  |  |  |
| --- | --- | --- | --- |
| **Version Number** | **Posted Date** | **Implementation Date** | **Summary of Changes** |
| 1.0 | 06.26.2025 | 06.26.2025 | New document  |

**Keywords:** Confidentiality