Please Note: Cybersecurity is a rapidly evolving field. This document was last updated on February 2, 2019. Some of the technical guidance within this document may change, and some of the risks defined may increase or decrease in their potential likelihood or impact.

Appendix B: Implementation Guidance

While many of the controls described in this guide are simple, that does not mean it is easy to decide where (or how strictly) to implement them in an organization. This section provides additional resources and guidance to help identify critical account, priority devices, and other information to help prioritize where an organization focuses its limited time and attention.

Strong Authentication

Read the description of this control here.

Set policy for this control here.

The below chart is a basic way to determine which accounts should be considered "critical" to an organization. By rating the accounts and mapping them to the staff with access, organization can determine which staff members need to prioritize enabling strong authentication.

Account Inventory		
What online accounts does your organization consider important to your mission? This could include email, social media, financial, online storage, etc.:		
Account	**Purpose**	**Impact on organization if access is lost** *(High, Medium, Low)*
What staff members have access to which account? Include if they "own" the account and are responsible for its activity.		
Account	**Staff**	**MFA Enabled?**

Automatic Updates and Software Licenses

Read the description of this control here.

Set policy for this control here.

Turning on Automatic Updates

If an organization uses enterprise software that requires centralized deployment of patches and updates, an IT administrator should be in charge of patch management for critical software.

Guides on how to enable automatic updates on common operating systems can be seen below:

- **Android Devices:** https://support.google.com/googleplay/answer/113412?hl=en
- **OSX Devices:** https://support.apple.com/kb/PH25532?locale=en_US
- **iOS Devices:** https://support.apple.com/en-us/HT202180
- **Windows 10:** https://support.microsoft.com/en-us/help/3067639/how-to-get-an-update-through-windows-update
    - **Previous versions:** https://support.microsoft.com/en-us/help/3067639/how-to-get-an-update-through-windows-update

Finding Affordable Software Licenses

Software is expensive. Cost is a major contributor to why many organizations fail to update their software. Organizations like TechSoup can help provide non-profits with affordable, discounted, or free software. But many cloud service providers offer free or discounted services for nonprofits and other public-interest organizations. Some examples of those services include:

- **Productivity Suites:**
    - https://products.office.com/en-us/nonprofit/office-365-nonprofit-plans-and-pricing?tab=1
    - https://www.google.com/nonprofits/
- **Web Services:**
    - https://aws.amazon.com/government-education/nonprofits/
- **Web Hosting:**
    - https://help.dreamhost.com/hc/en-us/articles/215769478-Non-profit-discount
- **Contact/Customer Relationship Management:**
    - http://www.salesforce.org/nonprofit/

The Cloud

Read the description of this control here.

Set policy for this control here.

Moving data to cloud-based services can be a challenge. And, just as important, ensuring that old devices are cleaned of that data can also be difficult. This section outlines a number of important steps to take into account when migrating important data away from legacy devices. For some organizations, this is a process that can be run internally. For other organizations with a greater "sprawl" of data or devices, services exist to support migration to cloud-based services. TechSoup provides cloud migration consultation services for non-profits: http://page.techsoup.org/cloud-services?cg=pc

Migrating Files to Cloud-Based Storage

It is likely that data - both sensitive and insensitive - is currently spread across many personal devices. These files should now be consolidated in a single place. Cloud storage services, such as Google Drive or Office OneDrive, provide a simple way for employees to migrate files into a centralized location. Employees can log into a cloud storage service and upload any legacy files. This process is imperfect - it is very easy to miss files. Here a few common locations that individuals often miss when looking for legacy files on a device:

- **Downloads folders:** This applies to both mobile devices and laptops. Files downloaded onto devices for one-time viewing are often forgotten, making the downloads file a honeypot of potentially sensitive information. Employees should search through their downloads for documents that need to be archived in the cloud, and delete the entirety of their downloads folders when they have finished. For information on how to find common downloads directories, see below:
    - Windows
    - OSX
    - Android

    - iOS
- **Search:** Organizations can save documents in many locations, sometimes accidentally, sometimes on purpose. The result is that most organizations end up having a sprawl of folders across their "documents" library, their desktop, and everywhere in-between. While spending time searching through common directories for important documents is worthwhile, it is not always clear where to look. Using the search function in your operating system can be a powerful shortcut - but what should you search for? Depending on what type of work you do, there are likely only a few file types with which you regularly work - Microsoft Word, Excel, and Powerpoint are some of the most common. By searching for their extension name (or the .xyz at the end of the file type - such as .doc or docx for Word, or .xls or .xlsx for Excel), you can search your operating system for documents that are important to migrate. The searching process can also reveal folders you may have forgotten about that are hiding important files. Some common extensions you may want to search for include:
    - **Microsoft Word:** .doc, .docx, .odt
    - **Microsoft Excel:** .xls, .xlsx, .csv
    - **Microsoft Powerpoint:** .ppt, .pptx
    - **Adobe:** .pdf
    - **Apple Pages:** .pages
    - **Apple Numbers:** .number
    - **Apple Keynote:** .key, .keynote
    - An exhaustive list of other file formats and their associated applications can be found here: https://en.wikipedia.org/wiki/List_of_file_formats.
    - **Temporary folders and other hidden locations:** Some operating systems will have "temp" folders for a number of applications, such as Office, that save in-progress documents. While it is possible to find these folder, they can often be hidden and rarely contain complete documents or files that you'll want to back up. The best way to ensure a device is clean of legacy files is to reinstall its operating system. Newer devices make this refresh easy - but many will ask if you'd like to keep an archive of the old files. This is fine, but make sure you remove that

archive and store it somewhere safe - like on a USB drive not connected to the internet.

> **WARNING:** Resetting a device to factory settings or reinstalling its operating system will purge all data and applications from the device. Make sure any information you want to keep is backed up in the cloud or on an external drive before resetting your device.

Information on how to reset, refresh, or reinstall common operating systems can be found here:

- Resetting Windows 10
- How to refresh, reset, or reinstall older versions of Windows
- How to restore iOS device to factory settings
- How to wipe and reset macOS device
- How to restore factory settings on an Android device

HTTPS

Read the description of this control here.

Set policy for this control here.

For most websites, enabling HTTPS will not be a giant task - but it does require some baseline technical knowledge. Trying to enable HTTPS may be possible without any technical experience if you use a platform like Wordpress or Squarespace that does some of the work for you - but depending on your site's style and configuration, it can still be a challenge. It is advisable to rely on whoever administers or designed your site for support in enabling HTTPs. Some general information about how to turn on HTTPS can be found in this guide: https://httpsiseasy.com/.

Other guides to enabling HTTPS can be found here:

- **Let's Encrypt** is a free source of the certificates needed to offer HTTPS on your website. Their documentation is generally geared toward more technical users: https://letsencrypt.org/

- **Facebook** has provided a quick guide on how and why to enable HTTPs, with links to a number of additional resources: https://developers.facebook.com/docs/facebook-login/web/enabling-https

Additional information on how to enable HTTPS in common site hosting and design services can be found here:

- **Wordpress:** https://make.wordpress.org/support/user-manual/web-publishing/https-for-wordpress/
- **Squarespace:** https://support.squarespace.com/hc/en-us/articles/205815898-Squarespace-and-SSL

Data Security

Read the description of this control here.

Set policy for this control here.

Data Inventory

Data security is a difficult task, and requires ongoing management and attention. However, basic measures to encrypt devices with access to sensitive information can go a long way for low-risk organizations. The below inventory is an example of how to identify which devices should be encrypted:

Data Inventory	
What data does your organization consider "sensitive" or to be essential to fulfilling its mission? This could include strategic plans, donor lists, financial records, HR records, etc. Where (what devices or systems) does that information reside?	
Data Type	**Location**
What staff members regularly access or process that information? Include if they "own" that data type.	
Data Type	**Staff**
What devices do those staff members use to access critical or sensitive information? Those devices should have full disk encryption enabled.	
Staff	**Devices**

Access Management in the Cloud

Access management is an ongoing task, but many cloud-based storage services provide a high-level view of document permissions in use across the organization. Larger organizations may need to deploy more robust solutions to manage access to organization resources, but these two guides are a good place to start for LROs using common cloud storage services:

- **Microsoft One Drive:** https://support.office.com/en-us/article/stop-sharing-onedrive-files-or-folders-or-change-permissions-0a36470f-d7fe-40a0-bd74-0ac6c1e13323

- **Google Drive:** https://support.google.com/a/answer/60781?hl=en

Not all documents or directories warrant constant monitoring for access permissions. However, a few key considerations that may help organizations identify documents and directories likely to need their permissions reviewed:

- **Documents of critical importance to organizational operations:** Strategic plans, budgets, funding agreements or plans.
- **Documents containing personal or sensitive information:** HR files, donor or outreach lists with contact information, payment records, or any data that might illustrate information about individuals' behavior or preferences
- **Files exposed to external viewers:** Documents shared outside of your organization for purposes of external review or collaboration.
- **Files accessed by departing staff:** When staff leave, they are unlikely to resolve any outstanding access permissions issues. For example: owners of documents may have allowed a personal account to access an organization-owned document. Once their organization account is disabled, they may be able to retain access to that document if their personal account has opened it even once. They may have also shared documents and directories outside the organization in away that other staff are unaware of. When staff leave, it is important to review their files for permissions issues - or to archive all their documents in a new directory where the permissions can be holistically altered.

Enabling Device Encryption

Windows Devices

Information on how to turn on device encryption in Windows 10 devices can be foud here: https://support.microsoft.com/en-us/help/4028713/windows-10-turn-on-device-encryption

Note: This feature is not available on Windows Home edition, requires at least Windows Professional license.

Apple Devices

FileVault is a disk encryption feature built in to Mac OS X. FileVault provides 128bit AES encryption with a 256 bit key to encrypt the disk and all files located on the drive. This is a very strong encryption mechanism. Strong encryption helps to prevent unauthorized access to the Mac since the disk and all file contents are encrypted, a requiring the password must be entered on boot before the computer, data, and files can be accessed.

The following link provides a step- by- step instructions on how to enable FileVault: https://support.apple.com/en-us/HT204837

All iOS devices (iPads, iPhones) from recent years have been encrypted by default, but the vast majority of iOS devices can have encryption enabled. If you need to enable device encryption on an iOS device, you can follow these directions: https://ssd.eff.org/en/module/how-encrypt-your-iphone

Android Devices

General instructions on how to enable full-disk encryption on Android devices can be found here: https://docs.microsoft.com/en-us/intune-user-help/encrypt-your-device-android, though the settings may differ across devices. Many new Android devices are encrypted by default.

Note: Chromebooks, which run a similar (but distinct) operating system called ChromeOS, are encrypted by default.