**Madelyn Speers’ Home Network**

**Manageable Network Plan**

Version 3.0

12/02/24

**VERSION HISTORY**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version #** | **Implemented**  **By** | **Revision**  **Date** | **Approved**  **By** | **Approval**  **Date** | **Reason** |
| 1.0 | Madelyn Speers | 10/19/24 | Madelyn Speers | 10/19/24 | Document Creation |
| 2.0 | Madelyn Speers | 11/11/24 | Madelyn Speers | 11/11/24 | Milestones 3, 4, 5 |
| 3.0 | Madelyn Speers | 12/02/24 | Madelyn Speers | 12/02/24 | Milestones 6, 7, 8 |
|  |  |  |  |  |  |

Table of Contents

[1 Overview 5](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723582)

[2 Introduction 6](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723583)

[1.1 Purpose 6](file:///C:\Users\maddy\Downloads\Manageable-Network-Plan-Milestone(1and2)%20(2).docx#_Toc147412648)

[1.2 Planning Overview (Milestone 1 Documentation Strategy) 7](file:///C:\Users\maddy\Downloads\Manageable-Network-Plan-Milestone(1and2)%20(2).docx#_Toc147412649)

[1.2.1 Network Description 7](file:///C:\Users\maddy\Downloads\Manageable-Network-Plan-Milestone(1and2)%20(2).docx#_Toc147412650)

[1.2.2 Assumptions and Constraints (Example Information, must be updated) 7](file:///C:\Users\maddy\Downloads\Manageable-Network-Plan-Milestone(1and2)%20(2).docx#_Toc147412651)

[1.2.3 System Organization (Milestone 2 Network Map & Milestone 1 Network Documentation) 8](file:///C:\Users\maddy\Downloads\Manageable-Network-Plan-Milestone(1and2)%20(2).docx#_Toc147412652)

[1.3 Glossary 12](file:///C:\Users\maddy\Downloads\Manageable-Network-Plan-Milestone(1and2)%20(2).docx#_Toc147412653)

[2 Management Overview 13](file:///C:\Users\maddy\Downloads\Manageable-Network-Plan-Milestone(1and2)%20(2).docx#_Toc147412654)

[2.1 Description of Implementation 13](file:///C:\Users\maddy\Downloads\Manageable-Network-Plan-Milestone(1and2)%20(2).docx#_Toc147412655)

[2.2 Points-of-Contact 13](file:///C:\Users\maddy\Downloads\Manageable-Network-Plan-Milestone(1and2)%20(2).docx#_Toc147412656)

[2.3 Major Tasks (Milestone 1 Task Consideration Documentation) 14](file:///C:\Users\maddy\Downloads\Manageable-Network-Plan-Milestone(1and2)%20(2).docx#_Toc147412657)

[2.4 Implementation Schedule (Milestone 1 Task implementation Documentation) 17](file:///C:\Users\maddy\Downloads\Manageable-Network-Plan-Milestone(1and2)%20(2).docx#_Toc147412658)

[2.5 Security and Privacy (Access Control Protections) 18](file:///C:\Users\maddy\Downloads\Manageable-Network-Plan-Milestone(1and2)%20(2).docx#_Toc147412659)

[2.5.1 System Security Features 18](file:///C:\Users\maddy\Downloads\Manageable-Network-Plan-Milestone(1and2)%20(2).docx#_Toc147412660)

[2.5.2 Security Set Up During Implementation (Access Control Protections) 18](file:///C:\Users\maddy\Downloads\Manageable-Network-Plan-Milestone(1and2)%20(2).docx#_Toc147412661)

[2.7 Open Issues 18](file:///C:\Users\maddy\Downloads\Manageable-Network-Plan-Milestone(1and2)%20(2).docx#_Toc147412662)

[Milestone 3: Protect Your Network (Network Architecture) 19](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723604)

[Overview 20](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723605)

[Facilities and Network Enclaves 21](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723606)

[High-Value Network Assets 21](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723607)

[Choke Points On This Network 22](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723608)

[Single Points of Failure 22](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723609)

[Legacy Systems 23](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723610)

[Plan Document Updates 24](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723611)

[Milestone 4: Reach You Network (Device Accessibility) 25](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723612)

[Overview 26](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723613)

[Laptop Computers 26](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723615)

[Mobile Devices 43](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723616)

[TVs 26](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723617)

[Remote Administration 26](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723618)

[Physical Security 26](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723619)

[Automating Administration 26](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723620)

[Administrative Tools 26](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723621)

[Plan Document Updates 27](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723622)

[Milestone 5: Control Your Network(User Access) 27](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723623)

[User Accounts 28](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723624)

[Privileged accounts 28](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723625)

[Least privilege administrative model 28](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723626)

[Users Installing Software 28](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723627)

[Expiration Dates On Accounts 28](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723628)

Plan Document Updates 28

**Milestone 6: Manage Your Network, Part I (Patch Management) ………………………....29**

**Milestone 7: Manage Your Network, Part II (Baseline Management) ……………………..32**

**Milestone 8: Document Your Network………………………………………………………..40**

[*APPENDIX A: Manageable Network Implementation Plan Approval* 43](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723630)

[*APPENDIX B: REFERENCES* 45](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723631)

[*APPENDIX C: System Hardware Inventory* 45](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723633)

[*APPENDIX D: System Software Inventory* 45](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723634)

[*APPENDIX E: Milestone-1 Check-List* 45](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723635)

[*APPENDIX F: Milestone-2 Check-List* 46](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723636)

[*APPENDIX G: Milestone-3 Check-List* 47](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723637)

[*APPENDIX H: Milestone-4 Check-List* 49](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723638)

[*APPENDIX I: Milestone-5 Check-List* 49](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723639)

[*APPENDIX J: Milestone-6 Check-List* 50](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723640)

[***APPENDIX K: Milestone-7 Check-List…………………………………………………...52***](file:///C:\Users\maddy\Downloads\ManagableNetworkPlan-Student-Example(3-4-5).docx#_Toc86723641)

***APPENDIX L: Milestone -8 Check-List…………………………………………………..53***

# Overview

“The Manageable Network Plan is a series of milestones to take an unmanageable and insecure network and make it manageable, more defensible, and more secure. The Plan is intended to be a long-term solution; implementing the milestones may take a significant amount of resources and time (possibly months or even years). But consider: If your network is not manageable, or only barely manageable, it will be very difficult for you to fully implement *any* security measures. Once your network is manageable, you will be able to consider and implement security measures—and verify their implementation—much more efficiently and effectively. Admins may start shouting, “We have no free time! How can we do all this???” Having a manageable network *increases* your free time; it allows you to be *proactive* instead of *reactive*. And if you do have a huge network, don’t take on the whole network at once: consider starting with individual subnets. Each of the Plan’s milestones contains a “To Do” list, and may also contain documentation requirements, points to consider, and ongoing tasks. Ideally, each milestone should be fully implemented before moving on to the next one, although some milestones can be implemented in parallel. If the earlier milestones are already implemented on your network, skip ahead to the first one that is not yet fully implemented. To determine this, each milestone has a checklist. For each question in a milestone’s checklist, answer Yes or No; if “No” or only partially implemented, provide an explanation. If you consider the explanation acceptable from a risk management standpoint, check Accepts Risk.1 If all the questions can be answered Yes or Accepts Risk, the milestone is complete. Document and date your answers to these milestone checklists. If a future network evaluation finds problems on your network, it may indicate that you should no longer accept the risks that you did in some areas, and that changes are needed. (Some checklist questions have suggested metrics that can be used to track progress.)

The Plan provides overall direction, offers suggestions, calls out crucial security tips,2 and gives references to books, Web resources, and tools.3 Every network is different, so use the Plan milestone “To Do” lists, documentation requirements, and ongoing tasks as a guide, and generate specific tasking for your network. The points to consider under each milestone may suggest additional tasks for your network. When developing these tasks, be mindful of any security assessment and authorization authorities that you must comply with. Use relevant standards (such as SCAP standards4) and community-vetted data models so that you can benefit from others’ work, both immediately and in the long term. Be sure each task states *what* is to be done, *who* is to do it, and *when* the task must be completed. Also be sure that your specific tasking does not water down or miss the point of the Plan milestones—that won’t help your network become more manageable! “ (NSA).



Figure 1: Milestones

# Introduction

## 1.1 Purpose

The Purpose of the Home Network Manageable Network Implementation plan is to create documentation about the existing home network, the hardware and software that interacts with it, and understand how to manage, update, secure, and backup the home network.

## ****1.2 Planning Overview (Milestone 1 Documentation Strategy)****

This home network was installed by Frontier and already in production at the time this plan was created. The network did not have any form of diagram or documentation, so this plan will create diagrams of the network and the devices interacting with it, as well as how to better implement the network, ensure security methodology, and install new devices on the network.

Documentation and changes to the network will be in this document, which will be automatically backed up to Madelyn Speers’ OneDrive as revisions are made.

Changes will be documented through revision control listed in this plan. All tasks that are proposed and implemented will be tracked in section 2.4’s Implementation Schedule. At the last Friday of each month this document will be hard copied and stored in the end user’s safe under his closet for safe keeping.

### **1.2.1 Network Description**

This home network is used by Madelyn Speers, primarily for schoolwork, web browsing, gaming, and streaming movies. The network use VLANs to ensure each tenant has its own isolated network segment. There are no additional users at time of revision but might be occasional depending on if friends visit the network. The current Frontier router utilizes WPA2 key with a password generated by the technology company.

The home network has endpoints that use wireless or wired ethernet cat6 connectivity.

Operating systems being used by endpoints on the network are:

* Windows 11
* Apple iOS 13
* Samsung Series 7 TV (Living Room)
* Amazon Alexa OS
* Samsung Series 6 TV (Bedroom 1)
* Samsung Series 6 TV (Bedroom 2)

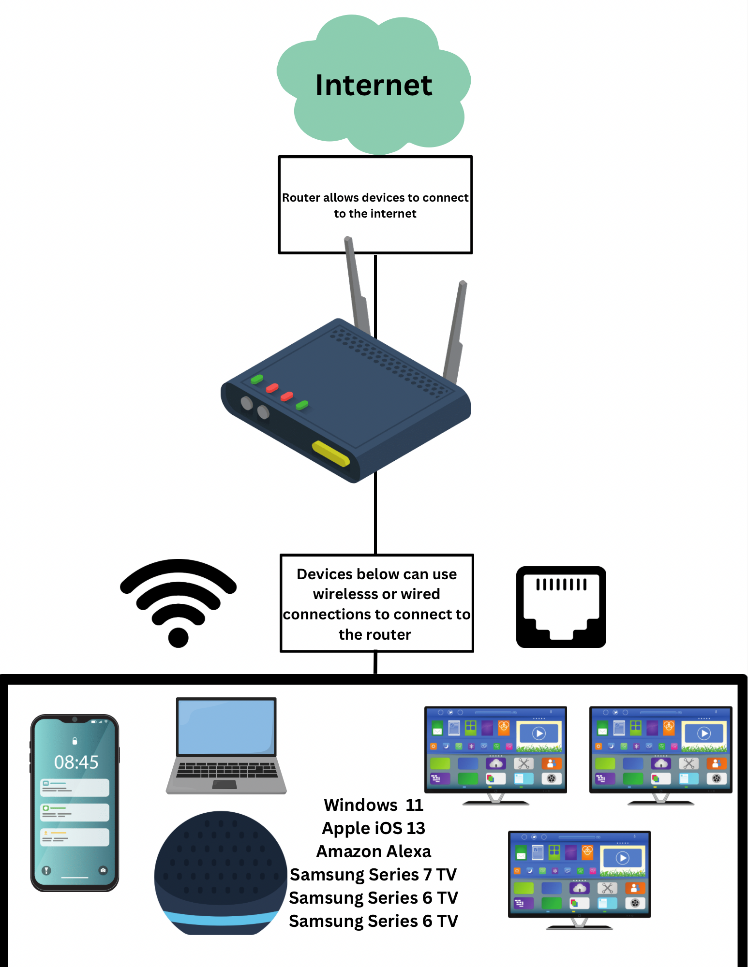
The router being used for wireless and wired connections is a commercial or enterprise-grade router (apartment complex).

### 1.2.2 Assumptions and Constraints

* Schedule:
  + The schedule will not have dates of changes and events prior to the creation of this document since the network was created before this plan was
* Budget:
  + This network plan intends to implement and improve the network with the least number of additional purchases or money necessary. Free software will be prioritized in this plan for upgrades and maintenance. Cost/benefit analysis will be conducted on paid software and hardware.
* Resource Availability and manpower:
  + The administrator of the network Madelyn Speers has access to resources and skillset to operate on the network with general maintenance, network upgrades, and more.
* Software and technology to be used:
  + Software and technology might be reused on multiple devices.
* Limitations with certain interfaces
  + Operating Systems such as TV OS’s, Alexa do not have an authentication method so guest access will be provided to all who use these devices.
  + Windows endpoints utilize the capability of logging in as separate users though family/friend’s personal windows accounts. No guest accounts are implemented.
  + All mobile devices utilize facial recognition or PIN for unlocking.

### **1.2.3 System Organization (Milestone 2 Network Map & Milestone 1 Network Documentation)**

All network mapping is conducted by utilizing the router’s connected device list and verified utilizing NMAP as well as Advanced IP Scanner. This list and graph will be updated as new devices are added or removed from the network. This update will occur weekly every Friday. Plans to automate this update task are being processed.



Routes to the apartment’s router are either Wi-Fi or ethernet.

As devices are end of life and removed from the network they will be removed from this document at the scheduled weekly update interval.

Windows 11 Device Information

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Device | Form Factor | Manufacturer | Model | MAC Address | RAM | OS Version | Assignment | Service Tag |
| Laptop | Laptop | Dell | Inspiron 14 Plus 7420 | FC:34:97:49:D0:E9 | 16GB | 23H2 | Madelyn Speers | FY2SFS3 |

Phone/Tablet Device Information

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Device | Model | Manufacturer | MAC Address | OS Version | Assignment | Service Tag |
| iPhone-1 | iPhone 13 | Apple | 52:94:39:7A:20:09 | iOS 18.0.1 | Madelyn Speers | Apple-1 |

IoT Device Information

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Manufacturer | Model | Mac Address | OS Version |
| TV | Samsung | 65” Series 7 | B8:B4:09:BA:22:94 | Tizen OS |
| TV | Samsung | 40” Series 6 | 00:7C:2D:2B:2E:95 | Tizen OS |
| amazon-device# | Amazon | Amazon Alexa | 90:F8:2E:78:61:FD | Fire OS 5.0 |
| TV | Samsung | 40” Series 6 | D0:03:DF:E8:B7:D1 | Tizen OS |

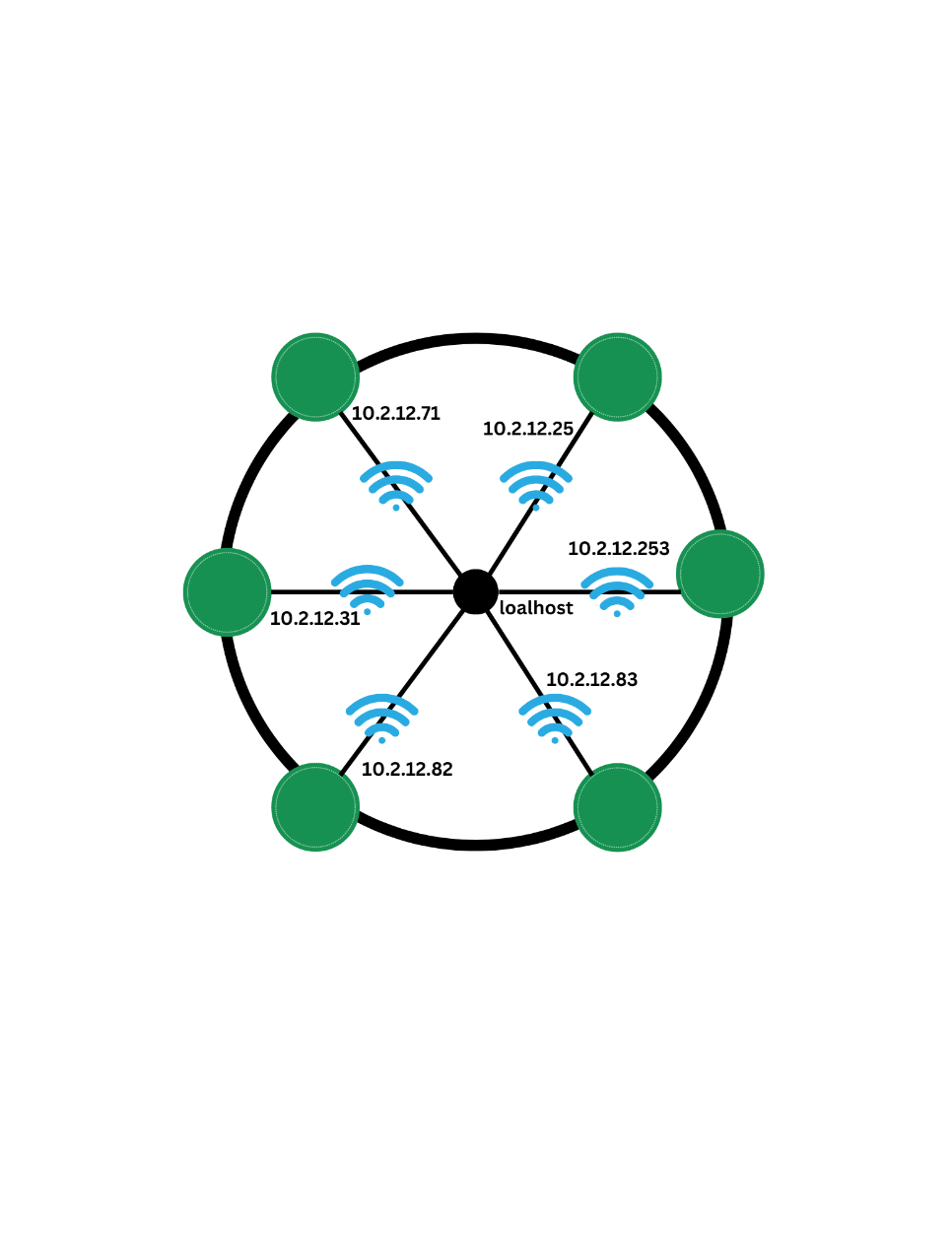
Total Device Count: 6

One thing to note is the naming convention of the devices, they are not uniform, and an attacker could simply name their device something similar and it would be hard to recognize. In the future a naming convention scheme will be considered for organizational purposes.

Utilizing an nmap network protocol scan a quick service investigation can be conducted.

Command: nmap -s0 10.2.12.1/24

A summary of the complexity of the network is displayed below:



A screenshot of a computer

Description automatically generated

Protocol Bundle:

Protocols used: HTTP/HTTPS, IMAP, TCP/UDP, SMTP, POP, ARP, DHCP.

Ports used: 22,23,53,80,111,443,49152,49153,49154,135,139,445,1042,1043,1236,2179,5357,1080,8888,8080,7676,32770,9100

Software:

This network uses the internet for educational and recreational purposes. All software listed is installed to windows 11 endpoints and is listed as Bundle-A in the NMAP inventory Table:

* Free
  + Windows Defender
  + TeamViewer
  + Nmap
  + Discord
  + Google Chrome
* Licensed
  + Microsoft Office 2019
  + VMware Workstation

In addition to the above software, a development software, Bundle-B is the following:

routinely used:

* VMWare
* Wireshark
* Snort
* Nmap
* Microsoft Teams
* Microsoft Office 2019
* Visual Studio Code
* Matlab
* Git
* OBS Studio

In addition to the above software, Bundle-C is the following:

routinely used:

* Netflix
* Hulu
* Prime
* Max
* Apple Music
* Peacock
* YouTube

In addition to the above software, Bundle-D is the following:

routinely used:

* Amazon Alexa Voice Service (AVS)
* Natural Language Processing (NLP) and Machine Learning (ML)
* Amazon Web Services (AWS)
* Echo Device Software
* Alexa Skills Kit (ASK)
* Wake Word Detection Software

In addition to the above software, Bundle-E is the following:

routinely used:

* iOS
* CoreML
* Siri
* Face ID
* Apple Secure Enclave
* iCloud
* App Store
* ARKit
* Handoff/Continuity
* Apple Pay

NMAP Inventory

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Host | Device | Software | NMAP- Details | NMAP-Ports/Protocols |
| 10.2.12.25 | Laptop | Bundle-A and Bundle-B | Hosts up: 6  Open ports: 21  Closed ports: 16264 | Protocol Bundle |
| 10.2.12.83 | Samsung Series 6 TV | Bundle-C | Hosts up: 6  Open ports: 21  Closed ports: 16264 | Protocol Bundle |
| 10.2.12.253 | Samsung  Series 6 TV | Bundle-C | Hosts up: 6  Open ports: 21  Closed ports: 16264 | Protocol Bundle |
| 10.2.12.82 | Samsung Series 7 TV | Bundle-C | Hosts up: 6  Open ports: 21  Closed ports: 16264 | Protocol Bundle |
| 10.2.12.31 | Amazon Alexa | Bundle-D | Hosts up: 2  Closed ports: 16264 | Protocol Bundle |
| 10.2.12.71 | iPhone | Bundle-E | Hosts up: 6  Open ports: 61  Closed ports: 16264 | Protocol Bundle |

## ****1.3 Glossary****

AP – Access Point: Device that allowed wireless devices to connect to a wired network using Wi-Fi, or related standards. The AP normally connects to a router (via a wired network) as a standalone device.

DHCP - Dynamic Host Configuration Protocol - a network management protocol used on Internet Protocol

GB – Gigabyte – 1000 megabytes IP – Internet Protocol Address – an address of a computer or other network device using TCP/IP.

IDS –Intrusion Detection System–a device or software application that monitors network or system activities for malicious activities.

IP –Internet Protocol Address –an address of a computer or other network device using TCP/IP.

LAN - Local area network

MB – Megabyte – 1000 kilobytes

NMAP – A network device and port scanner

MFA – Multi Factored Authentication, typically an email code, or a text message.

RAM – Random Access Memory.

KB – Windows OS Patches that generally contain fixes, improvements, or security updates.

TB – Terabyte – 1000 gigabytes

USB – Universal Serial Bus

WAN – Wide-area network

WEP – Wired Equivalent Privacy: Security algorithm for IEEE 802.11 wireless networks. Introduced in 1997.

WPA – Wi-Fi Protected Access: WiFi standard that provides greater service than WEP.

WPA2 – Wi-Fi Protected Access 2: Latest WiFi standard that provides greater service than WPA.

VPN –Virtual Private Network: A method employing encryption to provide secure access to a remote computer over the Internet.VM –Virtual Machine: An operating system OS or application environment that is installed on software which imitates dedicated hardware.

WPA2 –Wi-Fi Protected Access 2: Latest Wi-Fi standard that provides greater service than WPA.

# ****2********Management Overview****

This home network was configured by another organization but is now being managed by Madelyn Speers. The implementations and operations presented will be done by Madelyn Speers. The improvements and management suggested will be carried out within the next two months.

## ****2.1 Description of Implementation****

This network and the components that function with the network were established before the plan was created. It has been running fine for months, but there are aspects of the network that need to be improved or re implemented including high protection firewalls, OS upgrades, physical and software security implementations, as well as remote VPN access.

## ****2.2 Points-of-Contact****

|  |  |  |
| --- | --- | --- |
| Role | **Name** | **Contact Information** |
| All Roles (Network Administrator/Project Manager) | Madelyn Speers | 3155725645 / mspeers@usf.edu |

**Table 2.2 – Points-of-Contact**

## ****2.3 Major Tasks (Milestone 1 Task Consideration Documentation)****

Firewall:

To better improve network monitoring we can periodically check the network usage, open TCP connections, listening ports, and open processes by using the task manager setting and the resource manager tool. If something suspicious occurs, then the process can be suspended and blocked.

A screenshot of a computer

Description automatically generated

Whitelisting MAC addresses of approved devices will also be conducted to further increase security and remove unapproved devices off the network.

Resources: Free, 10-minute

Key Person: Madelyn Speers

Successful Criteria: Stricter firewall settings implemented

Anti-Virus:

The windows laptop endpoint on the network is already running Windows Defender, a free windows proprietary antivirus software. Other systems are not running any sort of antivirus software. Installing an antivirus software will allow for free improvements to endpoint security and enables routine scanning and web filtering based off their malicious URL database. Risks included with installing a new antivirus is it missing definitions, and ensuring it is up to date. All users will be taught to update the antivirus when the popup occurs.

Resources: Free, 10-minute install per endpoint

Key Person: Madelyn Speers

Successful Criteria: Antivirus is active and securing each endpoint

Data backup:

The existing network currently has no form of data backup. The Norton plan includes 50GBs of cloud storage that can be used as a backup for data such as, pictures, documents, and various other types of data that is important to the users. Additionally, an external 1TB hard drive can be purchase to store other sensitive/personal data in house. <https://www.amazon.com/Seagate-Portable-External-Hard-Drive/dp/B07CRG7BBH>

5 Seagate Backup 2TB External hard drives however would cost 180 dollars and would work for 5 users as well, being portable, physical and locally contained. The con is physical drives are likely to be stolen or break.

Both the local and remote back policies will be implemented

Resources: 180 dollars, 5 minute install per endpoint

Key Person: Madelyn Speers

Successful Criteria: Physical backups are enabled

## ****2.4 Implementation Schedule (Milestone 1 Task implementation Documentation)****

All changes will be logged and monitored once completed. This allows for a smooth transition to the new equipment and software.

* *Monitor Firewall and network traffic for suspicious activity across network*
* Download and install Norton Anti-Virus Security on other unprotected devices
* Purchase Seagate external 1TB hard drive

All changes and their status’s will be maintained and updated in the implementation schedule. Any tasks that are cancelled, rolled back, complete, or pending will be listed here.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Task | Start Date | End Date | Implementor | Rollback Plan | Status |
| Monitor Firewall and network traffic | 10/19/24 | 12/15/24 | Madelyn Speers | Set back Firewall rules to default | Pending |
| Downloading Anti-Virus Software | 10/19/24 | 10/19/24 | Madelyn Speers | Complete | Complete |
| Purchasing external hard drive for data backups | 10/19/24 | 10/19/24 | Madelyn Speers | Complete | Complete |

## ****2.5 Security and Privacy (Access Control Protections)****

The endpoints themselves however have windows implemented accounts with passwords and pin enablement. The iOS devices have PIN or facial recognition. This aspect of the network can be improved and will be continuously investigated and visited as security threats evolve. One potential implementation is mandatory MFA on all devices.

### **2.5.1 System Security Features**

* Passwords
* FaceID
* Voice recognition
* Operating System Updates
* Network monitoring
* Frontier firewall
* Antivirus software

### **2.5.2 Security Set Up During Implementation (Access Control Protections)**

This home network has no more than 5 concurrent end users, so the security implementation is as follows:

* All devices with sensitive information must have an encrypted drive, with username password authentication. External drives must also be encrypted.
* Devices that have no ability to use user authentication must be locked down to “guest” functionality. Meaning, it should have no access to sensitive data.
* Passwords must be strong (undecided) and changed periodically.
* All drives must be securely erased or destroyed if they are being sold or removed.

## 2.7 Open Issues

A few issues that need to be addressed later are:

1. Multifactor authentication
2. Approving/Removing devices to the network (Process creation)
3. Naming conventions of endpoints
4. Expanding guest access and controls
   1. What can guests do and not do
   2. How to control and share network resources like printers

# APPENDIX

## APPENDIX A: Approval

The undersigned acknowledge that they have reviewed the Madelyn Speers’ Home Network **Implementation Plan** and agree with the information presented within this document. Changes to this **Manageable Network Implementation Plan** will be coordinated with, and approved by, the undersigned, or their designated representatives.

|  |  |  |  |
| --- | --- | --- | --- |
| Signature: | Madelyn Speers | Date: | 10/19/24 |
| Print Name: | Madelyn Speers |  |  |
|  |  |  |  |
| Title: | Network Administrator |  |  |
| Role: | Project Manager |  |  |

## APPENDIX B: REFERENCES

The following table summarizes the documents referenced in this document.

|  |  |  |
| --- | --- | --- |
| **Document Name** | **Description** | **Location** |
| Amazon Seagae-Portable-External-Hard-Drive | 5 Seagate Backup 2TB External hard drive | <https://www.amazon.com/Seagate-Portable-External-Hard-Drive/dp/B07CRG7BBH> |
| Microsoft OS Builds | Lists OS builds and fixes to new windows updates | [September 30, 2021—KB5005611 (OS Builds 19041.1266, 19042.1266, and 19043.1266) Preview (microsoft.com)](https://support.microsoft.com/en-us/topic/september-30-2021-kb5005611-os-builds-19041-1266-19042-1266-and-19043-1266-preview-a37f5409-f320-4175-9a66-c2682fc11c07) |
|  |  |  |

## APPENDIX C: Milestone-1 Check-List

### Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts** **Risk**.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yes** | **No** | **Explanation** | **Accepts Risk** | **Milestone 1: Prepare to Document** |
| Yes |  | 1.2 |  | Do you have a way to document information about your network? |
| Yes |  | Weekly, updated Fridays 1.2 |  | Are you currently documenting all changes to your network? |
| Yes |  | 1.2 |  | Have you gone over the points to consider for this Milestone? |

*Checklist date: 10/19/24*

## APPENDIX D: Milestone-2 Check-List (Must be completed to reflect the state of your activity)

### Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts** **Risk**.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yes** | **No** | **Explanation** | **Accepts Risk** | **Milestone 2: Map Your Network** |
| Yes |  | Section 1.2.3 | Yes | Do you have a current, accurate network map? |
| Yes |  | Section 1.2.3  Checked every Friday | Yes | Do you have a current, accurate list of ALL devices on your network (or that ever connect to your network), that records host name, role, MAC address, service tag, physical location, OS/firmware, and responsible person/group?   * Total number of devices on your network, broken down by category (workstation/server/supporting/infrastructure/mobile/removable media)? * How often is this list checked for accuracy by using discovery tools? |
| Yes |  | Section 1.2.3 | Yes | Do you have a current, accurate list of ALL protocols that are running on your network? |
| Yes |  | Section Every Friday  7 Days | Yes | Are you updating your network map and lists of devices and protocols whenever a change is made to your network?  - When there is a change, how long before this documentation is updated? |
| Yes |  | Section 1.2.3, 2.5.2 | Yes | Have you gone over the points to consider for this Milestone? |

*Checklist date: 10/19/24*

## Milestone 3: Protect Your Network (Network Architecture)

### Overview

As outlined previously in section 2, the plan is to greatly enhance the security of this home network with both additional hardware and software. This includes a new wireless router, a dedicated hardware firewall and commercial antivirus software.

Currently, the host Windows 11 laptop is protected with the included Windows firewall and Avast free antivirus. Additionally, Malwarebytes anti-malware is installed, and manual scans are typically run weekly. While this has worked for the last two years and this network has not fell victim to a virus yet, it is certainly recognized that the security could be much improved.

### Facilities and Network Enclaves

The facility that accommodates this network is an apartment complex. Each apartment may have its own internal network for private devices (smartphones, computers, IoT devices). There are **VLANs** or isolated **subnets** for each apartment to prevent cross-communication between tenants while allowing internet access. There is an IDF room within the building that has multiple Cisco routers for the whole complex.

This IDF room is currently installed with a keypad lock, to prevent any unauthorized access to the network DSL modem, router, and hardware firewall.

The devices on this network are all contained within one room of the home that is configured as a bedroom with a key fob lock on the door.

The hardware is listed below and will be secured under lock and key in the above-mentioned IDF room within the complex.

#### Router

Cisco ISR 4331 Router

<https://www.cisco.com/c/en/us/support/routers/4331-integrated-services-router-isr/model.html>

Price: $700 - $1,200

Key Features:

* Security: Advanced security with IPSec VPN, SSL VPN, and firewalls. Supports WPA3 when used with compatible access points.
* Guest Network: Supports VLANs for network segmentation and secure guest access.
* VPN Support: Full VPN support (site-to-site, remote access).
* Performance: Dual-core processor, up to 100 Mbps throughput.
* QoS: Dynamic QoS to prioritize traffic (e.g., VoIP, video).
* Ports: Modular design with USB 3.0 ports and expandable interfaces.
* Management: Managed via Cisco Prime or Meraki (for Wi-Fi).

#### Hardware Firewall

Cisco Firepower 1010 Firewall

<https://www.cisco.com/site/uk/en/products/security/firewalls/firepower-1000-series/index.html>

Price: $500 - $1,000

Key Features:

* Security: Advanced threat protection with intrusion prevention, URL filtering, and malware defense.
* VPN Support: Full site-to-site VPN and remote access VPN (SSL and IPSec).
* Performance: Supports up to 1 Gbps firewall throughput and 750 Mbps VPN throughput.
* Management: Managed via Cisco Firepower Management Center or Cisco Defense Orchestrator.
* Ports: 8 x Gigabit Ethernet ports with flexible configurations.
* High Availability: Supports HA (High Availability) for redundancy.
* A diagram of a computer network

  Description automatically generated

### High-Value Network Assets

The following items are considered the high-value network assets for this home network due to their importance to the users and functionality of the network:

* Windows 11 Laptop
* Apple iOS 13
* Amazon Alexa
* Samsung Series 7 TV
* Samsung Series 6 TV
* Samsung Series 6 TV

The most important high-value item on this list as it relates to network connectivity is the Cisco router and firewall, as without this, there is no connection to the internet. It is for this reason that the complex has it secured.

The Cisco Router and the Cisco Firepower firewall are considered high-value network assets as well since they provide the additional sought security. Additionally, the Cisco router serves as a wireless access point for the wireless clients including laptops, tablets and smart phones. If these two devices were to fail, the network could be connected to the Cisco router and the wireless access re-enabled, to provide internet and LAN access until those devices can be replaced. This would certainly carry some security risks, as the hardware firewall would no longer be in the network.

The Windows 11 laptop is backed up weekly to an external hard disk and is the most critical machine now as it is utilized for college courses and contains the data associated with the course works. Currently the network only has a 3 mbps DSL connection to the Internet, as this is currently the only high-speed network service available. This limitation currently makes cloud back-up and storage an impractical solution. If a higher speed service becomes, available, cloud backup will be utilized as well. This network will rely on the physical external hard drive to restore data in the event of a laptop failure.

### Choke Points On This Network

The choke points of this network are primarily contained to the devices in the IDF room and would be the Cisco router and the Cisco Firepower firewall, which will be physically protected from intrusion by keypad door. The wireless access point is a function of the Cisco ISR 4331 and therefore is protected from physical tampering by being in the secured closet.

### Single Points of Failure

Single points of failure for this network are currently the Cisco ISR 4331 router as well as the Cisco Firepower firewall. There is a new spare router that is stored in the secured closet in the event that the installed unit fails. However, if the firewall itself fails outside the complex, there is currently no contingency plan for this event. There are no providers in this area for a backup as IT would have to travel from out of state.

One option would be to enable the "Hot spot" service on one of the smart phones to provide Internet connectivity to the wireless devices, however exceeding bandwidth caps would probably render this solution as cost prohibitive.

### Legacy Systems

There are currently not any legacy software or hardware systems to care for. If any of the current systems or software become unsupported, they will be documented within this section and evaluated to determine if they should remain as part of this network or if they can be eliminated.

### Plan Document Updates

If there are any architectural changes to the current network enclaves or choke points for this network, it will be the responsibility of Madelyn Speers to update this milestone to reflect such changes. This is to be performed within the five days of such changes.

## Milestone 4: Reach You Network (Device Accessibility)

### Overview

This section describes the accessibility and administration of devices on this network including all laptops, TVs, and mobile devices.

**Accessibility and Administration**

### Laptop Computers

The Windows 11 laptop is currently located in one room designated as the bedroom. There is only one administrative account, and it uses a complex password for the machine. This password will be changed monthly, and the password will be kept in the safe with the back-ups and Network Plan Document.

The admin account will be hardened with Windows Advanced Firewall protection, Norton Security, and any user accounts will be mandated to have complex passwords that require updating monthly. Windows automatic updates are enabled on each computer and Norton Security is to be configured so that users do not have the ability to disable it without administrative rights.

### Mobile Devices

Norton Security now offers protection for Android and iOS devices, therefore it will be installed on the Apple Ios 13 smart phone to provide host hardening.

### TVs

There is currently three TVs on this network and they are Samsung Series 6 and 7 TVs. Samsung periodically releases firmware updates to improve security and functionality. Updates can be applied via **Settings > Support > Software Update** or through a USB download from Samsung’s website. Both Series 6 and 7 TVs feature **Samsung Knox** to protect against malicious code and unauthorized access. Auto Update is enabled in the TV settings to ensure the latest security patches are applied automatically.

### Remote Administration

Remote administration for this network is not enabled autonomously at this time primarily because it is not necessary at the moment, and additionally to make the network more secure. Occasionally, if files or remote administration is required, we use the remote access software TeamViewer 10.

TeamViewer is utilized because it can provide the secure remote access that is needed on an occasional basis without having a remote administration tool running all of the time. It provides encryption that is base on RSA private/public key exchange and AES 256 bit session encryption. TeamViewer also provides two factor authentication and prevents man in the middle attack. It is important to note that TeamViewer generates a new required password each time a session is initiated.

This software is installed on the laptop provides remote access to files, remote control in the event it is necessary to help another user or work collaboratively and to provide remote administration capabilities.

### Physical Security

As described in Milestone 3, this network is installed within an apartment complex and all of the devices are currently located in one room of the home that is designated as the bedroom. The laptops and other mobile devices are used both in and out of the home.

The primary network components including the Cisco router and hardware firewall are all located in a secured IDF room with a locked keypad door.

### Automating Administration

At this point in time, this network does not have a server, which limits the automation of some of the administration tasks that could be handled by a centralized management system such as those that are contained within Microsoft Windows Server. Even without a centralized server this network will include the following policies to automate administrative tasks where possible.

* Enable Windows Update service on laptop and prevent users from disabling without administrative privileges.
* Enable automatic updating for the Norton Security product and prevent users from disabling without administrative privileges.

### Administrative Tools

The detailed processes above for each type of device will be managed the same. The password and security tools will be configured identically to ensure a consistent, standard process.

### Plan Document Updates

If there are any accessibility changes to the current network enclaves or changes to the security configurations for any device on this network, it will be the responsibility of Madelyn Speers to update this milestone to reflect such changes. This is to be performed within the five days of such changes.

## Milestone 5: Control Your Network (User Access)

### User Accounts

It is policy for this network that no user accounts will have admin access. There is an admin account built that currently is only accessed by the network administrator and owner. This account will only be used when necessary for maintaining the network and software. It is the policy of this network that the admin account will not be used for normal computing.

In the event a user needs elevated privileges for an application or other need, the network administrator must be informed and will make the decision on the necessity of the request. If deemed necessary, the administrator will enter the credentials at that time to proceed with the task.

As stated previously, there are only two users with actual accounts on this network at present time. This certainly makes managing users accounts and password policies easy to manage. There are guest accounts installed on each computer to provide internet access to family and guests, but these accounts only provide non-elevated access to the network and Internet.

### Privileged accounts

The privileged user account (admin) on this network will be used strictly for network and computer administration. The admin account is not to be used for general purpose computing, specifically web browsing and email access. This is to help prevent malicious attacks from email attachments and malicious mobile code that could be encountered at external websites.

### Least privilege administrative model

Although this network does not yet include a server, the plan is to eventually add one. It will be the policy of this network that all users will, and groups will be managed so that the principles of the least privilege model will be followed. That is to say that groups and users will be managed so that the user will only have access to applications, data, and data structures that are directly pertinent to their role and requirements.

### Users Installing Software

There are currently no users on this network that have elevated/privileged accounts except for the designated admin account. This prevents all users from having the ability to install software without the approval and assistance of the administrator.

### Expiration Dates On Accounts

There are not currently an expiration dates on accounts since there are so few at this point in time. If more users are on-boarded to the network, then this section will be updated to reflect any new policies that are created regarding account expirations. It will be policy that accounts are reviewed at a minimum of every six months to determine if any accounts need to be deleted.

### Plan Document Updates

If there are any changes or additions to the users of the network, it will be the responsibility of Student-Name to update this milestone to reflect such changes. This is to be performed within the five days of the changes.

## Milestone 6: Manage Your Network, Part I (Patch Management)

Vulnerable devices on a network are often used as entry points for dangerous network attacks. Actively managing your network devices in a few areas can dramatically improve your security; this milestone and the next are focused on setting up these management areas. Note that specific implementations will differ for different device roles and operating systems. Note also that truly *effective* management of these areas relies on the previous milestones being completed.

### To Do

 Establish a patch management process for ALL the operating system and application software on EVERY device on your network (workstations, servers, supporting devices such as printers, infrastructure devices such as routers and firewalls, and mobile devices such as laptops and smartphones).

* Suggestion: Prioritize your patch management. All of your systems should be patched regularly, but those systems and applications that handle data from untrusted sources (such as the Internet) must be patched more often. In addition, critical patches must be applied whenever they are released. The sensitivity and criticality of certain systems may warrant exceptions, however. If you make exceptions, be sure that those systems are isolated as much as possible and monitored closely for signs of known attacks.
* Consider: Patching your laptops and other mobile devices may be difficult, because they may not be regularly connected to your network. The plan to administer these devices (developed in Milestone 4) should include regular patching. Alternatively, consider using a network access control solution, to make sure that these devices are up to date before being allowed access to your network resources (see the *Network Access Control* Network Security Task).
* Suggestion: As much as possible, patching should be automatic. Remember that a reboot may be required for a patch to be properly applied. Be careful patching your servers, however, so they don’t all reboot at once and affect your network availability.
* Suggestion: As with any software, patches and updates should be verified to come from authorized or trusted sources, and tested so that they do not interfere with the proper functioning of your network. To harmonize this with the automatic patching suggestion above, consider automatically deploying first to a small, isolated subnet for testing (but be sure this testing reflects actual application usage!), and then to the rest of the network either after approval from the testing group, or after a brief time period with no problems found. Deploying patches in a tiered manner such as this also prevents your support personnel from being flooded with calls if something goes wrong.
* Suggestion: For the Windows operating system and Microsoft applications, use Windows Server Update Services (WSUS) or an automated commercial solution. Windows workstations should be set to automatically apply patches. For operating systems other than Windows, consider using Puppet, Spacewalk, or custom scripts.
  + For more information on WSUS, see [http://technet.microsoft.com/en-us/wsus/default.](http://technet.microsoft.com/en-us/wsus/default)
  + For more information on Puppet, see [www.puppetlabs.com.](http://www.puppetlabs.com/)
  + For more information on Spacewalk, see [http://spacewalk.redhat.com.](http://spacewalk.redhat.com/)
* Suggestion: Review after patching your systems, to verify that the patches were applied correctly. As a sanity check, use different tools than those used for pushing out the patches.
* Suggestion: For additional recommendations on patch management, see NIST Special Publication 800-40: “Guide to Enterprise Patch Management Technologies” (Available at [http://csrc.nist.gov/publications/)](http://csrc.nist.gov/publications/).

### Documentation

**1. Device: Dell Laptop**

* **Patch Frequency:** Patches should be applied monthly or as new critical patches are released.
* **Patch Download and Verification:** Patches are downloaded through the Dell Update Utility or manually through Dell’s website. Ensure patches are verified by checking their signatures.
* **Patch Application:** Patches should be applied automatically using Dell Update or manually if required.
* **Manual Patches:** If automatic patching fails, patches can be manually applied using Dell’s support site, ensuring the version matches the laptop's model.
* **Patch Verification:** Using the Dell Update Utility to verify that patches have been applied successfully.
* **Exceptions:** Any Dell hardware beyond warranty with no support for updates should be retired from the network. If needed, the security risk is mitigated by isolating such devices from critical systems.

**2. Device: iPhone**

* **Patch Frequency:** Apply patches automatically as part of iOS updates, which typically occur monthly or in response to critical vulnerabilities.
* **Patch Download and Verification:** Patches are downloaded automatically or manually from Settings > General > Software Update. Verification is done via Apple’s digital signatures.
* **Patch Application:** Automatically through the iOS update system.
* **Manual Patches:** If automatic updates are disabled, manually check for updates via the Settings app.
* **Patch Verification:** Verify the update has been applied by checking the device’s version after installation.
* **Exceptions:** Devices that cannot update to the latest iOS version due to hardware limitations should be considered for replacement or isolated in a secure network segment.

**3. Device: Samsung TVs (Series 6 & 7)**

* **Patch Frequency:** Apply firmware updates at least once every 3-6 months or as new updates are released.
* **Patch Download and Verification:** Firmware updates are typically downloaded directly through the TV’s software interface. The update’s authenticity is ensured by verifying the source as Samsung’s official servers.
* **Patch Application:** Updates can be applied manually through the TV's settings menu or automatically if enabled.
* **Manual Patches:** If automatic updates are disabled, manually check for updates in the settings.
* **Patch Verification:** Ensure the update is applied by checking the firmware version in the TV’s system information.
* **Exceptions:** Any Samsung TV models no longer supported by firmware updates should be considered for replacement. For older models, minimize exposure to untrusted networks.

**4. Device: Amazon Alexa**

* **Patch Frequency:** Alexa devices should update automatically, but the update schedule can be set to every 2-4 weeks or as critical updates become available.
* **Patch Download and Verification:** Patches are automatically downloaded from Amazon’s cloud service. Their authenticity is ensured by Amazon’s digital signature.
* **Patch Application:** Updates occur automatically in the background with no manual intervention required.
* **Manual Patches:** If automatic updates are not functioning, Alexa devices can be manually restarted to force an update check.
* **Patch Verification:** The device's software version can be checked through the Alexa app or the device settings.
* **Exceptions:** If there are devices that no longer receive updates, they should be replaced, or their access to the internet should be restricted.

**5. Non-Microsoft Updates (e.g., Adobe Acrobat, Browsers)**

* **Patch Frequency:** Check for updates monthly or when critical updates are released.
* **Patch Download and Verification:** Use each application’s built-in update mechanism or a third-party patch management tool like WSUS or a package manager like Chocolatey.
* **Patch Application:** Automatic for most applications (Adobe, browsers) or manual installation.
* **Manual Patches:** If automatic updates fail, manually download patches from trusted sources like Adobe’s website or the browser vendor's site.
* **Patch Verification:** After installation, check the version in the application’s About menu to confirm the patch.
* **Exception:** Some applications might not support updates due to EOL. In these cases, ensure they are isolated or removed. Regular security scans can mitigate vulnerabilities from unpatched software.

**6. End-of-Life (EOL) Software/Hardware**

* **Action:** Any EOL software or hardware should be replaced or removed immediately from the network. If replacement isn't feasible, consider using virtualization or a containerized environment with strict access control to minimize risk.
* **Mitigation:** Implement network segmentation or firewall rules to isolate EOL systems from sensitive resources.

**7. Using Virtualization**

* **Action:** Centralized patching of virtual machines and containers should be considered. This can allow patches to be tested and rolled out more efficiently, reducing the overhead of applying patches to each individual device.
* **Mitigation of Downtime:** Schedule patches during off-hours, ensuring minimal service disruption.

**8. Update Administrative Tools**

* **Patch Frequency:** Admin tools like nmap, Wireshark, and other security management tools should be updated monthly or whenever a critical update is released.
* **Patch Verification:** Ensure these tools are always running the latest versions by regularly checking their official websites or repository for updates.
* **Exceptions:** If administrative tools cannot be updated due to compatibility issues, they should be replaced, or mitigation measures like sandboxing and increased monitoring should be implemented.

### Ongoing

* Continue to execute the patch management process that you established in this Milestone.
* As necessary, update your patch management process and documentation.

## Milestone 7: Manage Your Network, Part II (Baseline Management)

### To Do

* Create a list of all the applications that are approved for use on your network. For each application, specify its name and specific version, the reason it was approved, the network ports and protocols it uses (if applicable), and whether it is approved for general use or only within specified enterprise functions.
* Establish the criteria and process for getting an application on the approved list.
  + Suggestion: The reason for having an application on the approved list should never be just

“Because so-and-so wants it.” The application should always be justified by a business case, like “We need Adobe Flash on our Internet-connected boxes because our clients’ websites use it.”

* + Suggestion: Before an application is added to the approved list, it should be researched for any security issues. Consider how much you trust the application’s developers—and their subcontractors—to deliver a product with no code from questionable sources and with a minimum of vulnerabilities. In addition, consider whether the application conflicts with any of your existing security policies, and how easily it can be updated.
  + Suggestion: Before an application is added to the approved list, it should be tested to make sure that it does not do anything malicious, that it works with the other applications in the baseline, and that it won’t interfere with your network. Consider setting up a small, isolated subnet for this testing.
  + Suggestion: Once an application is added to the approved list, your patch management process from Milestone 6 will need to be updated appropriately.
  + Suggestion: Implement restrictions so that only those applications that have been approved are allowed to execute on your network. Consider using application whitelisting (see the *Executable Content Restrictions* Network Security Task).
* Create device baselines (including for infrastructure devices and mobile devices). All software applications in a device baseline should be from the approved list for that device. Note that virtual machines and thin clients need baselines as well.
  + Suggestion: If similar devices are used in environments that require different capabilities or pose different threats, the devices should have different baselines. For example, the workstations used by developers should have a different baseline than those used by managers, because the managers will most likely not require all the applications and privileges that the developers will. Having more “special purpose” machines and less “general” machines will limit the damage that can be done if a machine is compromised.
  + Suggestion: When creating your device baselines, be sure to “harden” them by implementing the recommended security guidance for those devices. All software included in the baselines should be fully patched and correctly and securely configured. Remove unneeded components from default installs, disable unnecessary services, and change default (and blank) passwords to prevent their use by malware. Limit the number of cached credentials, implement screen lock timeouts, disable Windows auto-run, etc. In addition, be sure that your patch management process from Milestone 6 covers all software in your baselines.
    - **Securing Web browsers.** Properly securing the Web browsers in your workstation baselines is extremely important: the Internet can be a dangerous place!
      * For suggestions on securing Internet Explorer, Firefox, Safari, and other Web browsers, see [www.us-cert.gov/publications/securing-your-web-browser.](http://www.us-cert.gov/publications/securing-your-web-browser) In addition, consider minimizing the number of plug-ins in the browser, as these might contain security vulnerabilities.
      * For guidance on Google Chrome, see NSA’s “Deploying and Securing Google Chrome in a Windows Enterprise” (Available at [www.nsa.gov/ia/mitigation\_guidance/security\_ configuration\_guides/applications.shtml)](http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/applications.shtml).
    - The Microsoft Baseline Security Analyzer (MBSA) can be used to scan for security misconfigurations in your Microsoft baselines before deploying them. For more information on MBSA, see [http://technet.microsoft.com/en-us/security/cc184924.aspx.](http://technet.microsoft.com/en-us/security/cc184924.aspx)
    - The Center for Internet Security ([http://cisecurity.org)](http://cisecurity.org/) provides benchmarks and tools for checking that your operating systems, applications, and devices (including Windows, Linux, Solaris, Apple, Oracle, Cisco, etc.) are configured securely.
    - For additional configuration guidance, see the following:
      * NSA configuration guides ([www.nsa.gov/ia/mitigation\_guidance/security\_configuration\_guides/index.shtml)](http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/index.shtml)

|  |  |  |
| --- | --- | --- |
| –  –  – | NIST National Checklist Program ([http://web.nvd.nist.gov/view/ncp/information)](http://web.nvd.nist.gov/view/ncp/information)  DISA Security Technical Implementation Guides (STIGs) ([http://iase.disa.mil/stigs/index.html)](http://iase.disa.mil/stigs/index.html)  US Government Configuration Baseline (USGCB, formerly FDCC) ([http://usgcb.nist.gov)](http://usgcb.nist.gov/) |  |
| Page 19 of 39 | INFORMATION ASSURANCE DIRECTORATE | 11/27/2013 |

### Documentation

#### Approved Application List for Dell Laptop (Windows OS)

**Applications**:

1. Microsoft Office 365 – For business productivity (Word, Excel, PowerPoint, Outlook).
2. Google Chrome – For web browsing.
3. Adobe Acrobat Reader – For PDF document viewing and editing.
4. Discord – For team communication, collaboration, and community management.
5. Microsoft Teams – For team communication, collaboration, meetings, and file sharing.

**Criteria for Approval**:

1. Must serve an essential business function (e.g., communication, productivity, security).
2. Applications should be compatible with the organization's baseline configuration (e.g., Windows OS version).
3. Proven track record for security and regular updates.
4. No conflicts with existing software or network policies.
5. Must meet internal security requirements (e.g., data encryption, secure communication protocols).

**Process for Approval**:

1. Request: End users submit a request to IT with the application’s business use case.
2. Security Evaluation: IT performs a security check for vulnerabilities, developer trustworthiness, and potential compatibility issues.
3. Testing: The application is tested in a controlled, isolated environment to ensure it functions without issues.
4. Approval: Once tested, IT approves the app and adds it to the approved list.
5. Deployment: The app is deployed to devices via a patch management system.
6. Ongoing Maintenance: Ensure continuous updates, security patches, and the removal of unapproved versions.

**Approved Application List for iPhone (iOS)**

**Applications:**

1. Safari – Default web browser for browsing the internet securely.
2. Outlook – For email management and calendar integration with enterprise systems.
3. Microsoft Teams – For team communication, collaboration, meetings, and file sharing.
4. Instagram – Social media platform for business marketing, branding, and communication.
5. Snapchat – Social media platform for messaging and marketing purposes.
6. Facebook – Social media platform for business networking and communication.

**Criteria for Approval:**

1. Business Use: Each application must serve a clear and specific business or communication purpose (e.g., Microsoft Teams for business collaboration, Outlook for email management).
2. Security and Privacy: Applications must be secure, with strong data encryption, user authentication, and compliance with enterprise privacy policies (e.g., GDPR, CCPA).
3. Compatibility: Applications must be compatible with iOS versions deployed within the organization and must not conflict with existing security solutions.
4. Regular Updates: The app developers must regularly release security patches and updates to address vulnerabilities.
5. Network Compliance: Applications must not compromise the security of the network or interfere with other devices’ operations (e.g., avoid apps that require unnecessary open ports).
6. External Communication Platforms: For social media apps like Instagram, Snapchat, and Facebook, the usage must be business-focused (marketing, customer communication) and adhere to corporate communication guidelines.

**Process for Approval:**

1. Request: Employees or departments submit requests for new applications through IT support channels with a justification for their business need.
2. Security Assessment: IT assesses the security features of the app, including any risks related to unauthorized access, data leakage, and compliance with internal security standards.
3. Testing: Applications are tested in a controlled environment, ensuring that they function properly without compromising security or network stability.
4. Approval: After testing, IT approves the app for use, adding it to the official list of approved applications for the iPhone.
5. Deployment: The application is made available to the end users via the Mobile Device Management (MDM) system, ensuring compliance with organizational policies.
6. Ongoing Maintenance: IT ensures that applications are updated with security patches and that unapproved versions are promptly removed. Periodic reviews are done to ensure the app remains compliant with security policies.

**Approved Application List for Samsung TVs (Series 6 & 7)**

**Applications**:

1. Samsung Smart Hub – Interface for managing apps, streaming services, and connected devices.
2. YouTube – Video streaming service.
3. Netflix – Video streaming service.
4. Amazon Prime Video – Video streaming service.

**Criteria for Approval**:

1. Must serve an essential business or entertainment function.
2. Should not pose a security risk by exposing unnecessary services or data.
3. Regular updates to fix bugs and security vulnerabilities.
4. Must comply with security policies (e.g., authenticated access, encryption).

**Process for Approval**:

1. Request: Request approval for any apps not pre-installed or essential for the business.
2. Security Review: Check whether the app exposes the TV to security risks, such as unauthorized data access.
3. Testing: The app is tested to ensure it integrates seamlessly with the Smart Hub interface.
4. Approval: After successful testing, the app is approved for installation on corporate TVs.
5. Ongoing Monitoring: Regular review of apps for updates or vulnerabilities.

**Approved Application List for Amazon Alexa**

**Applications**:

1. Amazon Music – Music streaming service.
2. Spotify – Music streaming service.
3. News Briefing – Provides daily news updates and briefings.

**Criteria for Approval**:

1. Must be necessary for business productivity, communication, or entertainment.
2. Should not expose sensitive data (e.g., audio recordings) or violate privacy policies.
3. Compatible with the enterprise network and security policies.
4. Regular updates to enhance functionality and patch security vulnerabilities.

**Process for Approval**:

1. Request: End users must submit a request for specific Alexa skills or apps.
2. Security Review: Assess if the skill or app could create security or privacy risks.
3. Testing: Test functionality and ensure it integrates properly with other systems (e.g., calendar or messaging systems).
4. Approval: After testing, the skill is approved and installed.
5. OngoingMonitoring: Skills are regularly reviewed for updates and deprecation.

**Device Baselines**

**Dell Laptop (Windows OS)**

* **Hardware Baseline**:
  + Dell laptop with 16 GB RAM, 454 GB SSD, and Intel i7 processor.
  + Secure BIOS settings: Secure Boot enabled, USB ports disabled in BIOS, boot order restricted to internal hard drive.
  + Full disk encryption (BitLocker).
  + Network adapters configured to use secure protocols (e.g., WPA2 for Wi-Fi).
* **Software Baseline**:
  + Operating System: Latest Windows 11 version with all security patches applied.
  + Installed Applications: Only approved software listed above.
  + Security Configuration: Local admin accounts disabled, screen lock timeout set to 10 minutes, and automatic updates enabled.
  + Patch Management: Regularly updated via Windows Update and third-party patch management solutions.

**iPhone (iOS)**

* **Hardware Baseline**:
  + iPhone with iOS version 18 or later.
  + Secure settings: Face ID or Touch ID enabled for authentication; device encryption enabled.
  + Disabling of unnecessary Bluetooth or Wi-Fi services when not in use.
* **Software Baseline**:
  + Operating System: Latest version of iOS with security updates enabled.
  + Installed Applications: Only approved apps listed above.
  + Security Configuration: Device password policy enforced; automatic updates enabled.
  + Patch Management: Managed via Apple’s MDM system for updates and app installations.

**Samsung TVs (Series 6 & 7)**

* **Hardware Baseline**:
  + Each TV is connected to the network via secure Wi-Fi or Ethernet.
  + Disabling of unused ports (e.g., USB) and services (e.g., Bluetooth) when not in use.
* **Software Baseline**:
  + Firmware: Latest Samsung Smart Hub firmware version.
  + Installed Apps: Only approved streaming services (YouTube, Netflix, etc.).
  + Security Configuration: Strong authentication for device access and app installation. Limit unnecessary remote control access.
  + Patch Management: Automatic updates enabled for firmware and apps.

**Amazon Alexa**

* **Hardware Baseline**:
  + Alexa devices secured with device passwords and placed in secure areas to limit physical access.
  + Ensure no external unauthorized devices are connected.
* **Software Baseline**:
  + Firmware: Latest Alexa software version.
  + Installed Skills: Only approved entertainment skills.
  + Security Configuration: Voice ID enabled for secure access to sensitive tasks, device linked to secure Wi-Fi network.
  + Patch Management: Regular skill and firmware updates through Amazon’s management platform.

### Consider

* **Backing up offline.** Backup your baselines and store them offline. An adversary who gains access to network copies of your baselines may modify them.
* **Same password problem.** If you use an application to clone or “ghost” the same baseline image to multiple machines, keep in mind that every machine baselined this way will have the same local administrator/root account *and password*. Without ever having to crack the password, an attacker using a pass-the-hash technique could use the same password *hash* to compromise all your machines. If you consider this risk of compromise to be greater than the administrative overhead, either disable the local admin accounts or manually change all the passwords.
  + Suggestion: If you manually change all the passwords, *do not* store them in a file or e-mail on the network! Instead, use a simple algorithm to generate each password. For example, append the last few characters of the machine name to the original common password. This way your admins know all the passwords, but the password hashes are different across all your machines. This makes the pass-the-hash attack ineffective. It is not a foolproof solution, but it is better than all of your machines having the same password!
  + Suggestion: For more information on pass-the-hash attacks and step-by-step guidance for mitigations, see Microsoft’s “Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques” [(www.microsoft.com/en-us/download/details.aspx?id=36036)](http://www.microsoft.com/en-us/download/details.aspx?id=36036). For expanded implementation guidance including scripts to use on a Windows network, see NSA’s “Reducing the Effectiveness of Pass-the-Hash” (Available at [www.nsa.gov/ia/mitigation\_guidance/security\_ configuration\_guides/applications.shtml)](http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/applications.shtml).
* **Verify device integrity.** On a regular basis, use system integrity checking tools to verify the integrity of the baseline installs on your devices. This is very important to discover any unauthorized changes. If possible, automate these integrity checks. In addition, consider periodically reimaging your devices, to ensure compliance. An added benefit of reimaging is that it will encourage your admins to document system changes and fixes, so they don’t have to “rediscover” them after the devices have been reimaged. Be careful that reimaging does not lead to unacceptable user disruption or data loss, and that any host-based security still performs properly on the reimaged devices.
  + Suggestion: As part of verifying that no unauthorized software is present on your devices, do regular checks for malware (see the *Virus Scanners and Host Intrusion Prevention Systems* Network Security Task).
* **Automatic reboots.** Consider setting your workstations to automatically reboot on a regular basis (for example, every night) to keep any small problems from accumulating, clear up any memory issues, etc. Consider scheduling a server task to reboot all your workstations remotely; having this task on the server allows it to be easily adjusted for special situations, instead of having to modify a script on each individual machine. Be careful that rebooting does not lead to user disruptions (for example, if someone is working late), hardware failure, or data corruption if a process is interrupted.
* **Hardware configurations.** Do the baselines for your devices also include their hardware configurations? Some things to consider in this area might be disabling wireless cards, setting the boot order in the BIOS to hard drive only, and creating BIOS passwords. In addition, make sure that your systems support signed BIOS updates (check with your vendor), to help prevent unauthorized BIOS modifications.
  + Suggestion: Limit your hardware based on the capabilities needed and the threats posed. For example, not all of your laptops may need built-in microphones, cameras, and wireless capability. Not all of your workstations may need USB ports, huge hard drives, powerful graphics cards, and CD/DVD writers. (As a bonus, this may reduce your power and cooling requirements!)
* **Supply chain risk management.** Your supply chain is everything and everyone involved in getting products, systems, and services to your organization. It impacts the full system development life cycle, from R&D and acquisition to disposal. The modern IT supply chain is complex and international, and subject to a variety of threats such as counterfeiting, tampering, theft, and the introduction of unwanted functionality and malicious content. Consider how your organization will deal with these risks. For more information and a set of best practices, see NIST IR 7622: “Notional Supply Chain Risk Management Practices for Federal Information Systems” (Available at [http://csrc.nist.gov/publications/)](http://csrc.nist.gov/publications/).

### Ongoing

* Update your device baselines on a regular basis. As far as possible, baselines should contain the latest versions of operating system and application software. Baselines should never contain software or hardware that is end-of-life and no longer supported.
* Update your approved application list, criteria and process for getting an application on the approved list, and baselines documentation whenever there is a change.
* From now on, whenever a device is added or replaced on your network, the new device should conform to the appropriate baseline. If the device cannot be wiped and re-baselined, consider a network access control solution (see the *Network Access Control* Network Security Task), or quarantining the device.
* As time permits, any installed applications and services that are not approved should be removed from the network.
* As time permits, reimage current devices with the appropriate baseline.

## Milestone 8: Document Your Network

As time permits, your processes and procedures for your network should be documented. This helps keep your network manageable. Even if you only have time to document one process per week, that’s still better than nothing! Be sure to give priority to documenting those things that are most important to keeping your organization doing business.

### Documentation

**Procedures for Rebuilding Servers and Devices**

**Dell Laptop:**

Rebuilding Process:

* 1. Restore from Backup: Use your backup solution to restore essential user files and settings.
  2. Reinstall Operating System: Use Windows 11 installation media to reinstall the OS.
  3. Install Drivers: Download and install necessary drivers from Dell’s support page.
  4. Apply Patches: Ensure the latest security patches are applied.
  5. Install Applications: Install the approved applications list (e.g., Microsoft Teams, Discord).
  6. Network Reconnection: Configure VPN settings and network access.
  7. Security Configuration: Ensure BitLocker encryption is active, Windows Defender is enabled, and firewall settings are correct.

**iPhone:**

Rebuilding Process:

* 1. Restore from iCloud Backup: Restore user data from the most recent backup.
  2. Reinstall Apps: Download apps from the App Store (e.g., Outlook, Teams).
  3. Update iOS: Ensure the iPhone is running the latest iOS version (18).
  4. Reconfigure Email & Accounts: Set up email (e.g., Outlook).
  5. Security Configuration: Ensure that Face ID, strong passwords, and remote wipe are enabled.

**Samsung TVs (Series 6 & 7):**

Rebuilding Process:

* 1. Factory Reset: Perform a factory reset through the settings menu.
  2. Reinstall Apps: Reinstall required apps (e.g., Netflix, Amazon Prime).
  3. Update Firmware: Check and apply any available firmware updates.
  4. Network Reconnection: Reconnect TV to Wi-Fi or Ethernet.
  5. Security Configuration: Disable unused services (e.g., Bluetooth) and ensure the TV is not accessible outside the internal network.

**Amazon Alexa:**

Rebuilding Process:

* 1. Factory Reset: Hold the reset button to reset the device to factory settings.
  2. Reconfigure Wi-Fi: Reconnect Alexa to the Wi-Fi network.
  3. Reinstall Skills: Add approved skills from the Alexa app.
  4. Security Configuration: Enable two-factor authentication (2FA) for the Amazon account linked to Alexa.

**Administrative Processes and Procedures**

How to Add a New User:

1. User Request: New users are added via an internal ticketing system. Approval from HR or department leads is required.
2. Account Creation: Create the user’s profile in the Active Directory (for Dell laptops) or Apple ID (for iPhone). Assign the appropriate roles and permissions.
3. Assign Software: Install the approved applications (Microsoft Teams, Discord, Outlook, etc.) based on the user’s role.
4. Network Access: Ensure VPN, Wi-Fi, and file share access are configured.

How (and When) to Remove a User:

1. User Deactivation: Disable the user’s account in Active Directory and services (e.g., Microsoft 365, Teams).
2. Data Handling: Archive emails and files to secure cloud or physical storage.
3. Revoke Access: Remove access to all systems and devices.
4. Device Handling: Wipe Dell laptop, iPhone, or other devices and reassign or dispose of them securely.

How to Add a New System:

1. System Procurement: Document system specs (e.g., Dell laptop model, iPhone version, Samsung TV model).
2. Installation:
   * Dell Laptop: Install Windows OS, security software (antivirus), and necessary patches.
   * iPhone: Set up as new or restore from backup.
   * Samsung TVs: Set up network configurations and install necessary apps.
   * Amazon Alexa: Connect to Wi-Fi and configure the device in the Alexa app.
3. Security Configurations: Follow the baseline security guidelines, including enabling encryption and securing admin accounts.

How to Remove a System:

1. Decommissioning:
   * For Dell laptop, wipe hard drive and remove from the network.
   * For iPhone, wipe the device and unlink from the Apple ID.
   * For Samsung TVs, perform factory reset.
   * For Amazon Alexa, perform a factory reset.
2. Remove Access: Ensure the system is removed from any network or VPN configurations.

**Completeness of Documentation**

* Avoid Single Points of Knowledge: Ensure all knowledge is documented, even for tasks that may seem obvious.
* Review: Regularly review documentation to ensure its up-to-date and understandable.

**Hard Copy Storage and Redundancy**

* Primary Storage: Store hard copies of the recovery and administrative process documents in a fireproof safe or secure offsite location.
* Secondary Storage: Keep backup copies in a cloud-based, encrypted system.
* Remote Access: Remote access to essential documentation.

**Documentation Ownership and Enforcement**

* Ownership: Regularly update documentation and ensure it’s followed.

### Consider

* **Completeness.** Consider the following scenario to determine if your documentation is complete and up-to-date: Suppose one of your most knowledgeable admins cannot be contacted for an extended period of time. Will your network grind to a halt? Will it explode in chaos? What does that admin know that is not written down? To test if you’ve thought of everything, have that admin go on vacation… (Incidentally, “job security” is not a valid reason for not documenting!)
* **Hard copy.** Keep hard copies of your processes and procedures on hand, in case of emergencies. Keep duplicate copies at your continuity of operations site, in case of more serious emergencies.
* **Always followed.** The documented procedures should always be followed. Are they? Are new network admins required to become familiar with and use this documentation?

### Ongoing

* As time permits, continue to document your administrative processes and procedures.
* All documentation must be reviewed periodically (for example, annually) and updated as necessary. Consider occasionally hiring a technical writer to gather, clarify, and maintain your documentation.

APPENDIX

### *APPENDIX A: Manageable Network Implementation Plan Approval*

The undersigned acknowledge that they have reviewed the **Spotswood** **Implementation Plan** and agree with the information presented within this document. Changes to this **Manageable Network Implementation Plan** will be coordinated with, and approved by, the undersigned, or their designated representatives.

Signature: Date: 11/11/24

Madelyn

-

Speers

Network Owner

Project Manager

Print Name: Title: Role:

### *APPENDIX B: REFERENCES*

*The following table summarizes the documents referenced in this document.*

|  |  |  |
| --- | --- | --- |
| **Document Name** | **Description** | **Location** |
| Madelyn Speers Manageable Network Plan | Manageable Network Plan for Madelyn Speers’ home network | Digital copy also stored on Google drive cloud storage |
|  |  |  |
|  |  |  |

### *APPENDIX C: System Hardware Inventory*

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Name/ ID | Type | Model/ Version | Physical Location | Equipment  Owner  (Person or  Dept) | Maintenance Contract?  Y/N | Maintenance  Contact  Point | Maintenance Type/ Level of Coverage | Maintenance  Period  Expiration  Date | Required Licenses |
| Cisco ISR 4331 | Enterprise Router | ISR 4331/K9 | IDF room | Apartment  Complex | Yes | Cisco TAC | Smart Net Total Care / 24x7 | Unknown | Cisco DNA, Security licenses |

### *APPENDIX D: System Software Inventory*

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Name/  ID | Type | Model/ Version | Physical Location | Equipment  Owner  (Person or  Dept) | Maintenance Contract?  Y/N | Maintenance  Contact  Point | Maintenance Type/ Level of Coverage | Maintenance  Period  Expiration  Date | Required Licenses |
| Cisco Firepower 1010 | Enterprise Firewall | FPR1010-NGFW-K9 | IDF room / office | Apartment  Complex / IT department | Yes | Cisco TAC | Cisco Smart Net / 24x7 | Unknown | Threat Defense, Malware license |

### *APPENDIX E: Milestone-1 Check-List*

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **AcceptsRisk**.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yes** | **No** | **Explanation** | **Accepts Risk** | **Milestone 1: Prepare to Document** |
| X |  |  | Yes | Do you have a way to document information about your network? |
| X |  | This is the initial creation of this network plant. All future changes to the network shall be documented at the time of the change | Yes | Are you currently documenting all changes to your network? |
| X |  |  | Yes | Have you gone over the points to consider for this Milestone? |

*Checklist date: 11/11/24*

### *APPENDIX F: Milestone-2 Check-List*

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **AcceptsRisk**.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yes** | **No** | **Explanation** | **Accepts Risk** | **Milestone 2: Map Your Network** |
| X |  |  | Yes | Do you have a current, accurate network map? |
| X |  |  | Yes | Do you have a current, accurate list of ALL devices on your network (or that ever connect to your network), that records host name, role, MAC address, service tag, physical location, OS/firmware, and responsible person/group?   * Total number of devices on your network, broken down by category   (workstation/server/supporting/infrastructure/ mobile/removable media)?   * How often is this list checked for accuracy by using discovery tools? |
| X |  |  | Yes | Do you have a current, accurate list of ALL protocols that are running on your network? |
| X |  | This is the initial creation of this network plan. All future changes to the network shall be documented at the time of the change | Yes | Are you updating your network map and lists of devices and protocols whenever a change is made to your network?  - When there is a change, how long before this documentation is updated? |
| X |  |  | Yes | Have you gone over the points to consider for this Milestone? |

*Checklist date: 11/11/24*

### *APPENDIX G: Milestone-3 Check-List*

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **AcceptsRisk**.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yes** | **No** | **Explanation** | **Accepts Risk** | **Milestone 3: Protect Your Network (Network**  **Architecture)** |
| X |  | Yes. Detailed in section | Yes | Have you identified and documented your current network enclaves? |
| X |  | Yes. Detailed in section | Yes | Have you identified and documented the current high value assets and choke points on your network? |
| X |  | This is the initial creation of this network plan. | Yes | Are you updating your documentation whenever your network enclaves, high-value assets, or choke points change?  - When there is a change, how long before this documentation is updated? |
| X |  | This is the initial creation of this network plan. Items are described in section. | Yes | Are you periodically re-evaluating your network architecture to make sure it most effectively protects your high-value assets, limits access to sensitive information, and keeps damage contained?   * How often are these re-evaluations done? * How often do you review your network trust relationships? * If a trust relationship is found that can be eliminated or limited, how long before this elimination/limiting is actually done? |
| X |  | Yes. Detailed in section | Yes | Have you gone over the points to consider for this Milestone? |

*Checklist date: 11/11/24*

### *APPENDIX H: Milestone-4 Check-List*

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **AcceptsRisk**.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yes** | **No** | **Explanation** | **Accepts Risk** | **Milestone 4: Reach Your Network (Device**  **Accessibility)** |
| X |  | Detailed in section | Yes | Have you established and documented a process to properly, easily, and securely access and administer EVERY device on your network (workstations, servers, supporting devices, infrastructure devices, and mobile devices)? |
| X |  | Detailed in section | Yes | Are you updating your device access/administration process and documentation as necessary? |
| X |  | Detailed in section | Yes | Have you gone over the points to consider for this Milestone? |

*Checklist date: 11/11/24*

### *APPENDIX I: Milestone-5 Check-List*

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **AcceptsRisk**.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yes** | **No** | **Explanation** | **Accepts Risk** | **Milestone 5: Control Your Network (User**  **Access)** |
| X |  | Detailed in section | Yes | Have you established non-privileged user accounts for all users on your network? |
| X |  |  | Yes | - % of *total* users on your network that are allowed to use *only* non-privileged accounts? (Higher % is more secure) |
| X |  | Detailed in section | Yes | For all users with elevated privileges, have you documented the privileges given and the reasons for giving those privileges, and are those reasons regularly reviewed?   * How often are the reasons for giving those privileges reviewed? * If the reasons are no longer valid or no longer justifiable, how long before the privileges are actually removed? * % of elevated privilege accounts that do NOT have access to Internet or e-mail? (Higher % is more secure) |
| X |  | Detailed in section | Yes | Are you periodically verifying that all accounts on your network are tied to specific, current, authorized users?   * How often are these verifications done? * If an account is found that cannot be so verified, how long before this account is disabled? * If a user becomes unauthorized (terminated, etc.), how long before his account(s) are actually disabled? |
| X |  | Detailed in section | Yes | Have you gone over the points to consider for this Milestone? |

*Checklist date: 11/11/24*

***APPENDIX J: Milestone-6 Check-List***

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts** **Risk**.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yes** | **No** | **Explanation** | **Accepts Risk** | **Milestone 6: Manage Your Network, Part I (Patch Management)** |
| Yes |  | Detailed in section |  | Have you established and documented a patch management process for ALL the OS and application software on EVERY device on your network (workstations, servers, supporting devices, infrastructure devices, and mobile devices)?   * Within each device category, % of devices actually patched via this process? * Within each device category, % of devices that are assessed by an automated capability that they are adequately free of vulnerabilities? |
| Yes |  | Ongoing |  | Are you updating your patch management process and documentation as necessary? |
| Yes |  | Detailed in section |  | Have you gone over the points to consider for this Milestone? |

*Checklist date:* 12/02/24

***APPENDIX K: Milestone-7 Check-List***

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts** **Risk**.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yes** | **No** | **Explanation** | **Accepts Risk** | **Milestone 7: Manage Your Network, Part II (Baseline Management)** |
| Yes |  | Detailed in section | X | Have you created and documented a list of all the applications that are approved for use on your network?  - Within each device category, % of devices that have an automated capability to prevent or restrict execution of unapproved applications and other unapproved executable content? (Higher % is more secure) |
| Yes |  | Detailed in section |  | Have you established and documented the criteria and process for getting an application on the approved list? |
| Yes |  | Detailed in section | X | Have you created and documented device baselines (including for infrastructure devices and mobile devices)?   * Within each device category, % of devices actually covered by a documented baseline? * Within each device category, % of devices that are compliant with their documented baseline (no changes or additions)? * Within each device category, % of devices that have an automated capability to verify compliance (detect changes and additions)? |
| Yes |  |  |  | Are you updating your device baselines on a regular basis? |
| Yes |  | Detailed in section |  | Are you updating your approved application list, criteria and process for getting an application on the approved list, and baselines documentation whenever there is a change? |
| Yes |  | Detailed in section |  | Have you gone over the points to consider for this Milestone? |

*Checklist date: 12/02/24*

***APPENDIX L: Milestone-8 Check-List***

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts** **Risk**.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yes** | **No** | **Explanation** | **Accepts Risk** | **Milestone 8: Document Your Network** |
| Yes |  | Detailed in section |  | Are the procedures to rebuild servers and other important devices on your network fully documented and kept up to date? |
| Yes |  | Detailed in section |  | Are the procedures for adding and removing users and systems from your network fully documented and kept up to date? |
| Yes |  |  |  | As time permits, are you documenting all other administrative processes and procedures, and keeping them up to date? |
| Yes |  | Detailed in section |  | Have you gone over the points to consider for this Milestone? |

*Checklist date: 12/02/24*