Check List: Windows Machines

High Level

- Start Downloading Important Service Packs and Windows Updates.
    - DO NOT RESTART UNTIL LATER!!
- Look for alternatives to default applications
    - Install Firefox
- Install and maintain malware protection software
    - Install MalWare (Defender)
    - Install AntiVirus (Microsoft Security Essentials)
- Uninstall Dangerous Software
- Account Management
    - Remove guest user
    - Remove old accounts
    - Ensure all accounts use strong passwords
- Security Settings
    - Account Policies
    - Local Policies
- Action Center
- Windows Firewall
- Secure Internet Connections
- Services
    - Disable unnecessary services
        - IIS
        - Telnet
        - Web Services
        - FTP
- Delete Suspicious Files (Write down file names and locations that were deleted)
- Delete Unauthorized Files Write down file names and locations that were deleted)
- Disable dangerous features
- Configure System Startup
- Attach Detection
    - Task Scheduler & Task Manager
    - Monitor Performance and Resource Usage
    - Port Checks
    - Event Viewer
- Windows Update – Restart

Low Level

- Download Important Service Packs and Windows Updates.
  - **Control Panel -> Windows Update -> Install Updates**
  - Iconize Windows Update Window
  - **DO NOT RESTART UNTIL LATER!!! (Takes a while to update system)**
- Install/Update Firefox Browser as alternate to Internet Explorer
  - Firefox - https://www.mozilla.org/en-US/firefox/new/
- Install Malware and Anti-Virus Software
  - Install MalWare (Defender)
  - Install AntiVirus (Microsoft Security Essentials) - http://windows.microsoft.com/en-US/windows/security-essentials-download
- Unistall Dangerous Software
  - **Control Panel -> Programs and Features**
- Account Management
  - **Control Panel -> User Accounts -> Manage another account**
  - Delete or Turn off Guest Account
  - Delete Unauthorized Accounts
    - Write down deleted Account Names
  - Make sure all accounts are User accounts except those that authorized as Administrators
  - Ensure that all accounts are password protected.
- Security Settings
  - **Control Panel -> Administrative Tools -> Local Security Policy**
  - Account Policies
    - Password Policy
      - Enforce password history – 5
      - Maximum password age – 90 user 30 admin
      - Minimum password age – 10–30 days
      - Minimum password length – 8
      - Password must meet complexity requirement – Enable
      - Store password using reversible encryption – Disable
      - Passwords
        - Always use at least 3 of the following
          - Numbers
          - Lower case letters
          - Upper case letters
          - Symbols (%#*&!;{“>|)
        - Always use at least 8 characters
        - Use different password for each login
      - Do not use any personal info –can be easily found by other means
        - -Name
        - -Birthday
        - -Pet’s Name
        - -Mother’s Maiden Name
        - -Hometown
    - Account Lockout Policy
      - Account lockout duration - 30
      - Account lockout threshold – 3-10
      - Reset account lockout counter after - 30
  - Local Policy
    - Audit Policy Settings
      - Control Panel →System and Security → Administrative Tools → Local Security Policy → Local Policies → Audit Policy
        - Success: generates an event when the requested action succeeds
        - Failure: generates an event when the requested action fails

        - No Auditing: does not generate an event for the action
    - Right click the Security Setting column → Properties → Success, Failure
    - Must be set and enabled for logs to be available in the Event Viewer
        - Account logon events: Attempts to log into system accounts
        - Account management: Account creation or deletion, password changes, user group changes
        - Directory service access: Changes to shared resources on a network
        - Logon events: Attempts to log into a specific shared computer
        - Object access: Access to sensitive, restricted files
        - Policy change: Attempts to change local security policies, user rights, and auditing policies
        - Privilege use: Attempts to execute restricted system changes
        - Process tracking: Attempts to modify program files, which have rewritten or disrupted program processes (*key to detecting virus outbreaks)
        - System events:Computer shutdowns or restarts
        - *Recommended for Windows 7 users and Windows Server 2008 users
        - *Recommended only for Windows Server 2008 users
- User Rights Assignment
    - Access this computer from the network – Remove "Everyone"

- Action Center
    - **Control Panel -> System and Security -> Action Center**
    - Windows Updates
        - Install Updates Automatically
- Windows Firewall
    - **Control Panel -> System and Security -> Windows Firewall->Change notification settings**
    - Turn Firewall on for Home, Work, and Public
    - Select "Block all incoming connections, including those in the list of allowed programs" for both
    - Select "Notify me when Windows Firewall blocks a new program" for both
    - **Control Panel -> System and Security -> Windows Firewall->Advanced settings**
    - Allow trusted programs to connect without being blocked by adding them to your Windows Firewall Exceptions list
        - For each network type, you can customize whether you want the programs allowed through
    - It's much safer to allow only certain programs through your firewall than to open an entire port to traffic
        - Ports are numbers that identifies one side of a connection between two computers
    - Common Exceptions
        - Core Networking
            - Regular Microsoft Windows services that retrieve data from the Internet
            - If you don't enable this exception across all three types of networks, some Microsoft services and programs will not run properly
        - File and Printer Sharing - off
        - Remote Assistance - off
        - Remote Desktop - off
        - UPnP Framework (Universal Plug-and-Play) -off
    - Advanced Settings
        - Inbound Rules
        - Outbound Rules
        - Connection Security Rules
        - Monitoring
- Secure Internet Connections
    - **Control Panel -> Internet Options**
    - Security Tab
        - Security Level – High
    - Privacy Tab
        - Block All Cookies
        - Never allow websites to request your physical location
        - Turn on Pop-up Blocker

        - Disable toolbars and extensions when InPrivate Browsing starts
    - Advanced
- Services
    - **Control Panel -> Administrative Tools -> Services**
    - Disable unnecessary services (Stop and Disable)
        - IIS
        - NetMeeting Remote Desktop Sharing – VoIP
        - Remote Desktop Help Session Manager
        - Remote Registry
        - Routing and Remote Access
        - Simple File Sharing
        - SSD Discovery Service
        - Telnet
        - FTP
        - Universal Plug and Play Device Host
        - Windows Messenger Service
- Delete Suspicious Files
    - Look in C:\Windows\System & C:\Windows\System32 for programs with recent timestamps
    - Look in C:\Program Files\ for any suspicious programs
    - Write down file names and locations that were deleted
- Delete Unauthorized Files
    - Remove any unauthorized media files
    - Write down file names and locations that were deleted
- Disable Dangerous Features
    - **Control Panel -> System -> Remote settings**
    - Select “Don’t allow connections to this computer”
- Configure System Startup
    - **Control Panel -> Control Panel -> System and Security -> Administrative Tools -> System Configuration**
    - **Control Panel -> Control Panel -> Administrative Tools -> System Configuration**
    - Remove any unnecessary startup processes
- Attach Detection
    - Task Scheduler & Task Manager
        - Check for unusual processes
        - Check for any netcat processes running
    - Performance Monitoring
        - Allows you to track the use and performance of hardware and software resources on a system
        - Allows you to view real-time and historical data
            - Stop problems as they’re happening
            - Predict future problems
            - Conduct forensics to close vulnerabilities and stop intrusions of the same type from happening again
        - Allows you to decide if hardware or software needs updating
        - Allows you to determine if unknown programs and/or malware are running
        - Allows you to monitor and restrict user access
        - Task Manager
            - **Menu Bar -> Start Task Manager**
            - Applications
                - Programs you interact with on the desktop
                - Three tasks:
                    1. Close programs that are not responding
                    2. Check if an unnecessary piece of software is running
                    3. Find the process that is associated with certain software, so you do not shut it down when looking for illegitimate services
            - Processes
                - Some processes are essential for Windows and should not be shut down

- Some malware are not visible as applications and can only be ended by shutting down associated services
- Lookup processes to determine whether they are legitimate: www.processlibrary.com
- Terminate
- Set Priorites
- View CPU Usage
- View Memory Usage
-

- Services
  - Services are programs that run invisibly and automatically in the background
  - List of processes running in the background
    - Status:
      - Started: Currently running
      - Blank: Not running
    - Startup Type (how services start when the computer is booted up):
      - Automatic: Starts when computer is booted up
      - Manual: Starts when prompted to by user
      - Disabled: Cannot be re-enabled automatically or manually by regular users (only Admins)
  - Disable Services
    - Two reasons to disable services:
      i. Unnecessary
         - E.g. Spotify or other programs that decrease student/worker efficiency
      ii. Insecure
         - E.g. Remote Desktop Services or others than allow people to access your file systems from outside the organization's networks
    - To disable a service or otherwise change its startup type, right-click it and select "Properties"
  - Click the "Services" button to manage services in advanced window
- Performance
  - Monitor performance and resources
  - Overall statistics for system usage
    - CPU Usage by core
    - Memory Usage
      - Displays the amount of RAM being used over time. Extremely high values could indicate hidden malware is operating on your system.
      - Provides details on how RAM is being used. Cached RAM is used by system resources, available RAM is the amount immediately available for use by processes, drivers, or the OS, and free RAM is unused or does not contain useful information
      - Lists how much memory is being used by the OS as a whole. If these numbers are very high, Windows might be corrupt or there is a piece of malware that is hampering its ability to run effectively.
    - Number of processes
- Network Activity
  - Shows wired and wireless activity
  - Network connectivity problems can arise from a broken router, switch, or cable, or from the computer itself
    - The Networking tab will allow you to check whether the computer is the origin of the problem

- Lists the names of your connections and tells you the percentage of your overall network that each connection is utilizing, the speed of the link, and whether or not that link is fully connected.
- Shows network performance over time. If utilization is very high one or more programs on your may be eating up all of your available bandwidth. Or, if you are not currently using any programs connected to the Internet, a high number could indicate you have malware on your computer or that an intruder is accessing your computer remotely.

▪ Users
- Look for unknown users
- Users can be disconnected and/or logged off
- Shows you all of the users currently logged on to the system
- Allows you to "disconnect" users
  - Terminate the user's connection without shutting down the programs they were running
- Allows you to "logoff" users
  - Log the user off the computer completely and terminate any running programs

▪ View performance data for system, both real time and logs
- Event Log Performance
  - **Control Panel -> Performance Information and Tools -> Advanced Tools -> View performance details in Event Log**
- Resource Monitor
  - **Control Panel -> Performance Information and Tools -> Advanced Tools -> Open Resource Monitor**

▪ Obtain information about hardware, software components, and monitor security events on a local or remote computer
▪ Look for processes that may be over utilizing resources or not functioning properly
▪ Look for unknown processes running
▪ Identify and diagnose current system problems
▪ Predict potential system problems

o Port Checks
▪ Open command prompt and run command: netstat -aon

o Event Viewer
▪ Control Panel → System and Security → Administrative Tools → Event Viewer
▪ Security tool that allows you to view records of changes and other events that have happened on a computer
▪ Used by cybersecurity professionals to monitor system changes and the inner workings and less visible processes run by a computer
▪ Security logs can be a useful last defense against attacks and a tool for forensics investigations into the source of a past attack or unauthorized entry
▪ Customize what security logs are kept by setting **Audit Policies**
▪ Windows Log
- Application – Events logged by programs
- Security – Any successful or unsuccessful logon attempts
- Setup – Events that occurred during installation
- System – Events logged by system componenets
- Forward Events – Events forwarded from other computers

- Updates/Patches
  - o Windows Update
    - ▪ **Control Panel -> Windows Update -> Restart**