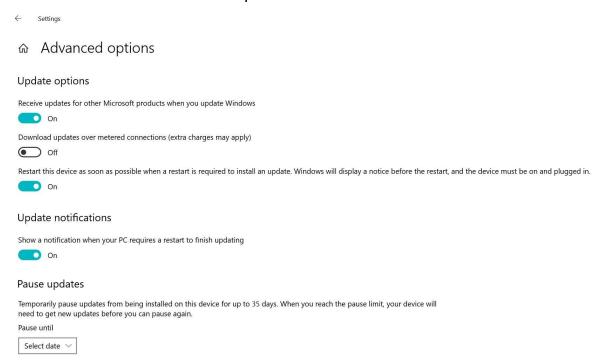# Windows Checklist

MAKE NOTES

- Read the Readme
- Forensics Questions
- Windows Settings
  - Updates (if Readme Allows)
    - Settings\Updates+Security\Windows Update
    - Check for updates

← Settings

⌂ Advanced options

Update options

Receive updates for other Microsoft products when you update Windows

🔵 On

Download updates over metered connections (extra charges may apply)

⚪ Off

Restart this device as soon as possible when a restart is required to install an update. Windows will display a notice before the restart, and the device must be on and plugged in.

🔵 On

Update notifications

Show a notification when your PC requires a restart to finish updating

🔵 On

Pause updates

Temporarily pause updates from being installed on this device for up to 35 days. When you reach the pause limit, your device will need to get new updates before you can pause again.

Pause until

Select date ∨

- Users (settings and control panel)
    - Account type correct
    - Passwords exist?
    - Groups (if specified in Readme)
    - Passwords length/complexity/strength
        - If not replace with ' CyberPatriot21 '
  - Hidden Files

- Update and security\for developers
- (or type "show hidden files" in windows search)
- click show hidden files, folders, and drives
  - o Malware + Virus
    - Windows Security\Virus + threat protection
      - Quick scan
      - Check for updates
  - o Remote Desktop Settings
    - Settings\update and security\for developers
      - Disable RDS by unchecking all Remote desktop boxes (Unless specified in readme to keep enabled)
    - System properties\remote
      - Uncheck remote assistance
      - Don't allow remote connections
- Control Panel
  - o Users (settings and control panel)
    - Account type correct
    - Passwords exist?
    - Groups (if specified in Readme)
    - Passwords length/complexity/strength
      - If not replace with ' CyberPatriot21 '
  - o Firewall
    - Windows Defender Firewall (in Control Panel)
    - Make sure its on (private and public)
    - Restore default settings if needed
  - o Programs/Suspicious apps (in file explorer and control panel)
    - Control panel\Programs\programs and features
      - Check for suspicious programs/hacking tools/ non work related files
      - CHECK README
- Computer Management
  - o Shared files
    - Computer management\system tools\shared folders\shares
      - Stop share for Admin$, C$, IPC$ (right click)

- File Explorer
  - Programs/Hidden Files
    - AFTER YOU HAVE SHOWN HIDDEN FILES IN SETTINGS
    - In file explorer search *.mp3
      - .mp3, .mp4, .avi, .mov, .jpeg, .png, etc
      - You can right click file to open file location then delete
    - Check C drive for program files/ suspicious files
      - HashCat, Wireshark, TeamViewer, Steam, iTunes, CCleaner, (hacking tools)
- Program Updates
  - README
  - Notepad++, Firefox, sometimes edge or other web browser
  - Firefox options
    - Don't save logins
    - Check for updates
    - Auto install updates
    - In Privacy and Security switch to Standard or Strict
    - Do Not Track → Always
    - Clear cookies and delete cookies when closed
    - Disable autofill logins + psswds
    - Enable block popup windows
    - Enable Warn when try to install add ons
    - Enable block dangerous + deceptive content
- Password Policy
  - Type "sec pol" in windows search → security policy
  - Account policies\password policy
    - Password history → 7 days
    - Max password age → 90 days
    - Min password age → 15 days
    - Min password length → 10 characters
    - Complexity requirements → enabled
    - Store psswd w/reversible encryption → disable
  - Account policies\account lockout policy
    - Lockout threshold usually between 5-10

- Local policies\audit policy
    - Audit all w/success + failure checked
    - If you lose points → uncheck it :)
- Local policies\user rights assignment
    - Disable guest

- Examples.xlsx = Mini checklist made by Coach Jake