CyberPatriots Windows Checklist:

User Management: <Computer Management< System Tools< Local Users&Groups<

- Remove users that are not supposed to be there
- Add the users that should be there
- Fix bad passwords (safe password example: BlueTiger01!)
- Check user groups (especialy administrators, there is probably people that are not supposed to be there)
- Disable Guest Account
- Disable Administraor Account
- Do README user tasks

Updates:

- Update system: <Settings < Update&Secuity < Download
- Update Firefox: <Firefox< three lines< options< scroll down and download the update< Restart to update once dowloaded

Security Policies: <Local Security Policy< Account Policy

Set Password Policy:

- Enforce password history – 7
- Maximum password age – 90
- Minimum password age – 30
- Minimum password length – 8
- Password must meet complexity requirement – Enable
- Store password using reversible encryption – Disable

Set Account Lockout Policy: (tip: fist chnage the invalid atmenpts)

- Account lockout duration 30
- Account lockout threshold/invalid atempts 5-10
- Reset account lockout after 30

Audit Policy: <Local Security Lolicy <Local Polices < Audit Policy<

- Audit EVERYTHING (both success and failure)

Remove access to the computer from network: <Local Security Policy <Local Polices < Users rights assignment< access this computer from network<

- Remove “everyone” not everyone but the “everyone” group.

Firewall: <Control Panel< System&Security< Windows defender firewall< Turn firewall on/off<

- Turn on for both public and private networks,
- Say Yes to block “all incoming…” and “Notify when…” for both private and public

Remove Bad Programs: <Control Panel< Programs&Features<

- Look for bad programs, if you dont know what it does google it or ask chatGPT.
- Remove the bad programs, CHECK if they are mentioned in the README.

Stop bad Services: <Control Panel < System&Security < Administrative Tools < Services> (pause and stop the services)

- Check for unnecessary/bad services like;
  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

Secure Internet connections: <Control Panel < Network&Internet < Internet Properities>

- Security tab: set security level high

- Privacy teb: advanced (block all cookies), Never allow websites to request your location, turn on pop-up blocker.

Delete Media files: < File Explorer < Local Disk < Search bar < Search for mp3, mp4, avi, mov…. Etc.

Set Windows Smart Screen: <Group Policy editor< Administrative Templets< Windows Components< Windows defender smart screen< configure windows defender smartscreen for both explorer and microsoft edge

Disable AutoPlay: < Local Group Policy Editor< Windows Components< Auto-Play Policies< TurnOff auto-play< Enabled

Notify Admin on User Susbicius Activity: Control Panel<System&Security < Security and Maintace< Security < Change user account control settings< always.

Disable Remote Conncetions: <Control Panel < System&Security < System < Remote Settings < Select “ dont allow remote conncetions to this computer”

Check Shared Folders: <Computer Management < System Tools < Shared Folders <

- Check if you are sharing anything that is unnormal.