Firmware Security (BIOS/UEFI Password)

1. **Restart your PC**.
2. **Enter BIOS/UEFI Setup**: Press F2, DEL, or ESC during startup (varies by manufacturer).
3. **Navigate to Security Settings**:
   - Look for “Supervisor Password”, “Administrator Password”, or similar.
   - Set or verify that a password is configured.
4. **Ensure Boot Order is Locked** (optional, for added protection).
5. Exit and **save settings**.

BIOS settings **cannot be accessed from Windows.**

Operating System Access Control

1. Genuine Windows Activation

- Go to **Settings → Update & Security → Activation**.
- Confirm: **“Windows is activated”** is displayed.

2. Strong User Passwords

- Open **Control Panel → User Accounts → Manage User Accounts**.
- Ensure:
  - Each user account has a **non-blank password**.
  - Remove any **unnecessary user accounts**.

3. Screen Saver Lock

- Right-click Desktop → **Personalize → Lock screen → Screen saver settings**.
- Enable:
  - A screensaver.
  - **Check**: “On resume, display logon screen”.

4. Password Policy

- Press Win + R → type secpol.msc → press Enter.
- Go to **Account Policies → Password Policy**:
  - Minimum password length
  - Password complexity
  - Password history
  - Maximum/Minimum password age

5. Account Lockout Policy

- In secpol.msc, go to **Account Lockout Policy**:
  - Set **Account Lockout Threshold** (e.g., 3 attempts).
  - Set **Lockout Duration** and **Reset Counter** time.

6. Security Audit Policy

- In secpol.msc, go to **Local Policies → Audit Policy**.
- Enable:
  - Audit logon events (Success/Failure)
  - Audit object access (Success/Failure)
  - Audit policy change (optional)

7. NTFS File Permissions

- Right-click any **important folder** → Properties → **Security tab**.
- Review permissions for:
  - Users
  - Groups (Administrators, Everyone, etc.)

8. Share Permissions

- Right-click folder → **Properties** → **Sharing** → **Advanced Sharing** → **Permissions**.
- Review who has access and their permissions (Read, Change, Full Control).

9. Windows Updates

- Go to **Settings** → **Update & Security** → **Windows Update**.
- Click **Check for updates**.
- Ensure system is **fully updated**.

10. USB Port Access Control

Option A: Device Manager

- Press Win + X → **Device Manager** → Expand **Universal Serial Bus controllers**.
- Disable unwanted ports/devices.

Option B: Group Policy

- Press Win + R → gpedit.msc → Enter.
- Navigate to:

```
Computer Configuration → Administrative Templates → System →
Removable Storage Access
```

- Configure access restrictions to USB mass storage.

Network Access Control

1. Host Firewall

- Go to **Control Panel → Windows Defender Firewall**.
- Ensure it's **ON for all network profiles** (Domain, Private, Public).

2. Antivirus

- Open **Windows Security → Virus & threat protection**.
- Verify:
  - Antivirus is **enabled** and **up-to-date**.
  - Last scan was recent.

3. Browser Security

Chrome/Edge:

- Go to **Settings → Privacy and Security**.
- Enable features like:
  - **Safe Browsing**
  - **Do Not Track**
  - Review **Site Permissions** (location, camera, notifications).

Physical Security Control

1. Cabinet Locks

: Verify physically (manual inspection).

2. Biometric Device

- Go to **Settings → Accounts → Sign-in Options**.
- Check for **Fingerprint / Facial Recognition** setup.

3. Smart Card Logon

- Open **Control Panel → Administrative Tools → Local Security Policy**.
- Navigate to **Public Key Policies → Smart Card** options.

4. Entry Logs

- If integrated: Check system-generated **access logs**.
- If not: Use **manual logbooks** or access-control software.

Asset Management Control

1. Inventory Devices

- Open **System Information** (msinfo32) – shows hardware/software summary.
- Or use tools like:
    - **Spiceworks Inventory**
    - **Belarc Advisor**

Change Management Control

1. App & Hardware Compatibility

- Confirm compatibility of apps and drivers with OS.
- Check on **official vendor websites** before major updates.

2. Backup and Restore Plan

- Go to:
    - **Control Panel → Backup and Restore (Windows 7)**
    - Or **Settings → Update & Security → Backup**
- Configure:
    - **Backup location**
    - **Automatic schedule**

User Awareness Control

1. Cybersecurity Training

- Ensure employees have undergone training.
- Check:
    - **Certificates**
    - **LMS logs**
    - **Participation records**

Disaster Recovery Control

1. Backup & Restore Schedule

- Verify **automated backup schedule**.
- Confirm:
  - **Backup history**
  - Restore points set in:
    - **Control Panel → System → System Protection**