

Fundamental Security Concepts Checklist

- Confidentiality

Ensure only authorized users can access sensitive information. Use encryption (e.g., BitLocker) and access controls.

- Integrity

Protect data from unauthorized alteration. Use file checksums, auditing, and version control.

- Availability

Ensure systems and data are accessible when needed. Maintain regular, tested backups.

- Least Privilege

Assign users and systems only the access necessary for their roles. Avoid admin rights unless essential.

- Defense in Depth

Implement multiple overlapping layers of security: firewalls, antivirus, MFA, patching, and monitoring.

- People Are the Perimeter

Educate users on phishing, password hygiene, and acceptable use policies.

- Patching and Updates

Automate software updates and prioritize critical security patches.

- Backups

Follow the 3-2-1 rule: 3 copies, 2 types of storage, 1 offsite. Test restores regularly.

- Security as a Process

Continuously assess, monitor, and improve your security posture. It's not a one-time setup.