IT Security Checklist

An organizational checklist of IT security controls for teams and businesses.

Access control and identity

- [ ] Maintain a current inventory of all user accounts and their access levels.
- [ ] Apply least privilege so users have only the access they need.
  Review and revoke excess permissions regularly.
- [ ] Enforce multi-factor authentication for all remote and admin access.
- [ ] Use unique accounts per person and avoid shared logins.
- [ ] Disable accounts immediately when staff leave or change roles.
- [ ] Restrict and closely monitor privileged and administrator accounts.
- [ ] Enforce a strong password policy and a secure single sign-on where possible.

Network and perimeter

- [ ] Document the network with an up-to-date diagram and asset list.
- [ ] Configure firewalls to deny by default and allow only required traffic.
- [ ] Segment the network to separate critical systems and user devices.
- [ ] Secure remote access with a VPN or zero-trust gateway.
- [ ] Disable unused ports, services and default accounts on network devices.
- [ ] Encrypt data in transit with TLS across internal and external connections.

Endpoint and server hardening

- [ ] Deploy endpoint protection or EDR on all servers and workstations.
- [ ] Harden systems against a secure baseline such as CIS Benchmarks.
- [ ] Enable full-disk encryption on laptops and mobile devices.
- [ ] Remove or disable unnecessary software and services.
- [ ] Enforce screen locks, device policies and mobile device management.
- [ ] Control USB and removable media use according to policy.

Patch and vulnerability management

- [ ] Maintain an inventory of operating systems, software and firmware versions.
- [ ] Apply security patches on a defined schedule, prioritizing critical fixes.
- [ ] Run regular vulnerability scans across systems and applications.
- [ ] Track and remediate findings with owners and deadlines.
- [ ] Test patches in a staging environment before wide rollout where feasible.
- [ ] Replace or isolate end-of-life systems that no longer receive updates.

Logging and monitoring

- [ ] Enable logging on servers, network devices, applications and security tools.
- [ ] Centralize logs in a SIEM or log management platform.
- [ ] Synchronize clocks with NTP so events line up across systems.
- [ ] Define alerts for suspicious activity such as failed logins and privilege changes.
- [ ] Protect logs from tampering and retain them per policy.
- [ ] Review alerts and dashboards regularly, not just after an incident.

Policies and training

- [ ] Document security policies covering acceptable use, access and data handling.
- [ ] Classify data and define how each level must be stored and shared.
- [ ] Run security awareness and phishing training for all staff.
- [ ] Assess third-party vendors for security before granting access.
- [ ] Define backup and recovery requirements with tested restores.
- [ ] Assign clear ownership for each security control and policy.

Incident response

- [ ] Maintain a written incident response plan with defined roles.
- [ ] Keep an up-to-date contact list for the response team and key vendors.
- [ ] Define severity levels and escalation paths for incidents.
- [ ] Prepare steps to detect, contain, eradicate and recover from incidents.
- [ ] Run tabletop exercises to test the plan at least annually.
- [ ] Document lessons learned and update controls after each incident.