



IT Readiness Checklist

A practical, no-fluff list to get your business secure, resilient, and audit-ready.

Business Basics

- ☐ Maintain a current employee roster and role-based org chart.
- ☐ Keep a catalog of critical apps (version, owner, support contact).
- ☐ Track all third-party vendors and their support SLAs.

Identity and Access

- ☐ Multi-factor authentication enforced on email, VPN, and admin tools.
- ☐ Single Sign-On (SSO) in place for core apps where possible.
- ☐ Company password policy documented and communicated.
- ☐ Password manager deployed to all staff; shared vaults for teams.
- ☐ Admin accounts are separate from day-to-day user accounts.

Devices and Endpoints

- ☐ Asset inventory (owner, model, serial, OS, last check-in) is accurate.
- ☐ Supported OS versions only; end-of-life devices flagged for refresh.
- ☐ Next-gen endpoint protection active and reporting on every device.
- ☐ Full-disk encryption enabled on laptops and workstations.
- ☐ Screen lock and idle timeout policies enforced.

Patching and Updates

- ☐ Automated OS patching cadence defined and monitored.
- ☐ Third-party software patching in place (browsers, Java, Adobe, etc.).
- ☐ Firmware updates scheduled for critical hardware (BIOS, NIC, SSD).

Email and Collaboration Security

- ☐ SPF, DKIM, and DMARC configured for your email domains.
- ☐ Security awareness training running quarterly (new hires within 14 days).
- ☐ Phishing simulations at least quarterly; results reviewed with leadership.
- ☐ External sender banner and attachment type controls enabled.

- ☐ Email encryption available for sensitive messages.

Data Protection and Continuity

- ☐ Backups follow the 3-2-1 rule (3 copies, 2 media, 1 offsite or offline).
- ☐ SaaS backups enabled for Microsoft 365 or Google Workspace.
- ☐ Restore tests performed and documented within the last 90 days.
- ☐ RTO and RPO defined per system and agreed by the business.
- ☐ Critical data locations mapped; exclusions reviewed.

Network and Remote Access

- ☐ Business-class firewall with documented, reviewed ruleset.
- ☐ Wi-Fi uses WPA3 where supported; guest and staff networks segmented.
- ☐ VLANs separate servers, workstations, VoIP or IoT, and guest traffic.
- ☐ VPN required for remote admin access; split tunnel reviewed.
- ☐ DNS filtering and safe-search policies applied.
- ☐ Central logging and alerting for firewall and VPN events.

Compliance and Policies

- ☐ Acceptable Use, Remote Work, Incident Response, and WISP policies published.
- ☐ Industry needs covered (for example, IRS Pub 4557 for CPAs, HIPAA, PCI as applicable).
- ☐ Vendor risk assessments completed for critical providers.
- ☐ Annual security review with leadership; action plan tracked.

Physical and Office

- ☐ Network and server gear in a secure, cooled, access-controlled area.
- ☐ Labeling and cable management in place for quick recovery.
- ☐ UPS installed, batteries tested, runtime documented; graceful shutdown configured.

Incident Readiness

- ☐ Playbooks for ransomware, email compromise, and data loss printed and accessible.
- ☐ Current emergency contacts list (internal, MSP, cyber insurer, legal, PR).
- ☐ Cyber insurance policy details stored and renewal dates tracked.

Onboarding

- ☐ Role-based access template defines accounts, groups, and apps per role.
- ☐ Standard device build with baseline security hardening.
- ☐ Security training assigned within first 14 days; phishing baseline captured.

Offboarding

- ☐ Accounts disabled within 24 hours; access keys and tokens revoked.
- ☐ Company data collected; devices wiped or repurposed to standard.
- ☐ Mail forwarding, auto-reply, and data archive handled per policy.

Documentation

- ☐ Central documentation system updated (network diagrams, SOPs, credentials).
- ☐ Change logs maintained; last full review within 6 months.

Optional Enhancements

- ☐ Application allow listing or zero-trust controls for endpoints.
- ☐ Mobile device management (Windows, macOS, iOS, Android).
- ☐ Cloud and SaaS posture monitoring and alerting.

Questions or want help implementing this? Schedule a 45-minute consult: ITForProps.com