methodology IT
we make IT work

methodologyit.tech

Remote Work Security Checklist

Remote and hybrid work expands your attack surface: employees connect from home, coffee shops, and on-the-go. Without the right protections in place, sensitive data, customer records, and intellectual property are at risk. This checklist helps you evaluate your organization's readiness and highlight areas where Methodology IT can close the gaps.

Secure Access & Identity

- ☐ Multi-Factor Authentication (MFA) required for all accounts
- ☐ Single Sign-On (SSO) to reduce password fatigue and shadow IT
- ☐ Privileged Access Management for administrators
- ☐ Conditional Access rules (device compliance, geo-blocking, time-based access)

Endpoint Protection

- ☐ Company-managed laptops with security baselines applied
- ☐ Endpoint Detection & Response (EDR) with 24×7 SOC monitoring
- ☐ Disk encryption enabled on all devices
- ☐ Automated patch management for OS and applications
- ☐ Mobile Device Management (MDM) for smartphones and tablets

Network & Connectivity

- ☐ VPN or secure remote access for all offsite connections
- ☐ DNS filtering and web filtering to block malicious sites
- ☐ Firewalls configured for least-privilege and segmentation
- ☐ Prohibition of unsecured public Wi-Fi without VPN

Cloud & Collaboration Security

- ☐ Data Loss Prevention (DLP) for email, Teams, SharePoint, and file sharing
- ☐ Email filtering against phishing, spam, and malware
- ☐ Controlled external sharing (with expiration dates and access tracking)
- ☐ Backup of SaaS data (Microsoft 365, Google Workspace, etc.)
- ☐ Policies for safe AI tool usage (no sensitive data into unapproved platforms)

Network & Connectivity

- ☐ Mandatory Security Awareness Training & phishing simulations
- ☐ Acceptable Use Policy for personal vs. work devices
- ☐ Clear process for reporting suspicious activity
- ☐ Documented onboarding & offboarding security steps
- ☐ Regular refreshers on social engineering and remote-work risks

Please scan the QR code to book an appointment with our expert to learn more or visit: calendly.com/methodologyit/intro

800-270-0016

hello@methodologyit.tech

methodology IT
we make IT work

methodologyit.tech

Remote Work Security Checklist

Employee Awareness & Policies

- ☐ Mandatory Security Awareness Training & phishing simulations
- ☐ Acceptable Use Policy for personal vs. work devices
- ☐ Clear process for reporting suspicious activity
- ☐ Documented onboarding & offboarding security steps
- ☐ Regular refreshers on social engineering and remote-work risks

Incident Response & Business Continuity

- ☐ Incident Response Plan documented and tested
- ☐ Remote wipe capability for lost/stolen devices
- ☐ Backups tested for successful restores
- ☐ Tabletop exercises conducted at least annually
- ☐ Cyber insurance and/or security warranty in place

Quick Self-Assessment

80–100% Complete: Great work! Most of the key security measures are in place. Continue reinforcing policies and testing your defenses regularly.
50–79% Complete: You've covered many important items, but several areas still need attention. Completing the remaining steps will strengthen your overall security.
Below 50% Complete: Several critical items are missing from your checklist. Addressing them promptly will help better protect your data and operations.

Next Steps

Your checklist results highlight where your defenses stand today. The next step is turning those checkboxes into an actionable plan:

- Prioritize fixes in the areas with the most gaps.
- Engage experts to implement the right tools, policies, and monitoring.
- Validate readiness with testing, training, and continuous improvement.

Methodology IT is here to help—from quick gap assessments to full implementation and ongoing support. Together, we'll strengthen your security posture and give your distributed workforce the protection it needs.

Please scan the QR code to book an appointment with our expert to learn more or visit: calendly.com/methodologyit/intro

800-270-0016 hello@methodologyit.tech