# Remote Work Security Checklist

Steps your organization can take today to protect work-from-home (WFH) and remote employees against cyberattacks.

Protecting your remote workforce against cyber threats is crucial to maintaining your organization's data integrity, network security, and overall brand reputation. Our Remote Work Security Checklist is designed to help you systematically evaluate and enhance your current security measures. It covers key areas such as plans, policies, procedures, training, compliance, testing, and safeguards.

To use the checklist, review each section, assess your current status, and prioritize actions based on urgency. Mark items as "Needed," "In Progress," or "Done" to track your progress. Once completed, develop a security roadmap to address any gaps identified, schedule regular audits, and continuously update your policies to stay ahead of emerging threats.

| Action Item | Needed Y/N | In Progress Y/N | Complete Y/N |
|---|---|---|---|
| **Plans, Policies and Procedures** | | | |
| Cyber-Incident Response Plan | | | |
| Cybersecurity Policies and Procedures | | | |
| BYOD Policy | | | |
| Remote Working Policy | | | |
| IT User Policy | | | |
| Internal Controls (Wire Transfer, Approval Workflows) | | | |
| **Training** | | | |
| Security Awareness Training | | | |
| WFH Cybersecurity Awareness Training | | | |
| Phishing Prevention Training | | | |

Ntiva
Your Success. Secured.

| Action Item | Needed Y/N | In Progress Y/N | Complete Y/N |
|---|---|---|---|
| **Compliance** | | | |
| Security standards (ISO 27001, NIST, FAR/DFARS, HIPPA, CJIS, FINRA) | | | |
| Privacy Regulations (GDPR, CCPA) | | | |
| Supplier Policy | | | |
| **Testing** | | | |
| Vulnerability Scanning | | | |
| Firewall Configuration | | | |
| Remote Access Security | | | |
| Phishing Assessment | | | |
| **Safeguards** | | | |
| Software Updates/Patches | | | |
| WFH staff use Multi-Factor Authentication | | | |
| WFH staff access corporate networks through a VPN | | | |
| If allowed, remote hard drives and thumb drives are encrypted | | | |
| WFH staff cannot save sensitive documents to personal devices | | | |
| **Identity and Access** | | | |
| WFH employees are using strong passwords | | | |
| WFH staff protect against lost or stolen login credentials with MFA and self-serve password reset option | | | |

| Action Item | Needed Y/N | In Progress Y/N | Complete Y/N |
|---|---|---|---|
| **Personal and Company-Owned Devices** | | | |
| WFH employees keep all work documents and data on company-owned devices | | | |
| WFH employees have remote desktop access so that apps and data are no longer stored on WFH computers | | | |
| Diversity of storage repositories available to WFH employees is few to limit the number of avenues of attack | | | |
| WFH employees cannot use using cloud-sharing applications that have not been vetted for privacy and security | | | |
| **Confidential Business and Customer Data** | | | |
| WFH employees access corporate networks only through secure VPN connections | | | |
| Backup data on remote devices to guard against loss or theft | | | |
| You encrypt email communication and all sensitive documents | | | |
| **Protection Against Cyberattacks** | | | |
| You defend against impersonation and spoofing with Defender for Office 365 | | | |
| You use AI-powered malware scanning to detect malicious email attachments | | | |
| You guard against malicious web content by filtering for offensive, inappropriate, and dangerous content | | | |
| **Corporate Initiatives** | | | |
| Cloud Backup and Recovery | | | |
| Vulnerability Scanning and Remediation | | | |
| Intrusion Detection and Response | | | |
| Endpoint Detection and Response | | | |

For additional support, consider partnering with a Managed Security Services Provider like Ntiva to implement comprehensive security solutions tailored to your needs. By following this checklist, you can create a secure remote work environment that safeguards your organization's critical assets.

Did you miss the BYOD Policy Template? Stay ahead of security threats with our up-to-date Bring Your Own Device policy and click here. Save time and protect your business with expert guidelines.

Are you ready to talk with someone about your IT support needs? We'd love to help. Feel free to book a consultation!

**Schedule Your Consultation**

Ntiva
Your Success. Secured.