Remote Work Security Checklist

ntiva
Managed IT, Security, & Cloud Services

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

Guarding your networks, data and brand reputation in the age of WFH and remote workers means re-thinking many fundamental areas of your security posture. You need to re-think your BYOD policies, your acceptable use policies and other policies and procedures. You need to get a handle on the protections you currently have in place, and then take orderly steps to add security where needed. Use our checklist below to audit your organization's current cybersecurity posture and determine what you need to put in place to fill any gaps.

Item	Needed	Started	Done
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			
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			

Item	Needed	Started	Done
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			
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			

During your journey, you may want to consider using the services of a company that delivers Managed Security Services.

At Ntiva, we build affordable, comprehensive cybersecurity solutions for businesses of all sizes, in any environment. Our in-house team of cybersecurity experts protect your data, help you meet compliance requirements, and give you confidence that your business is safeguarded against the cyber threats posed by WFH and remote work.

If this sounds like something you'd like to explore, read our Cyber Security Solutions Overview, or contact us today.