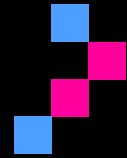


Remote Work Security Checklist



Initial
TECH

Overview

This simple checklist helps remote and hybrid teams secure home setups, devices, and access — in the same tick-box style as the Essential Eight self-assessment. It blends guidance from NIST SP 800-46 (telework), CISA/NSA VPN hardening, NCSC home working and MFA updates, and Microsoft Entra/Intune best practices.

How to use

- 1) Complete each section and tick Status.
- 2) Paste screenshots under Evidence (router settings, MFA registration, device compliance).
- 3) Keep the Action Plan updated and review quarterly.

1. Accounts & MFA

Task	How to (plain English)	Status	Evidence / notes
Enable MFA on email and all work apps	Use app-based or passkey methods; avoid SMS except as backup.		
Use strong passphrases + password manager	Unique passwords for each account; manager stores and autofills securely.		
Block legacy sign-in	Disable POP/IMAP/SMTP basic auth; enforce modern auth.		

2. Device security (laptop/phone/tablet)

Task	How to (plain English)	Status	Evidence / notes
Update OS & apps automatically	Turn on auto-update; reboot weekly to apply patches.		
Run antivirus/EDR	Ensure Defender/EDR is installed and active.		
Encrypt the device & enable screen lock	BitLocker/FileVault; auto-lock after 5–10 minutes.		
Separate work and personal use	Use company-managed device or work profile; avoid unapproved apps.		

3. Home network & Wi-Fi

Task	How to (plain English)	Status	Evidence / notes
Change default router admin password	Use a long unique password.		
Use WPA3 (or WPA2) encryption	Select WPA3-Personal; upgrade router if needed.		
Update router firmware	Check admin page; apply latest firmware.		
Separate guest/IoT network	Put smart devices on guest Wi-Fi; keep work devices separate.		

4. Secure access (VPN / Conditional Access)

Task	How to (plain English)	Status	Evidence / notes
Use company VPN on untrusted networks	Connect to corporate VPN before accessing internal resources.		
Require compliant devices	Entra Conditional Access: only allow access from Intune-compliant devices.		
Block legacy protocols & risky flows	Disable legacy auth; review device code flow policies and exclusions.		

5. Data protection

Task	How to (plain English)	Status	Evidence / notes
Use approved storage & sharing	SharePoint/OneDrive with org policies; avoid personal email/apps.		
Turn on backups/versioning	Enable cloud version history; backup key folders.		
Label sensitive data	Apply sensitivity labels; restrict external sharing.		

6. Working in public spaces

Task	How to (plain English)	Status	Evidence / notes
Avoid public Wi-Fi (or use VPN)	Prefer mobile hotspot; otherwise VPN before any work.		
Use privacy screen & lock device	Prevent shoulder-surfing; lock when away.		
Keep devices with you	Don't leave laptops unattended; enable remote-wipe.		

7. Phishing & social engineering

Task	How to (plain English)	Status	Evidence / notes
Think before clicking	Hover links; verify sender; report suspicious emails.		
Beware QR-code lures	Do not scan unknown QR codes; check destination domain.		

Action plan (next steps)

Action	Owner	Due date	Resources	Status

References

- NIST SP 800-46 Rev.2 – Guide to Enterprise Telework, Remote Access, and BYOD Security
- NSA/CISA – Selecting and Hardening Remote Access VPN Solutions
- NCSC – Device security & updated MFA guidance
- CISA – Telework Guidance & Toolkit
- Microsoft Learn – Conditional Access: require device compliance
- Microsoft Intune – Endpoint best practices