Remote Work Security Checklist

Cyber Liability Resource | Free Download

Remote and hybrid work environments expand your organization's attack surface and introduce unique cybersecurity risks. Unsecured home networks, personal devices, and public Wi-Fi create vulnerabilities that threat actors actively exploit. This checklist helps organizations assess and strengthen security controls for remote workers—a key area of focus for cyber liability insurers during underwriting and renewals.

WHY IT MATTERS: Cyber insurance carriers increasingly evaluate remote work security practices during underwriting. Weak remote access controls, lack of endpoint protection, and inadequate employee training are common reasons for coverage restrictions, higher premiums, or claim denials. Completing this checklist demonstrates proactive risk management.

Organization Information

Organization: _____ **Date:** _____

Completed By: _____ **Role / Title:** _____

1. Network Security & Remote Access

Secure all remote connections to prevent unauthorized access to corporate systems and data.

	Checklist Item	Status / Notes
☐	VPN is required for all remote access to corporate systems and data	
☐	VPN uses strong encryption (AES-256 or equivalent)	
☐	Split tunneling is disabled on corporate VPN connections	
☐	Multi-factor authentication (MFA) is required for VPN and all remote access	
☐	Remote Desktop Protocol (RDP) is disabled or restricted to VPN-only access	
☐	All remote access sessions are logged and monitored	
☐	Employees are prohibited from using public Wi-Fi without VPN protection	

2. Endpoint Protection & Device Security

Ensure all devices used for remote work meet minimum security standards.

	Checklist Item	Status / Notes
☐	All remote devices have current endpoint detection and response (EDR) software	
☐	Automatic OS and software updates are enabled and enforced	
☐	Full-disk encryption is enabled on all laptops and desktops (BitLocker / FileVault)	
☐	Screen lock is required after 5 minutes of inactivity or less	
☐	Local administrator privileges are restricted on corporate devices	
☐	USB and removable media are restricted or disabled by policy	
☐	Mobile Device Management (MDM) is deployed on all corporate mobile devices	
☐	Remote wipe capability is enabled on all corporate and BYOD devices	

3. Authentication & Access Control

Implement strong identity verification and least-privilege access for all remote workers.

	Checklist Item	Status / Notes
☐	Multi-factor authentication (MFA) is enforced on all cloud services and applications	
☐	Single Sign-On (SSO) is implemented for centralized access management	
☐	Password policy requires minimum 14 characters with complexity requirements	
☐	Password manager is provided and required for all employees	
☐	Privileged access (admin accounts) uses separate credentials and enhanced MFA	
☐	Access is granted on a least-privilege basis and reviewed quarterly	
☐	Inactive accounts are automatically disabled after 30 days	
☐	Conditional access policies restrict login from unapproved locations or devices	

4. Email & Communication Security

Email remains the primary attack vector. Secure all communication channels used by remote workers.

	Checklist Item	Status / Notes
☐	Advanced email threat protection (anti-phishing, anti-spoofing) is deployed	
☐	DMARC, DKIM, and SPF records are configured and enforced for all domains	
☐	External email warning banners are displayed on inbound messages	
☐	Employees are trained to identify phishing, BEC, and social engineering attacks	
☐	Sensitive data is prohibited from being shared via personal email accounts	
☐	Video conferencing tools require passwords and waiting rooms by default	
☐	Only approved collaboration platforms (Teams, Slack, etc.) are authorized for use	
☐	File sharing is restricted to approved cloud storage with access controls	

5. Data Protection & Cloud Security

Protect sensitive data wherever it is stored, accessed, or transmitted by remote workers.

	Checklist Item	Status / Notes
☐	Data classification policy defines handling requirements for sensitive data	
☐	Data Loss Prevention (DLP) tools are deployed to prevent unauthorized data transfer	
☐	Cloud storage access requires MFA and is limited to approved platforms	
☐	Sensitive data is encrypted in transit and at rest across all platforms	
☐	Personal cloud storage (Dropbox, Google Drive personal) is blocked for work use	
☐	Printing of sensitive documents from home is restricted or monitored	
☐	Backup procedures include data stored on remote devices and cloud platforms	
☐	Data retention and disposal policies apply to remote work environments	

6. Physical Security & Home Office

Physical security of remote workspaces is often overlooked but critical for data protection.

	Checklist Item	Status / Notes
☐	Remote workers secure devices when not in use (locked room or cabinet)	
☐	Privacy screens are required on laptops used in shared or public spaces	
☐	Home Wi-Fi networks use WPA3 (or WPA2 minimum) with strong passwords	
☐	Default router admin credentials have been changed	
☐	IoT devices are on a separate network segment from work devices	
☐	Confidential documents are stored securely and shredded when no longer needed	
☐	Employees are prohibited from allowing family members to use work devices	

7. Employee Training & Awareness

Human error remains the leading cause of security breaches. Training is essential.

	Checklist Item	Status / Notes
☐	Annual cybersecurity awareness training is mandatory for all remote workers	
☐	Quarterly phishing simulation exercises are conducted and results tracked	
☐	Training covers remote-specific threats (public Wi-Fi, shoulder surfing, device theft)	
☐	Employees know how to report suspected security incidents immediately	
☐	Remote work security policy is acknowledged in writing by all employees	
☐	New hire onboarding includes remote security procedures and expectations	
☐	Targeted training is provided for employees who fail phishing simulations	

8. Incident Response & Monitoring

Ensure your incident response plan accounts for the unique challenges of a distributed workforce.

	Checklist Item	Status / Notes
☐	Incident response plan addresses remote work scenarios and communication channels	
☐	Remote workers know how to report incidents using out-of-band communication	
☐	Endpoint detection and response (EDR) provides real-time monitoring of remote devices	
☐	Security Information and Event Management (SIEM) includes remote access logs	
☐	Remote device isolation can be performed within 30 minutes of incident detection	
☐	VPN and remote access logs are retained for a minimum of 12 months	
☐	Incident response tabletop exercises include remote work scenarios	

9. Policy & Compliance

Formalize remote work security expectations in written policies reviewed by all employees.

	Checklist Item	Status / Notes
☐	Written remote work / telecommuting security policy is in place	
☐	Acceptable use policy covers remote devices, networks, and cloud services	
☐	BYOD policy defines security requirements for personal devices accessing work data	
☐	Remote work policy is reviewed and updated at least annually	
☐	Policy compliance is audited or spot-checked at least semi-annually	
☐	Cyber insurance policy requirements for remote access controls are reviewed annually	
☐	Third-party and contractor remote access follows the same security standards	

Review & Sign-Off

This checklist has been reviewed and the items above accurately reflect the current state of our organization's remote work security posture. Any gaps identified will be addressed according to the action plan below.

Name	Title / Role	Signature	Date

Action Items for Identified Gaps

Document any gaps identified during this review and assign corrective actions with target completion dates.

#	Gap / Issue Identified	Corrective Action	Assigned To	Target Date
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Disclaimer

This checklist is provided by First Underwriters Insurance Brokers as a complimentary resource for informational and risk management purposes only. It does not constitute legal, technical, or professional advice. Every organization's IT environment and risk profile is unique; this checklist should be customized to fit your specific needs. Completion does not guarantee insurance coverage or claim approval. Consult with your IT provider, legal counsel, and insurance broker.

First Underwriters Insurance Brokers

4055 Lake Washington Blvd NE, Suite 100, Kirkland, WA 98033 | (425) 242-5357 | firstunderwriters.com