Secure Remote Work Checklist for Small Businesses (2026 Edition)

This checklist helps ensure your team can work remotely without increasing your security risk.

Secure Remote Work Checklist

1. Secure Every Login (Identity First)

☐ MFA is required for all remote access
☐ Email, cloud apps, and admin accounts are protected
☐ Shared accounts are not used

Why this matters:
Most remote attacks target identities, not networks.

2. Use a Password Manager Across the Team

☐ All work credentials are stored in a password manager
☐ Password reuse is eliminated
☐ Credentials are never shared through email or chat

Why this matters:
Remote teams rely heavily on logins. Centralized control reduces risk.

3. Use Secure Devices Only

☐ Work is done on company-approved devices
☐ Personal devices follow security rules if allowed
☐ Devices require PIN, password, or biometric login

Why this matters:
Unsecured personal devices are one of the most common remote vulnerabilities.

4. Keep Devices Updated and Protected

□ Operating systems are up to date
□ Antivirus or endpoint protection is active
□ Software updates are installed regularly

Why this matters:
Outdated systems are easy entry points for attackers.

5. Protect Internet Connections

□ Employees avoid public Wi-Fi when possible
□ VPN or secure connection is used when needed
□ Home networks use strong passwords and updated routers

Why this matters:
Unsecured networks can expose sensitive data during transmission.

6. Control Access to Company Data

□ Employees only access data they need
□ File sharing is done through approved platforms
□ Sensitive data is not stored locally when avoidable

Why this matters:
Remote work increases the risk of accidental data exposure.

7. Use Cloud Services Securely

□ Business apps are accessed through secure platforms
□ Shadow IT (unauthorized tools) is discouraged
□ Access is managed centrally

Why this matters:
Cloud misuse—not cloud itself—is the risk.

8. Train Employees to Recognize Remote Threats

□ Employees know how to spot phishing emails
□ Suspicious login requests are verified
□ Security concerns are reported quickly

Why this matters:
Remote employees are more likely to encounter phishing attempts.

9. Lock Devices When Not in Use

□ Screens auto-lock after inactivity
□ Devices are not left unattended in public spaces
□ Sensitive work is not displayed in public view

Why this matters:
Physical exposure is still a real risk in remote environments.

10. Enable Remote Device Control

□ Devices can be remotely locked or wiped
□ Lost or stolen devices are reported immediately
□ Device tracking or management is enabled

Why this matters:
Quick response limits damage if a device is lost.

11. Back Up Work Data Regularly

□ Work files are backed up automatically
□ Backups are not stored only on the device
□ Recovery has been tested

Why this matters:
Remote work increases the risk of data loss and ransomware impact.

12. Secure Remote Access Tools

□ VPN, remote desktop, or access tools are protected with MFA
□ Unused remote access tools are disabled
□ Access logs are reviewed periodically

Why this matters:
Remote access tools are a common attack vector.

13. Separate Work and Personal Use

□ Work accounts are not used for personal services
□ Personal apps are not used for business data
□ Browser profiles or devices are separated when possible

Why this matters:
Mixing personal and business use increases risk and reduces control.

What Secure Remote Work Looks Like

- **Employees can work from anywhere safely**
- **Access is controlled and monitored**
- **Devices are secure and managed**
- **Data stays protected—even outside the office**

Quick Rule of Thumb

If your security only works in the office, it doesn't work anymore.

SofTouchSystems.com
No-Surprise IT — Predictable. Proactive. Proven.