



Tips for Cyber Security when Managing a Virtual Team

Visualize your firm's data like a wheel

- **The hub** = your office/server (where your data lives)
- **The spokes** = your remote employees and devices accessing it



Use this checklist to ensure every spoke is secure

- Use a Virtual Private Network (VPN).**
All remote workers must connect to firm data only through a secure VPN using a single DNS entry. Require strong passwords and MFA.
- Require strong passwords and MFA.**
Passwords must be 14+ characters (or stored in a password manager) and all PII access must use multi-factor authentication.
- Encrypt all data.**
Ensure data is encrypted in transit and on remote devices; laptop theft should not equal data loss.
- Enable automated software updates.**
All remote workstations, servers, and websites must auto-update to avoid security gaps.
- Provide dedicated work hardware.**
Remote users may not browse, shop, or access personal email from their work workstation.
- Install endpoint security.**
Every remote machine must have security software, plus timed shutdowns of both the workstation and VPN.
- Secure the office/network hub.**
Use firewalls at the office and consider one at the remote location; keep guest Wi-Fi separate.
- Apply least privilege access.**
Give users access only to the data required for their role to limit breach exposure.
- Document a remote work policy.**
Have remote workers sign acknowledgment that no PII can be stored on their workstation. Review yearly.
- Perform secure and disconnected backups.**
Backups must be encrypted, offsite, and tested regularly — with at least one backup offline.
- Maintain a disaster recovery plan.**
Document all hardware, software, vendors, passwords, and recovery procedures — update annually.
- Train, test, and monitor.**
Conduct phishing tests, WISP reviews, and periodic audits to ensure no PII is stored on remote devices.

Security starts with awareness.

WISP Builder is the only web app that helps you build and securely maintain your IRS-required written information security plan (WISP).

[Sign Up Here!](#)