Remote Work Security Kit

A practical checklist for securing your remote and hybrid workforce, written for small business decision-makers.

1. Device & Access Controls

1. [ ] All work laptops/desktops are enrolled in endpoint management or validated before access
2. [ ] Multi-factor authentication (MFA) is enabled for all accounts with sensitive data access
3. [ ] Remote access is gated by Conditional Access policies (location, device health, identity)
4. [ ] No business data is stored on unencrypted personal devices or shared home PCs

2. Network & Connection Security

1. [ ] Employees use secure Wi-Fi (WPA2 or better) with changed default router passwords
2. [ ] VPNs or ZTNA solutions are used for connecting to internal or cloud resources
3. [ ] DNS filtering is enabled on all roaming laptops to block known malicious domains
4. [ ] Public Wi-Fi use is limited or secured via trusted VPN services

3. Data Loss Prevention & Monitoring

1. [ ] Cloud DLP or CASB tools are in place to monitor file uploads and sharing behavior
2. [ ] Access to company data is granted only on a need-to-know and least-privilege basis
3. [ ] Business email and file storage are protected by spam filtering and ransomware scanning
4. [ ] Alerts are configured for abnormal file access, transfers, or login attempts

4. Onboarding & Offboarding Processes

1. [ ] New hires receive basic cybersecurity awareness and remote work security training
2. [ ] Devices are provisioned with secure baseline configurations before being distributed
3. [ ] Offboarding includes revoking all credentials and access rights on last day
4. [ ] Company data is wiped from personal or BYOD devices upon offboarding

Need help locking down your remote workforce?
Contact Wentz IT Consulting for a customized remote work security assessment.
https://wentzitconsulting.com/contact