Remote Employee Security Checklist

Make sure every remote team member is secure and compliant.

Device Security

- Laptop is encrypted (BitLocker, FileVault, or similar)
- Antivirus and anti-malware are installed and running
- Device is password-protected and auto-locks after inactivity
- Operating system is fully updated

Wi-Fi & Network

- Using a trusted private network (no public café Wi-Fi)
- Router is secured with a strong password (not default)
- VPN is required for accessing any internal systems
- Firewall is enabled

Account & Access

- Multi-Factor Authentication (MFA) is enabled for all logins
- Passwords are unique and stored in a password manager
- Access to work apps is limited to only what is necessary (least privilege)

Communication & Files

- Company files are shared using secure, approved platforms
- File sharing with external parties is reviewed or approved
- Email attachments are scanned automatically or manually before opening

Physical Security

- Laptop is not left unattended in public places
- No work data is stored on personal USBs or external drives
- Screen privacy filter is used if working in public areas
- Devices are shut down when not in use

Incident Readiness

- Knows how to report a security incident
- Contact info for IT/security is saved and accessible
- Understands basic steps to take after a suspected breach