CRENSHAW, WARE & MARTIN, PLC

Teleworking Data Security Tips

Teleworking data-security is essential to protecting company data when employees are working at remote locations. Consider these simple tips to encourage your company and employees to maintain data security outside of the office.

Employees

Secure Connection Do not access company data via unsecured home or public Wi-Fi networks. When working remotely, protect data by using a Virtual Private Network (VPN) and a home firewall. Directly plug your machine into the router if possible. Segregate and conceal your work connection from other home Wi-Fi traffic.

Data Protection Avoid transferring sensitive company data to personal devices, non-company applications, and/or prohibited external storage (physical or cloud). Do not share personal or company information on line or store in personal accounts (email or cloud). Securely back up files on company storage in case of a data incident.

Device Security Do not leave your personal or company device unsecured. Physically secure your device and external storage. Enable automatic lock and log-off screens to prevent unauthorized access when away. Do not allow anyone to use computers or devices that have access to company data. Use complex passwords and keep passwords secure when working remotely.

Software & Updates Ensure all device applications, anti-virus, operating systems, and web browsers are up to date. Run a complete scan of your entire device before accessing company data. Remove all peer to peer, file sharing and outdated/unused applications from personal devices that access company data.

Avoid and Report Suspicious Activity Contact the company and follow the company's incident response plan to report all data security issues. Disable pop-ups and do not click on suspicious links or open unknown emails.

Do not take any significant business actions (i.e. transfer funds) without verifying the transaction with actual parties to the transaction over the phone.

Businesses

Secure Connection Ensure Wi-Fi networks are secure, encrypted, and hidden. Configure your firewall to prevent unauthorized access to company data and applications. Provide those working remotely with device security software.

Data Protection Implement mandatory complex passwords and multi-factor authentication for devices and applications. Limit access to data and applications based on employee roles and information needs.

Device Security Ensure all devices that access company data are properly configured, i.e. enable automatic screen locks to engage after a period of inactivity. Implement device and communication encryption as needed.

Security Software and Updates Increase the sensitivity of network security tools. Ensure all applications, anti-virus, operating systems, and web browsers are automatically updating on all devices.

Security Training Keep employees trained on best practices and how to handle security issues when they arise. Ensure employees are familiar with device, email, and storage encryption practices when handling sensitive data.

Incident Management Provide employees with clear data incident response guidance outlining how to report an issue, plan of action, and escalation path for remote technical and security issues.

150 W. Main Street, Suite 150 Norfolk, Va 23510 | (757) 623-3000 | www.cwm-law.com