

# Remote Work & Telecommuting Data Security Standard



One of the most significant risks of allowing employees to work from a remote site is the potential to compromise your company's Information Technology and data security systems and protocols. That makes it essential to address these issues in your Remote Work Policy and the individual agreements you make with your employees. Here's a template Data Security Standard you can adapt for your company's own systems and technology that you should refer to and attach as an Appendix to the above-referred Policy and individual agreement.

\*\*\*\*\*

## **REMOTE WORK DATA SECURITY STANDARD**

### **1. Purpose**

The purpose of this Standard is to protect the confidentiality, integrity, and availability of Company information when employees work remotely. This Standard applies to all employees, contractors, and other authorized individuals who access Company information or systems while working outside Company premises. Failure to comply with this Standard may result in disciplinary action, termination of remote work privileges, or other appropriate corrective action.

### **2. Employee General Responsibilities**

Employees working remotely must:

- Safeguard Company information and data at all times.
- Comply with all Company information security and privacy policies.
- Use Company information solely for authorized business purposes.
- Immediately report suspected security incidents.
- Cooperate with investigations involving security or privacy breaches.

### **3. Company Devices**

Employees working remotely must use Company-issued computers and mobile devices whenever practicable. Such Company devices must:

- Be protected by passwords or passphrases meeting Company requirements.

- Employ multi-factor authentication where required.
- Receive security updates promptly.
- Maintain approved anti-malware software.
- Use full-disk encryption where available.

Employees may not disable security software installed by the Company.

#### **4. Personally Owned Devices (BYOD)**

Employees working remotely may use personally owned devices only when expressly authorized. Such approved devices must:

- Meet Company security standards.
- Maintain current operating system updates.
- Employ approved security software.
- Support required encryption.
- Allow for installation of Company security applications where applicable.

The Company may revoke authorization to use personal devices at any time.

#### **5. Password Security**

Employees working remotely must:

- Create strong, unique passwords or passphrases.
- Never share passwords.
- Never reuse Company passwords for personal accounts.
- Use password managers where approved.
- Enable multi-factor authentication whenever available.

Passwords must never be written where unauthorized individuals may access them.

#### **6. Network Security**

Employees working remotely must:

- Use secure, password-protected Wi-Fi.
- Change default router passwords.
- Install firmware updates when available.
- Avoid unsecured public Wi-Fi unless connected through an approved VPN.

When public Wi-Fi cannot reasonably be avoided, employees must use Company-approved VPN protection before accessing Company systems.

#### **7. Confidential Information**

Employees working remotely must protect confidential information from unauthorized disclosure by:

- Positioning monitors to prevent viewing by others.
- Using privacy screens where appropriate.
- Not discussing confidential matters where conversations may be overheard.
- Securing paper documents when not in use.
- Shredding confidential documents using approved methods before disposal.

#### **8. Physical Security**

Employees working remotely must:

- Lock computers whenever leaving the workspace.
- Secure laptops during travel.
- Prevent unauthorized access by family members, visitors, or roommates.
- Store Company equipment in a secure location when not in use.

Company devices must not be left unattended in vehicles unless it is unavoidable and the devices are appropriately secured.

## **9. Artificial Intelligence Tools**

Employees working remotely must not upload Company confidential information, personal information, client information, proprietary documents, source code, trade secrets or other sensitive data into publicly available generative artificial intelligence (AI) platforms unless specifically authorized by the Company. Employees using approved AI tools must:

- Verify the accuracy of AI-generated information before relying upon it.
- Comply with Company AI governance requirements.
- Protect confidential information at all times.

## **10. Cloud Storage**

Company information and data must be stored only in Company-approved cloud storage systems. Employees working remotely must not:

- Save Company files to personal cloud storage accounts.
- Transfer Company documents to unauthorized file-sharing services.
- Synchronize Company information with personal accounts.

## **11. Email Security**

Employees working remotely must:

- Exercise caution before opening attachments or clicking links.
- Verify unusual payment requests or requests for confidential information.
- Report suspected phishing emails immediately.
- Use Company-approved email accounts for Company business.

## **12. Video Meetings**

Employees working remotely must:

- Conduct meetings in locations that protect confidentiality.
- Verify participant identities where appropriate.
- Avoid displaying confidential information unnecessarily.
- Use Company-approved conferencing platforms.

Screen sharing should be limited to information required for the meeting.

## **13. Printing & Paper Records**

Employees working remotely must take practicable steps to minimize printing confidential documents. Printed materials must:

- Be secured from unauthorized access.
- Not be left unattended.
- Be destroyed securely when no longer required.

## **14. Travel**

When working while travelling, employees working remotely must:

- Maintain physical control of Company devices.
- Avoid discussing confidential matters in public places.
- Avoid connecting to unknown charging stations unless approved protective devices are used.
- Report any lost or stolen equipment immediately.

#### **15. Cross-Border Remote Work**

Employees may not perform Company work from another country without prior written approval. Approval must be obtained before commencing work from another country.

#### **16. Security Incidents**

Employees working remotely must immediately report any:

- Lost or stolen devices
- Suspected phishing attacks
- Ransomware incidents
- Malware infections
- Unauthorized access
- Accidental disclosure of confidential information
- Suspected privacy breaches
- Unusual system activity.

Employees must not attempt to conceal security incidents.

#### **17. Remote Access**

Remote access to Company systems may occur only through Company-approved methods. Employees working remotely may not:

- Bypass security controls
- Install unauthorized software
- Share remote access credentials
- Permit another person to use Company login credentials.

#### **18. Monitoring**

Employees working remotely do not have and should not expect to have rights to privacy in Company systems beyond rights provided by applicable law. Subject to applicable law, Company systems may be monitored for legitimate business purposes, including cybersecurity, protection of confidential information, regulatory compliance, investigation of suspected misconduct, and system maintenance.

#### **19. Compliance**

Employees working remotely must immediately notify their supervisor or Information Technology department if they become aware of any actual or suspected violation of this Standard.

Questions regarding interpretation or application of this Standard should be directed to the Information Technology department or Human Resources.

#### **Employee Acknowledgement**

I acknowledge that I have received, read and understand the Company's Remote Work Security Standard. I agree to comply with its requirements and understand that

violations may result in disciplinary action, including termination of remote work privileges and, where appropriate, further disciplinary measures.

Employee: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_