

This document involves employment or workplace-compliance obligations that vary by state and by employer size. It is a general starting point only — not legal advice — and should be reviewed by an employment attorney licensed in your state before use.

Remote Work Security Policy

Employee: [Employee name] **Date:** [Date]

1. Purpose

This policy sets security requirements for anyone accessing [Company name]'s systems or data from outside the office.

2. Network & Device Requirements

Connect to Company systems only over a secure, password-protected network — avoid public Wi-Fi without a Company-approved VPN. Keep devices' operating systems, browsers, and security software up to date.

3. Physical Security

Lock your screen whenever you step away from your device. Keep Company devices and any physical documents containing confidential information out of view of others and secured when not in use, especially in public or shared spaces.

4. Data Handling

Store Company data only in approved systems, not on personal cloud storage or personal devices unless specifically authorized. Avoid discussing confidential information where others could overhear, including on video calls in public or shared spaces.

5. Incident Reporting

Report a lost or stolen device, a suspected compromise, or any other suspected security incident to [IT/security contact name] immediately, regardless of where you were working when it happened.

6. Consequences

Violating this policy may result in corrective action up to and including termination, consistent with [Company name]'s other disciplinary policies.

☐

Acknowledgment

I have read and understand this Remote Work Security Policy and agree to follow it.

[Employee name] ("Employee")

Signature: _____ Printed name: _____ Date: _____

This template is a general starting point, not legal advice — customize it and have it reviewed for your situation.