

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.

Cybersecurity Policy

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

1. Purpose

This policy sets baseline security practices for anyone accessing [Company name]'s systems, accounts, or data, to reduce the risk of unauthorized access, data loss, or a security incident.

2. Passwords & Account Security

Use unique, strong passwords for Company accounts and a password manager where provided. Enable multi-factor authentication wherever it is available. Never share your credentials or leave accounts logged in on shared devices.

3. Phishing & Suspicious Activity

Be cautious of unexpected emails, links, or attachments, especially those requesting credentials, payments, or urgent action. Report suspicious messages to [IT/security contact name] rather than clicking or replying.

4. Software & Updates

Keep company-issued devices' operating systems and software up to date, and only install software approved by [IT/security contact name]. Do not disable security software (antivirus, disk encryption, etc.) provided on company devices.

5. Incident Reporting

Report a lost or stolen device, a suspected account compromise, or any other suspected security incident to [IT/security contact name] immediately — quick reporting meaningfully limits damage.

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 Cybersecurity 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.