

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.

Data Privacy & Handling Policy

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

1. Purpose

This policy sets expectations for handling personal and confidential data belonging to [Company name], its employees, customers, and other third parties.

2. Data Covered

This policy applies to personal data (e.g., names, contact details, financial or health information) and other confidential business data, however it is stored — digital or physical.

3. Handling Requirements

Access data only as needed to do your job ("need-to-know"). Store data only in approved systems, not personal devices or accounts unless specifically authorized. Do not share data outside [Company name] without authorization, and dispose of physical or digital records containing personal data securely when no longer needed.

4. Data Breach Reporting

Report any suspected loss, theft, or unauthorized access to data immediately to [Privacy/security contact name] — many jurisdictions impose short legal deadlines for notifying affected individuals or regulators once a breach is known, so speed matters.

5. Third-Party Data

Data belonging to customers, vendors, or other third parties must be handled according to any specific commitments [Company name] has made to them (e.g., in a contract or privacy notice), in addition to this policy.

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 Data Privacy & Handling 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.