Stateline AI Solutions

Customer Data + AI Handling Policy

AI policy template for small businesses. Review with qualified counsel for regulated or high-risk use.

Purpose

This policy defines how employees should handle customer and business data when using AI tools.

Data That Requires Protection

Do not enter the following into unapproved AI tools:

- Customer names connected to private details.
- Addresses, phone numbers, emails, account numbers, or payment details.
- Health, insurance, financial, employment, or legal information.
- Contracts, bids, pricing, margins, supplier terms, or proprietary methods.
- Internal strategy, passwords, credentials, source code, API keys, or security information.
- Photos, documents, or recordings that contain sensitive customer or employee information.

Safer Alternatives

When using AI for general help:

- Remove names, account numbers, and identifying details.
- Replace sensitive facts with placeholders.
- Use general examples instead of real customer information.
- Use approved internal tools for company documents and customer data.
- Ask a manager if the data type is unclear.

Approved AI Workflows

AI may be used with customer data only when:

- The tool has been approved by company leadership.
- The workflow has a defined business purpose.
- Access is limited to appropriate employees.
- Outputs are reviewed by a human before use.
- Data retention, privacy, and security settings have been reviewed.

Customer-Facing AI Output

Before sending AI-assisted content to a customer, employees must confirm:

- The customer facts are accurate.
- The tone matches company standards.
- The content does not disclose private or internal information.
- The recommendation is appropriate for the customer situation.
- Any quote, price, delivery date, or commitment is approved.

Incident Response

If sensitive data is entered into an unapproved AI tool, employees should notify a manager immediately and include:

- What information was entered.
- Which tool was used.
- When it happened.
- Whether the output was saved, shared, or sent.

Policy owner: _____

Effective date: _____

Review date: _____