

Written Information Security Plan

Maple Street Studio LLC

9 Oak Ave, Boston, MA 02108

Effective date	November 1, 2026
Next review date	November 1, 2027
Data Security Coordinator	Jordan Lee, Owner
Version	1.0

Prepared with WispMint. This plan is structured on the FTC's guide Protecting Personal Information: A Guide for Business, the NIST Cybersecurity Framework small business resources, and the written-program elements found in state data security laws such as Massachusetts 201 CMR 17.00.

1. Purpose and scope

Maple Street Studio LLC (the "Business") collects and keeps personal information about its customers and employees, including names, email addresses, phone numbers and mailing addresses, payment card information and employee HR and payroll records. Many state laws require businesses to protect personal information with reasonable security and to notify people if it is breached, and some, such as Massachusetts 201 CMR 17.00, require a written information security program. The FTC also treats a failure to use reasonable security as an unfair business practice.

This plan sets out the administrative, technical and physical safeguards the Business uses to protect customer information. It applies to every owner, employee, contractor and seasonal worker, at both of its locations and wherever Business work is performed.

2. Objectives

1. Ensure the security and confidentiality of the personal information the Business holds.
2. Protect against anticipated threats or hazards to that information.
3. Protect against unauthorized access to or use of that information that could result in substantial harm or inconvenience to any customer, employee or other person.
4. Meet the Business's obligations under applicable state data security and breach notification laws and the FTC Act.

3. Data Security Coordinator

Jordan Lee, Owner, is the Business's Data Security Coordinator and is responsible for implementing, maintaining and annually reviewing this plan, training staff, overseeing service providers and leading the response to any security incident. The Coordinator may delegate tasks but remains accountable for the program.

4. Information covered by this plan

This plan covers all personal information the Business holds about customers, employees and other individuals in any form, including names, email addresses, phone numbers and mailing addresses, payment card information and employee HR and payroll records, whether held on paper or electronically. It also covers the passwords and accounts that give access to that information.

System	Used for	Where
Payments or point-of-sale software and accounting or payroll software	Running the business	Installed or vendor cloud
Google Workspace / Gmail	Customer correspondence	Cloud
Cloud storage and paper files	File storage	As listed
A secure portal or online forms and email attachments	Receiving customer information	As listed
Card payments	Taking card payments	As handled today (see Section 7.6)
Paper files	Source documents and records	9 Oak Ave, Boston, MA 02108, locked storage

5. Risk assessment

The Coordinator assesses risks to customer information at least annually and whenever the Business changes software, storage, staffing or location. The assessment considers employee training and management; information systems, including network, software, storage, transmission and disposal; and the detection of and response to attacks and system failures.

The Business is a business of 6 to 10 people that uses payments or point-of-sale software and accounting or payroll software, Google Workspace / Gmail for email, and stores files using cloud storage and paper files.

For a business of this size and setup, the most likely risks are phishing and account takeover against Google Workspace / Gmail and business app logins, customer information sent by plain email or text, theft of stored payment card numbers and paper files left out or thrown away unshredded. This plan addresses them through multi-factor authentication and access control (Section 6), device, network and backup safeguards

(Section 7), physical safeguards and disposal (Section 8), and a written incident response plan (Section 10). Any safeguard not yet fully in place appears in the gap list in Section 11 with an owner and a due date.

Current status from the most recent assessment:

Area	Status	Action
Email MFA	Not in place	See Section 11
Business app MFA	In place	Maintain
Card data handling	Not in place	See Section 11
Device encryption	Verify	See Section 11
Backups	In place	Maintain
Endpoint protection	In place	Maintain
Automatic updates	In place	Maintain
Wi-Fi security	In place	Maintain
Password manager	In place	Maintain
Secure disposal	In place	Maintain
Staff training	Not in place	See Section 11
Hiring checks	Not in place	See Section 11

6. Administrative safeguards

6.1 Staff responsibilities. Every person with access to customer information must read this plan, sign the acknowledgment in Appendix A, and complete security awareness training on hire and annually.

6.2 Hiring and departure. Beginning December 31, 2026, the Business will check references for new hires with access to personal information. When anyone leaves, their accounts, keys and access are removed on their last day and Business devices are returned.

6.3 Access control. Access to customer information is limited to those who need it for their work. Each person uses their own named account; shared logins are not permitted. Passwords are stored in a password manager.

6.4 Multi-factor authentication. MFA is required on email, business apps, online banking, cloud storage and remote access. MFA is not yet on for email and will be turned on by November 8, 2026. MFA is in place on business apps and online banking.

6.5 Service providers. The Business uses the service providers listed in Appendix C. Before using a provider that stores or processes personal information, the Coordinator confirms the provider offers appropriate safeguards (encryption, MFA, published security practices) and keeps a record. Providers are reviewed at the annual plan review.

6.6 Customer communication. Sensitive documents are exchanged through the Business's secure portal or online forms. Staff do not send Social Security numbers, bank details, card numbers or other sensitive information by unencrypted email or text, and ask customers to use a secure method instead.

6.7 Annual review. The Coordinator reviews and updates this plan every year, after any security incident, and after material changes to the business. Each review is recorded in Appendix D.

7. Technical safeguards

7.1 Devices. All Business computers run a supported operating system with automatic updates turned on, a screen lock after 10 minutes, and a paid endpoint protection product. Full-disk encryption (BitLocker or FileVault) will be confirmed or turned on for every computer by November 15, 2026.

7.2 Network. Wi-Fi is protected by a strong password, guests use a separate network, and the router's default admin password has been changed.

7.3 Data storage and transmission. Files are stored using cloud storage and paper files. Data is encrypted in transit (HTTPS/TLS) and at rest where the platform supports it. Customer and employee information is not stored on personal devices, USB drives or personal cloud accounts.

7.4 Backups. Business data is backed up automatically to an offsite cloud service. The Coordinator tests a restore at least twice a year.

7.5 Monitoring. The Coordinator reviews sign-in alerts and unusual activity notices from Google Workspace / Gmail, payments or point-of-sale software and accounting or payroll software and the Business's bank, and reviews bank and payment activity for anything unexpected at least monthly.

7.6 Card payments. Card payments will be taken only through a payment provider. By November 8, 2026, the Business will stop writing down or storing full card numbers and will securely destroy any it holds. The Business follows its payment provider's security requirements (PCI DSS).

8. Physical safeguards

Paper files containing personal information are kept in locked cabinets or a locked room when not in use. Desks are cleared of sensitive documents at the end of the day. Visitors do not have unescorted access to work areas, and screens are positioned so that visitors cannot read customer data. Paper is destroyed with a cross-cut shredder or a shredding service, and retired drives are wiped or physically destroyed.

9. Data retention and disposal

Personal information is kept only as long as needed for business, tax and legal purposes, then destroyed as described in Section 8. The Coordinator reviews stored records at the annual review and removes what is no longer needed. The Business keeps only the information it needs.

10. Incident response plan

An incident is any suspected or confirmed unauthorized access to, loss of, or misuse of personal information, including a lost or stolen device, a compromised email account, a ransomware infection, or a payment or banking fraud alert.

1. **Contain.** Disconnect affected devices from the network. Change passwords and sign out all sessions on affected accounts. Do not wipe or power off devices that may be needed for investigation.
2. **Notify the Coordinator** immediately: Jordan Lee, Owner, jordan@maplestreet.example.
3. **Notify affected people and state authorities** as required by MA breach notification law and the law of any other state whose residents are affected. Deadlines can be short, so check them right away.
4. **Notify the payment provider** right away if card data may be involved, and follow its instructions.
5. **Notify** the Business's cyber insurer, its bank if accounts or payments are affected, and law enforcement where appropriate (local police, or the FBI at [ic3.gov](https://www.ic3.gov) for online crime).
6. **Recover** from backups, confirm systems are clean, and restore normal operation.
7. **Record** the incident and the response in Appendix D, and update this plan within 30 days.

The Business reported an incident within the last three years. The safeguards in this plan and its review cycle are intended to address the lessons from that event, and the Coordinator will confirm at the first review that any remaining follow-up items are closed.

11. Gap list and action items

#	Gap	Action	Owner	Due
1	Email MFA (not in place)	Turn on multi-factor authentication for every email account.	Jordan Lee, Owner	November 8, 2026
2	Card data handling (not in place)	Stop writing down or storing full card numbers; take payments only through your payment provider and securely destroy any stored card numbers.	Jordan Lee, Owner	November 8, 2026
3	Staff training (not in place)	Complete security awareness training for everyone and record the date.	Jordan Lee, Owner	December 31, 2026
4	Hiring checks (not in place)	Check references for new hires who will handle personal information.	Jordan Lee, Owner	December 31, 2026
5	Device encryption (verify)	Confirm status. If not in place: Turn on BitLocker (Windows) or FileVault (Mac) on every computer that holds personal information.	Jordan Lee, Owner	November 15, 2026

Appendix A. Employee acknowledgment

I have read and understand the Maple Street Studio LLC Written Information Security Plan and agree to follow it.

Name: _____ Signature: _____ Date: _____

Name: _____ Signature: _____ Date: _____

Name: _____ Signature: _____ Date: _____

Name: _____ Signature: _____ Date: _____

One line per person. Add pages as needed.

Appendix B. Security awareness training checklist (annual)

- Recognizing phishing emails, texts and calls, including fake invoices and payment-change requests
- Using MFA and the password manager
- Handling personal information: secure method first, never ID or card numbers by plain email
- Locking screens, clean desk, shredding
- Reporting an incident right away, with no blame
- Review of this year's plan changes

Appendix C. Service provider list

Provider	Service	Holds personal data?	Safeguards confirmed	Date reviewed
Payments or point-of-sale software and accounting or payroll software	Business apps	Yes		
Google Workspace / Gmail	Email	Yes		
Cloud storage / portal	File storage	Yes		
Payment provider	Card payments	Yes		
Managed IT provider	IT support	Yes		
Backup provider	Backup	Yes		

Appendix D. Review and incident log

Date	Event	Summary	Signed
November 1, 2026	Plan adopted	Version 1.0	Jordan Lee

--	--	--	--

Appendix E. Key contacts

Contact	Details
Data Security Coordinator	Jordan Lee, Owner, jordan@maplestreet.example
Payment provider support	_____
Bank fraud line	_____
FBI Internet Crime Complaint Center	ic3.gov
Identity theft help for affected people	IdentityTheft.gov
MA Attorney General	State breach notification page
Cyber insurance carrier	_____