TRUST & SECURITY

Security and Compliance

How mailing.com protects customer, financial, and health data across the mail we run.

Security is the foundation of our business and built into every step of our process. Data is encrypted in transit, stored in access-controlled systems, and processed under role-based permissions. Printed materials follow a documented chain of custody through USPS handoff, and every stage is logged, monitored, and tied to named accountability.

At a glance

- Certified under SOC 1 Type II, SOC 2 Type II, HIPAA, NIST CSF, and PCI DSS v4.0
- Secure file transfer through an online portal and SFTP, never over email
- Mirrored production sites and recurring third-party audits
- Data encrypted in transit and at rest, processed under role-based access
- Documented chain of custody from data intake through USPS handoff
- SOC 1 and SOC 2 reports available on request under a mutual NDA

01 A security-first operating model

Security isn't a layer we add at the end. It's built into our facilities, systems, processes, and access controls, and it governs every job we run, every day.

Most mail programs carry sensitive customer, financial, or health data, and we treat every program that way by default. Access is restricted by role, data is segmented, production floors are controlled, and responsibility for each stage is assigned to a named owner. The same standards apply whether a job is a one-time campaign or a recurring program that runs every cycle.

02 Certifications and compliance standards

mailing.com maintains certified production environments audited under recognized industry standards. These give your security and compliance teams fast validation during a review.

SOC 1 Type II

Independent audit of controls relevant to financial reporting, confirmed as operating effectively over a defined period.

SOC 2 Type II

Independent audit of controls for security, availability, and integrity, confirmed over a defined period.

HIPAA

Compliant handling of protected health information across administrative, physical, and technical safeguards.

NIST CSF

A structured framework for identifying, protecting against, detecting, responding to, and recovering from risks.

PCI DSS v4.0

Compliance with the current Payment Card Industry Data Security Standard for handling cardholder data.

Every job runs inside these certified environments by default, whatever its size or mail type.

- Certifications apply to the production environments where client data is processed and mail is produced.
- Audits are recurring and maintained, not one-time events.
- Controls span people, process, and technology, so the standard holds across staffing, workflows, and systems.

03 Secure file transfer

Every file you send moves through an encrypted channel. We support two methods for getting data to us, and both are documented in our policy resources.

Secure online portal

A browser-based upload that encrypts files in transit and routes them directly into access-controlled storage. The simplest option for one-time or ad hoc transfers.

SFTP

An encrypted protocol for automated or recurring data feeds, with credentials issued per client and access limited by role. The standard choice for scheduled programs.

We don't accept sensitive data over email or other unsecured methods. If your team needs a specific transfer configuration, we set it up during onboarding.

04 Controls across data, facilities, and operations

Protection runs end to end, from the moment a file leaves your systems through production, mailing, and the monitoring that keeps the standard in place between audits.

Data protection and access controls

- Secure data intake and encrypted transmission
- System access restricted by role, granted only to staff who need it
- Customer data segmented so programs stay isolated from one another
- Controlled access to production systems
- Logging and monitoring of data access across the environment

Production and facility safeguards

- Controlled production floors with restricted entry
- Limited access to sensitive areas within each facility
- Documented chain of custody from data intake through mailing
- Separation of duties so no one person controls a job end to end
- Secure staging and handling of printed materials until USPS handoff

Operational security and continuity

- Mirrored production sites that keep work moving if one location is affected
- Redundancy for volume spikes, system issues, and facility-level disruptions
- Incident response and recovery procedures defined in advance

Ongoing monitoring and accountability

- Continuous monitoring of systems and workflows
- Regular internal reviews alongside recurring third-party audits
- Defined ownership for each security control
- Documented processes for issue escalation and remediation

Documented chain of custody, end to end

Every piece is tracked and tied to named accountability from the moment your data arrives until it enters the mail stream.

05 Requesting documentation and audit reports

Most security reviews can be completed with the information in this document and the policies published in our documentation. When you need formal reports, we provide them on request.

- **SOC 1 Type II and SOC 2 Type II reports** are available to current and prospective clients, typically under a mutual non-disclosure agreement.
- **Detailed policies** covering data handling, access control, file transfer, incident response, and business continuity are maintained in our policy documentation.
- **Vendor questionnaires and internal risk assessments** can be sent to your mailing.com account contact. Our team responds directly and points you to the relevant policies.

06 Frequently asked questions

What security certifications does mailing.com hold?

mailing.com maintains SOC 1 Type II, SOC 2 Type II, HIPAA, NIST Cybersecurity Framework (CSF), and PCI DSS v4.0. These apply to our production environments and are audited on a recurring basis.

Is mailing.com HIPAA compliant?

Yes. We operate HIPAA-compliant production environments for protected health information, with restricted facility access, role-based system controls, encrypted transmission, and a documented chain of custody from intake through mailing.

How does mailing.com handle data in transit?

All data moves through encrypted channels. We accept files through a secure online portal or SFTP, and we don't accept sensitive data over email or other unsecured methods.

Can I get a copy of your SOC reports?

Yes. SOC 1 Type II and SOC 2 Type II reports are available to current and prospective clients on request, typically under a mutual non-disclosure agreement.

Does mailing.com support our vendor risk assessment?

Yes. Send your questionnaire to your account contact and our team will respond directly and point you to the relevant policies in our documentation.

What happens if there's a disruption at a facility?

Production runs across mirrored sites with built-in redundancy, so programs continue during volume spikes, system issues, or facility-level disruptions. Documented procedures govern incident response and recovery.

Need our SOC reports or full policy documentation?

Contact your mailing.com account representative to request audit reports, policy access, or a response to your vendor questionnaire.

Contact Us