ClosingPoint Signing

Standard Operating Procedures

Document Security, Handling, and Confidentiality

Version	Effective date	Next scheduled review
1.0	July 1, 2026	June 30, 2027

1. Purpose and scope

These procedures describe the administrative, technical, and physical safeguards ClosingPoint Signing applies to non-public personal information (NPI) encountered while performing loan signing, mobile notary, and closing agent services.

It exists so that title companies, escrow offices, closing attorneys, and lenders engaging ClosingPoint Signing can document the practices of an outside service provider within their own vendor management and information security programs.

ClosingPoint Signing is not itself a financial institution. These procedures are maintained because the obligations of our clients extend contractually to the service providers they engage, and because the information handled warrants it regardless.

It applies to every engagement, every document set, and every location where work is performed, and it serves as the written information security program for ClosingPoint Signing.

2. Designated responsible individual

Lori Nicholas, owner of ClosingPoint Signing, is the individual responsible for these procedures — their implementation, their annual review, and the response to any incident affecting protected information.

ClosingPoint Signing is a single-operator business. No employees, contractors, or subcontractors perform signings, and no work is delegated to any third party. Every document set is handled from receipt to return by Lori Nicholas alone.

3. Information covered

Non-public personal information includes any personally identifiable financial information a consumer provides, that results from a transaction, or that is otherwise obtained in the course of providing a service. In loan signing work this routinely includes:

- Full legal names, residential addresses, and dates of birth
- Social Security numbers and taxpayer identification numbers

- Loan, deposit, and account numbers
- Income, employment, and asset information
- Government-issued identification details recorded in the notarial journal
- Property addresses and transaction terms

All of the above is treated as protected regardless of the medium in which it appears — printed, electronic, or handwritten.

4. Risk assessment summary

The principal risks to protected information in this line of work, and the controls applied to each:

Identified risk	Control applied
Documents intercepted in transit to or from the signing	Documents remain in the personal custody of the signing agent at all times; never left unattended in a vehicle or public space
Unauthorised access to printed packages at the work location	Printing, scanning, and storage occur in a dedicated private office; documents are held in a locked container whenever not in active use
Interception of documents in electronic transmission	Documents are transmitted only through the client's designated secure portal or an encrypted channel; never as unsecured email attachments
Compromise of devices used to receive or transmit documents	Device access controls, disk encryption, multi-factor authentication, and current operating system and security updates
Retention of information beyond its purpose	Defined retention limits with cross-cut destruction of all printed material not returned to the client
Undetected or unreported incident	Written incident response procedure with prompt client notification

5. Physical safeguards

Dedicated work location

All printing, scanning, assembly, and storage of client document packages occurs in a private, dedicated home office used solely for business purposes. Document packages are not printed, assembled, reviewed, or stored in shared or common living areas.

Dedicated equipment

Printing is performed on a dual-tray laser printer and scanning on a dedicated scanner, both located in that private office and both reserved for business use. Neither device is shared with any other household member, and neither is accessible outside the office.

Securing documents at the work location

- Client documents are stored in a locked container within the office whenever they are not in active use
- Documents are never left out, in view, or on open surfaces when the office is unattended
- Only the pages actively being worked on are out at any time; the remainder of the package stays secured
- Client documents are not accessible to anyone other than the signing agent

Custody in transit

- Document packages remain in the personal custody of the signing agent from the moment they are printed until they are returned to the client
- Packages are never left unattended in a vehicle, at a residence or office, or in any public space
- Packages are never left with a third party, a receptionist, or a signer for later collection
- Return shipment is made through the carrier and method specified by the client, with tracking retained

At the signing appointment

- Only the documents required for that appointment are brought to it
- Documents are not left in view of anyone other than the signers and parties entitled to be present
- Identification is examined and recorded but never photographed or copied unless the client instructs otherwise

6. Technical safeguards

- Every device used to receive, view, print, or transmit protected information is protected by a unique account password and locks automatically when idle
- Full-disk encryption is enabled on all such devices
- Multi-factor authentication is enabled on email and on every client portal that supports it
- Operating systems, applications, and security software are kept current
- Removable media — USB drives, memory cards, external disks — is not used to store or transfer protected information
- Work is not performed over public or unsecured wireless networks; the office network is private and encrypted
- Documents are received and returned electronically only through the client’s designated secure portal or another encrypted method the client approves
- Protected information is never sent as an unsecured email attachment, and is not stored in personal cloud accounts
- Electronic copies are removed from local devices once the engagement is complete and the client has confirmed receipt

7. Administrative safeguards

Screening

ClosingPoint Signing is NNA certified, and background screening is maintained current through the National Notary Association in accordance with Signing Professionals Workgroup standards. The most recent screening was completed in April 2026. Evidence of certification and screening is available to any client on request.

Confidentiality

- Protected information is used only to perform the engagement for which it was provided
- No client, borrower, or transaction information is discussed with, or disclosed to, any party outside the engagement
- No transaction details are used in marketing, testimonials, social media, or examples of any kind
- A confidentiality or non-disclosure agreement will be executed at any client's request

No delegation

Engagements are not subcontracted, reassigned, or shared. If ClosingPoint Signing is unable to perform a scheduled signing, the client is notified so that the client may reassign it. A replacement agent is never arranged independently.

8. Retention and destruction

ClosingPoint Signing does not retain client documents. Every page either returns to the client or is destroyed. No archive of completed transactions is kept, in any form, at any time.

Documents are in our possession only for the working window between printing and return shipment — typically one to two days. During that window they are handled as described in section 5.

- Printed materials not returned to the client are destroyed on site once the engagement is complete and the client has confirmed receipt of the package
- Destruction is by cross-cut shredder meeting DIN 66399 level P-4 or finer, so that the resulting output is not reconstructable
- Electronic copies are deleted from devices and from any local backup on the same schedule
- A notarial journal is maintained as a matter of practice. Minnesota does not require one; it is kept because it protects all parties if a signing is later questioned. It is stored secured in the private office and is not kept electronically
- No archive of completed client document packages is retained beyond those journal entries

9. Incident response

An incident is any actual or suspected loss, theft, unauthorised access to, or unauthorised disclosure of protected information — including a lost or misdirected package, a lost or stolen device, or a suspected compromise of an account.

On discovery of an incident:

- Contain — take immediate steps to limit further exposure, including suspending the affected account or device
- Notify — inform the affected client by telephone and in writing within 24 hours of discovery, without waiting for the assessment to conclude
- Assess — determine what information was involved, whose, and how it was exposed
- Cooperate — support the client's own incident response, notification obligations, and any investigation, and follow the client's direction on external notification
- Remediate — correct the cause
- Review — record the incident and revise these procedures where it would prevent recurrence

Notification is never delayed in order to complete an internal assessment first.

10. Credentials, licensing, and insurance

Item	Detail
Business entity	ClosingPoint Signing, Minnesota
Minnesota Closing Agent License	41045394
Minnesota Notary Commission	1469837400035
Certification	NNA Certified Loan Signing Agent
Background screening	National Notary Association — completed April 2026
Errors & omissions insurance	$25,000
E&O carrier	Merchants Bonding Company
Carrier address	P.O. Box 14498, Des Moines, IA 50306-3498

Current certificates and screening documentation are available to any client on request.

11. Client requirements take precedence

Where a client's own information security program, vendor agreement, or written instructions impose requirements stricter than or different from these procedures, the client's requirements govern. ClosingPoint Signing will comply with the client's security program and signing instructions as a condition of engagement.

Where a client's instructions appear to conflict with these procedures, with Minnesota notarial law, or with the lender's instructions, the matter is raised with the client before the signing proceeds rather than resolved unilaterally.

12. Review and maintenance

These procedures are reviewed at least annually, and additionally whenever there is a material change in the equipment, locations, or methods used, or following any incident. The date of each review is recorded below and an updated copy is made available to active clients.

Review date	Reviewed by	Changes made

Document control

Field	Detail
Document owner	Lori Nicholas, Owner
Version	1.0
Effective date	July 1, 2026
Next scheduled review	June 30, 2027
Issued to	Title companies, escrow offices, closing attorneys, and lenders on request

These procedures describe the actual working practices of ClosingPoint Signing. They are provided so that clients can document the practices of an outside service provider in their own vendor files. Where a client requires a signed vendor agreement, confidentiality agreement, or acknowledgement of their own information security program, ClosingPoint Signing will execute it.

Lori Nicholas — Owner, ClosingPoint Signing

612-399-6149 | lori@closingpointsigning.com | www.closingpointsigning.com