GLOBAL SIGNING PARTNERS

Information Security Program

Version 1.0 Effective November 2, 2026 Next review November 2027
Owner Global Signing Partners management

This document contains the written policies of Global Signing Partners' information security program. The current version is always at itsgsp.com/security.

1. Information Security Policy
2. Secure Software Development Policy
3. Physical and Environmental Security Policy
4. Incident Management and Response Policy and Plan
5. Record Retention and Data Destruction Policy
6. Business Continuity and Disaster Recovery Policy and Plan

POLICY 1

Information Security Policy

How GSP classifies information, controls access to it, encrypts it, and keeps its systems, vendors and people accountable.

1. Purpose and scope

This policy sets the rules Global Signing Partners ("GSP") follows to protect the confidentiality, integrity and availability of the information it handles, in particular the non-public personal information (NPI) and personally identifiable information (PII) of borrowers, signers, clients and signing agents.

It applies to everyone who works for or with GSP (owners, employees, contractors and independent signing agents), to every system that stores or processes GSP information (the client and agent portal at portal.itsgsp.com, the website itsgsp.com, email and the cloud services listed below), and to paper documents handled for GSP orders.

GSP maintains this program to meet the Gramm-Leach-Bliley Act Safeguards Rule (16 CFR Part 314), applicable state privacy and data-breach laws, and the requirements of the title, escrow and lending clients it serves.

2. Roles and responsibilities

- Management owns this program, approves the policies, accepts risk and decides on breach notifications.
- The designated security contact (the "Qualified Individual" under the Safeguards Rule) runs the program day to day: access reviews, backups and restore tests, vulnerability management, incident response, and an annual report to management.
- Everyone with access to GSP information protects it as described in these policies and reports suspected incidents immediately.
- Signing agents handle loan documents only for the assigned appointment and follow the handling rules in the Physical and Environmental Security Policy.

3. Information classification

Class	Examples	Handling
Restricted	Loan documents and signed scans, signer ID details, signing-agent background checks and credentials, account passwords and keys	Stored only in the portal; reached only through an access-checked, time-limited link; never emailed, texted or kept on personal storage
Confidential	Order details, client and agent contact information, fees and payouts, internal notes	Visible only to the parties to an order and GSP staff; shared by email only as needed to complete the order
Public	Website content, published policies, pricing	No restrictions

4. Access control

- Access follows least privilege and role: clients see only their own orders, signing agents see only orders assigned to them, and GSP administrators are limited to a named allowlist that the server re-checks on every request.
- Every portal action is authorized on the server for the person making it. Documents open only through 10-minute signed links issued after that check; the storage bucket itself is not publicly readable.
- Every person has their own account; shared accounts are not allowed. Passwords are at least 10 characters, screened against common and breached patterns, and stored only as bcrypt hashes.
- Sessions expire after 24 hours and use secure, HTTP-only cookies. Sign-in, sign-up, password-reset and public upload endpoints are rate-limited, and sign-in errors do not reveal whether an account exists.
- Multi-factor authentication is required on every administrative account for GSP infrastructure (hosting, storage, source code, payments and email).
- Access is removed the same business day a person leaves GSP or no longer needs it. The security contact reviews the administrator allowlist and infrastructure accounts every quarter.

5. Encryption

- In transit: the portal and website accept HTTPS only, with TLS 1.2 or 1.3 (older protocols are refused) and HTTP Strict Transport Security. Traffic between the application and storage is also encrypted with TLS.

- At rest: all portal records and documents are stored in Cloudflare R2, which encrypts every object with AES-256. Backups are encrypted the same way. Passwords are hashed with bcrypt, and application secrets are kept in the hosting provider's encrypted environment settings, never in source code.
- Email notifications are sent over TLS and contain only what is needed to complete the order. Loan documents are never attached to email or text messages; recipients sign in to the portal to view them.

6. Logging and monitoring

- The portal records security events (administrator sign-ins, failed sign-ins, password resets, account deletions, backup and retention runs, and security reports) in an append-only log kept for one year and copied to the off-site backup.
- Failed backups, failed retention runs and outside security reports alert the security contact by email.
- Hosting and storage provider logs supplement the application log during an investigation.

7. Vulnerability and patch management

- Application dependencies are pinned in a lockfile and checked for known vulnerabilities before each release and through automated repository alerts. High and critical issues in production code are fixed before release, or within 7 days of disclosure for software already in production.
- Operating systems and browsers on devices used for GSP work install security updates automatically.
- The application gets a full security review at least once a year and after major changes. The most recent full review was completed on October 21, 2026.

8. Vendors and service providers

GSP uses service providers that maintain independent security attestations. Before using a new provider that will handle NPI, the security contact reviews its security documentation, and each provider is re-checked every year. Current providers:

Provider	Purpose	Data	Assurance
Cloudflare (R2 storage)	Stores portal records and documents; off-site backup in a second U.S. region	All portal data, including NPI in loan documents	SOC 2 Type II, ISO 27001; AES-256 encryption at rest
Vercel (on AWS, U.S. East)	Runs the portal application	Processes portal data in memory; does not store documents	SOC 2 Type 2, ISO 27001
Resend	Sends account and order notification emails	Names, email addresses, appointment details; never loan documents	SOC 2 Type II
Stripe	Card payments on Stripe-hosted checkout pages	Billing details; card numbers never reach GSP systems	PCI DSS Level 1, SOC 2
GitHub	Private source-code repository	Application code only; no customer data	SOC 2 Type II, ISO 27001

9. People

- Everyone with access to NPI signs a confidentiality agreement and completes security awareness training when they start and every year after that.
- Signing agents are commissioned notaries who pass GSP's credential review (commission, E&O insurance and background check) before they can see any order.
- GSP information is used only for GSP business.

10. Related policies

- Secure Software Development Policy
- Physical and Environmental Security Policy
- Incident Management and Response Policy and Plan
- Record Retention and Data Destruction Policy
- Business Continuity and Disaster Recovery Policy and Plan

11. Exceptions, enforcement and review

Exceptions require written approval from management with a documented reason and an end date. Violations may lead to removal of access and termination of the working relationship. Management reviews this policy and the rest of the program at least once a year and after any significant incident or change.

POLICY 2

Secure Software Development Policy

GSP builds and runs its own client and signing-agent portal. This is how changes are written, tested, reviewed and released.

1. Scope

Yes, GSP performs software development for its services. GSP develops and operates the portal at portal.itsgsp.com, where clients place signing orders, signing agents receive and complete them, and documents are exchanged. This policy covers all code, configuration and infrastructure changes to it.

2. Source control and change management

- All code lives in a private GitHub repository, and every change is recorded as an attributable commit.
- Each release gets a version number and a changelog entry describing what changed and why.
- Production is deployed only from the main branch through the hosting provider, and any release can be rolled back to the previous version in minutes.
- Infrastructure settings (storage rules, scheduled jobs, environment configuration) are changed deliberately and recorded in the repository documentation.

3. Security requirements for every change

- Every endpoint checks on the server who is calling and whether that person may see or change the specific record. Nothing relies on hidden fields or browser-side checks.
- Input is validated on the server, output is escaped, and file uploads go only to storage locations the server picks, with an approved file type.
- Secrets (API keys and signing keys) live only in encrypted environment settings, separate for each environment, and never in code, logs or the browser.
- Error messages shown to users do not reveal internal details, and diagnostic and maintenance tools are not exposed in production.
- Changes to stored data use versioned writes, so two simultaneous edits can never silently overwrite each other.

4. Testing and review

- Security-relevant changes are checked against these requirements before release.
- An automated authorization test suite, which tries to reach other users' orders, documents and admin functions, is run before releases that touch access control and must pass in full.
- After each production deploy, the affected flows are verified on the live site.
- Testing uses designated test accounts only. Real customer accounts and documents are never used for testing, and test notifications go to the developer, not to customers or staff.

5. Dependencies

- Third-party packages are pinned to exact versions in a lockfile and come only from the official package registry.
- Known vulnerabilities are checked before each release and monitored by automated repository alerts; high and critical findings in production code are fixed before release.
- Unused packages and features are removed to keep the attack surface small.

6. Periodic assessment

The full application is reviewed against a recognized web-application security checklist (covering authentication, authorization, injection, uploads, secrets, logging, dependencies and configuration) at least once a year. The October 21, 2026 review fixed every high-risk finding before release, and its open items are tracked to closure.

POLICY 3

Physical and Environmental Security Policy

Environmental controls and physical access for the data centers that run GSP systems, the places GSP people work, and the paper documents signing agents carry.

1. Purpose and scope

This policy defines the environmental controls and physical access rules that protect GSP information systems and the facilities and devices used to reach them. It covers the cloud data centers, GSP work locations and devices, and paper loan documents handled by signing agents.

2. Data centers and environmental controls

- GSP runs no servers of its own. The portal runs on Vercel (on Amazon Web Services, U.S. East), and its data and backups are stored in Cloudflare R2 in two separate U.S. regions.
- These providers operate their data centers under independently audited controls (SOC 2 Type II and ISO 27001), including badge and biometric entry, 24/7 on-site security and video monitoring, redundant power with generators, fire detection and suppression, climate control, and secure media destruction.
- The security contact reviews each provider’s current audit reports every year as part of vendor review.

3. GSP work locations

- GSP information is reached only through the portal and the cloud services above. GSP keeps no paper files containing borrower NPI at its offices.
- Work is done from a GSP office or a private home office that is locked when unattended. Screens showing restricted information are not left visible to visitors or the public.
- Visitors to a GSP office are accompanied, and no visitor uses a GSP device or account.

4. Devices

- Devices used for GSP work have full-disk encryption, a screen lock that engages within 10 minutes, automatic security updates and malware protection, and are never shared with someone outside GSP while signed in.
- Restricted documents are opened in the portal and not saved to devices, except where a signing agent must print an assigned package for an appointment.

- A lost or stolen device is reported to the security contact immediately; affected passwords are changed and sessions ended under the incident response plan.
- Devices are wiped before they are reused or disposed of.

5. Access to information systems

Logical access to GSP systems follows the access-control rules in the Information Security Policy: individual accounts, role-based least privilege, server-side authorization, MFA on administrative infrastructure accounts, and quarterly access reviews.

6. Paper documents handled by signing agents

- Print loan packages only for an assigned appointment, keep them in your possession or locked away, and never leave them unattended in a vehicle or public place.
- Do not copy or photograph documents, except the scans the order requires, which are uploaded only through the portal.
- After the signing, return the package by tracked courier or hand delivery exactly as the order instructs, and record the tracking number in the portal.
- Cross-cut shred misprints and spare copies. Report a lost or misdelivered package to GSP within one hour.

7. Review

Management reviews this policy at least once a year and after any physical-security incident.

POLICY 4

Incident Management and Response Policy and Plan

How GSP detects, contains, investigates and recovers from security incidents, and when and how it notifies clients, consumers and regulators.

1. Purpose and definitions

This policy and plan make sure security incidents are handled quickly, consistently and lawfully.

A security event is anything that might affect GSP information or systems. A security incident is an event that actually or probably compromises the confidentiality, integrity or availability of GSP information, including any unauthorized access to NPI, whether electronic or on paper.

2. Roles

Role	Responsibility
Incident lead (security contact)	Triage, coordinates the response, keeps the incident record
Management	Approves containment that affects service; decides on and signs off client, consumer and regulator notifications
Technical responder	Investigates, contains, fixes and restores systems
Everyone, including signing agents	Reports suspected incidents immediately and preserves evidence

3. How to report

- GSP staff and signing agents: tell the security contact immediately by phone or email, and no later than one hour after discovery.
- Clients, researchers and the public: use the "Report a security issue" form at itsgsp.com/security. It goes straight to the security contact.
- Automated alerts for failed backups and other monitored events reach the security contact by email.

4. Severity

Level	Examples	Triage
1, Critical	Confirmed exposure of NPI; compromised administrator or infrastructure account; portal down more than 4 hours	Within 1 hour, any day
2, High	Suspected exposure; leaked secret; lost device or loan package; malware on a work device	Within 4 hours
3, Low	Blocked attack, phishing attempt, policy violation with no data exposure	Next business day

5. Response steps

- 1. Identify and record: open an incident record with time, reporter, systems and data involved; assign a severity.
- 2. Contain: for example, end all portal sessions at once by rotating the session-signing key; disable or reset affected accounts; revoke and replace exposed keys; block abusive traffic at the firewall; take a feature or the portal offline if needed.
- 3. Investigate and preserve evidence: review the security event log, hosting and storage logs and backups; establish what data and which people were affected and how.
- 4. Eradicate and recover: fix the cause, restore affected data from backup under the Business Continuity and Disaster Recovery Plan, and confirm normal operation.
- 5. Notify: follow the notification rules below.
- 6. Learn: hold a post-incident review within 10 business days, record root cause and corrective actions, and update controls and these policies.

6. Notification

- Clients (title, escrow and lending companies) whose information or borrowers are affected are told without unreasonable delay, targeting 72 hours after confirmation, or sooner if a client agreement requires.
- Affected individuals and state regulators are notified as each applicable state data-breach law requires.
- The Federal Trade Commission is notified as soon as possible, and no later than 30 days after discovery, when unencrypted information of 500 or more consumers is acquired without authorization (16 CFR 314.4(j)).

- Law enforcement is contacted when appropriate; a law-enforcement request to delay notice is documented.
- Notices describe what happened, what information was involved, what GSP is doing, and what recipients can do.

7. Playbooks

Scenario	First actions
Compromised portal account	Reset the password, end sessions, review the account's recent activity and the orders it could reach
Leaked secret or API key	Rotate the key in the provider and hosting settings, redeploy, and check provider logs for use
Lost device	Change passwords used on it, end sessions, confirm disk encryption, wipe remotely where possible
Lost or misdelivered loan package	Contact the courier and recipient, notify the client the same day, and assess notification duties
Data deleted or corrupted	Stop the cause, restore from the off-site backup, and verify against the restore checklist
Provider breach or outage	Get the provider's incident details, assess GSP exposure, and fail over or use manual workarounds per the BC/DR plan

8. Records and testing

Incident records and post-incident reviews are kept for at least five years. The plan is exercised at least once a year with a tabletop exercise, and the contact details in it are checked every quarter.

POLICY 5

Record Retention and Data Destruction Policy

How long GSP keeps each kind of record, and how it is securely destroyed afterwards.

1. Principles

- GSP keeps personal information only as long as it is needed to complete the work, meet legal and contractual obligations, or resolve disputes, and then destroys it.
- Documents are held in one controlled place, the portal, so they can be found, protected and destroyed on schedule.
- Destruction is suspended for any record under a legal hold (litigation, subpoena, regulatory inquiry or a client's written hold request) until the hold is released.

2. Retention schedule

Record	Kept for	Disposal
Signing packages and signed scans (order documents)	90 days after the order is closed or cancelled	Deleted from the portal automatically; the order keeps a note of what was removed and when (automated)
Files uploaded but never attached to an order or account, or replaced by a newer upload	30 days after upload	Deleted automatically (automated)
Order records (parties, appointment, fees, status history; no documents)	7 years after the order closes	Deleted at the annual records review
Client and signing-agent accounts and profiles	While the account is open	Deleted within 30 days of account closure or a verified deletion request, except records the law requires us to keep
Signing-agent credentials (commission, E&O, background check, ID)	While the agent is active with GSP	Deleted with the agent account; unattached copies are removed by the 30-day rule
Declined or withdrawn signing-agent applications	1 year after the decision	Deleted at the annual records review

Record	Kept for	Disposal
Security and access logs	365 days	Deleted automatically (automated)
Point-in-time data copies inside the portal	35 days	Deleted automatically (automated)
Off-site backups	Daily data snapshots 90 days; document copies 35 days after the original is deleted	Expired automatically by the backup storage rules (automated)
Paper loan documents handled by signing agents	Only for the appointment	Returned to the client by tracked courier or hand delivery as instructed; misprints and spare copies are cross-cut shredded. GSP never stores paper loan documents
Incident records and post-incident reviews	5 years	Deleted at the annual records review
Destruction log (what was deleted, when)	5 years	Deleted at the annual records review

3. How destruction is done

- Electronic records: deleted through the storage service, after which the provider’s secure-deletion process applies. Automated deletion runs every day; anything still referenced by an open order or account is never deleted.
- Backups: copies expire on the schedule above, so deleted information leaves the backups within 35 days (90 days for daily data snapshots).
- Devices and media: wiped with a secure erase or physically destroyed before reuse or disposal.
- Paper: cross-cut shredded, or destroyed by a bonded shredding service that provides a certificate of destruction.

4. Records of destruction

Each automated deletion is logged with the file, the rule that applied and the time, and copied to the off-site backup. The annual records review is documented by the security contact.

5. Requests from individuals and clients

Requests to delete personal information are verified and completed within 30 days, except for information GSP must keep by law or contract, in which case the requester is told what is kept and why. Clients may request return or deletion of their documents when a relationship ends.

POLICY 6

Business Continuity and Disaster Recovery Policy and Plan

How GSP keeps working through an outage and restores its systems, with a tested recovery time objective of 4 hours and recovery point objective of 24 hours.

1. Purpose and objectives

This policy and plan keep GSP's critical services running, or restore them quickly, after a disruption: a provider outage, data loss or corruption, a cyber attack, or loss of key people.

Objective	Target
Recovery Time Objective (RTO): time to restore the portal after a disaster	4 hours
Recovery Point Objective (RPO): maximum data loss, measured in time	24 hours
Bad release rolled back	15 minutes

2. Critical functions and manual workarounds

Function	If the portal is unavailable
Order intake	Clients email or phone orders to GSP staff, who log them
Agent assignment	Staff call and email signing agents from the agent roster export
Document exchange	Clients send packages directly to the assigned agent through their own secure channel
Status updates	Staff update clients by phone and email until the portal is back, then enter the history

3. Resilience and backups

- The portal runs on Vercel's managed platform across multiple availability zones; code is in a private GitHub repository, so the application can be redeployed at any time.
- Portal data and documents are stored in Cloudflare R2 (Eastern U.S.), which keeps redundant copies within the region.
- Every day an automated job copies all data and documents to a separate backup bucket in a different region (Western U.S.). Backup copies of documents and the daily data snapshots cannot

be deleted or overwritten by anyone for 30 days (an immutability lock), which protects against ransomware and mistakes. Daily snapshots are kept for 90 days.

- Inside the portal, the first change of each day to a data file keeps a copy of the previous version, and simultaneous edits are detected, so nothing is silently overwritten.
- Backup results are logged, and a failed backup alerts the security contact.

4. Recovery procedures

Scenario	Recovery
Faulty release	Roll back to the previous deployment in the hosting dashboard, then fix forward
Records corrupted or deleted	Restore the affected data files from the most recent good daily snapshot; restore deleted documents from the backup copy
Storage region lost or unavailable	Point the portal at the backup bucket (one configuration change and redeploy), then rebuild the primary from it
Hosting provider outage	Communicate with clients and agents, use manual workarounds, and redeploy from source control once service returns or to an alternate project
Email provider outage	Staff contact clients and agents directly; queued notifications are re-sent
Loss of key person	Infrastructure credentials are held in a shared password vault accessible to GSP management

5. Communication

Clients and signing agents with active orders are told about an outage expected to last more than one hour, with an estimate and the manual workaround, and again when service is restored.

6. Testing

A restore test is run at least once a year and after major changes to storage or backup. The test restores a full copy from the off-site backup into an isolated location, checks every record and document, and runs the portal against it. The time taken and the age of the restored data are measured against the RTO and RPO. Results and any fixes are recorded below.

Restore test log

Date	Scenario	Measured	Result
November 2, 2026	Full restore of all data and documents from the off-site backup into an isolated location, then the portal run against the restored copy	Data restored in under 1 minute (278 files, 551 MB, 15 seconds) plus a few minutes to switch the portal over, against the 4-hour RTO. Data loss at the time of the test was under 1 hour, against the 24-hour RPO	Passed. Every record matched the backup snapshot, all 269 documents were byte-identical to the live copies, and orders and documents opened normally through the portal. The test copy was then deleted