

Security overview

How TitleMagic protects client data. Updated October 18, 2026.

TitleMagic lets title and escrow teams send clients a secure Magic Link to fill and sign forms, with no client login. This overview describes the controls we operate today. The live version, with our policies, is at <https://gettitemagic.com/trust>.

TitleMagic does not currently hold a third-party security certification or audit report (for example SOC 2 or ISO 27001). This material describes the controls we operate; it is not a certification, and it is not a substitute for your own vendor review.

Encryption at rest and in transit

- In transit: every page and API is served over HTTPS (TLS), and browsers are told to use HTTPS only (HTTP Strict Transport Security, one year).
- At rest, fields: Social Security numbers, bank account and routing numbers, tax ID numbers and any other field marked sensitive are encrypted with AES-256-GCM before they are stored.
- At rest, documents: files a client uploads (a driver's license, formation documents) are encrypted with AES-256-GCM on disk. They have no public URL and can be downloaded only by a signed-in user of the company that sent the form.
- Keys: the encryption key is held in server configuration, separate from the database. Keys can be rotated, and stored data is re-encrypted under the new key.
- Passwords are stored only as salted hashes.

Two-factor login

- Staff can protect their sign-in with two-factor authentication: an authenticator app plus single-use backup codes.
- Account Owners can require two-factor for everyone in their company. TitleMagic administrator accounts must use it.
- Signing in from a new device or location sends an email to the account holder.
- Companies can also require each client to enter a 6-digit code, emailed to them, before a Magic Link form opens. Codes expire after 10 minutes and work once.

Access roles

- Each company's data is isolated: a signed-in user sees only submissions sent by their own company.
- Owners manage company settings, billing, team members, templates, data retention and bulk exports. Processors send forms, resend links, view submissions and download signed PDFs. These limits are enforced on the server.
- Sensitive values are masked in the dashboard (for example ***-**-1234). Showing a full value takes an explicit click.
- TitleMagic administration pages return "not found" to everyone except designated administrators, who must have two-factor enabled.

Audit trails

- Signing: for every signature we record the date and time, IP address, browser, signature method, the full legal name typed and the version of the e-sign consent shown. The signed PDF carries the audit trail and the consent text.
- Tamper evidence: a SHA-256 fingerprint of each final signed PDF is saved, so a later change to the stored file is detectable.
- Access log: every reveal of a sensitive value, every document and signed-PDF download, every bulk export, every CSV download and every “send to file email” is recorded with the user, time, IP address and browser. If the log entry cannot be written, the data is not released.
- Administrator actions that change a customer account (such as granting complimentary access, resetting two-factor or deleting a company) are recorded in an audit log.

Backups and restore testing

- Every night we back up the production database and every stored file (uploaded documents, signed PDFs and logos), together with the application configuration. Backups are encrypted with AES-256 before they are stored, in an encrypted repository on our server.
- We keep 7 daily, 4 weekly and 6 monthly backups.
- Every week an automated test restores the newest backup into a separate test database and a temporary folder, compares record counts and the checksum of every stored file, and checks the backup’s integrity. A failed backup or failed test emails our owner.
- Before every production release we also take a full backup and restore it into a test database; the release stops if record counts differ. A failed release rolls back automatically to the previous build.

Data retention and deletion

- By default, client data is kept while the account is active. An Owner can instead choose a retention period (1, 3 or 7 years, or up to 30), after which each submission is deleted automatically. The Owner can choose to keep an encrypted copy of the signed PDF.
- Owners can export all records in one click: signed PDFs, uploaded documents and CSV files of every answer.
- If a subscription ends, the account stays available read-only for at least 30 days so records can be downloaded. Submission data and documents are permanently deleted 90 days after cancellation, with reminders to account Owners beforehand.
- Deletion applies to the live system. Backups are not edited when data is deleted: deleted data ages out of the nightly backups within six months, and earlier pre-release backups are kept as they were taken.

Incident response

- We have a written incident response policy covering detection, containment, investigation, notification and review.
- If we learn of a security incident affecting personal information in our systems, we notify affected customers without undue delay so they can meet their own obligations, and give other notices the law requires.
- Report a concern to security@gettitemagic.com.

Hosting

- TitleMagic runs on servers leased from IONOS Inc. in the United States. The application, database, uploaded documents and our email server run there. We do not use a third-party email delivery service.

- Development and production are separate: the development site uses fake data only and has its own database, encryption key and secrets.
- Secure form pages opened from a Magic Link load no analytics, fonts or other resources from third parties.

Subprocessors

IONOS Inc. (United States)

Hosting, database, document storage and our email server. Client form data: Yes: client form data and documents are stored on the servers we lease (encrypted as described above).

Stripe, Inc. (United States)

Subscription billing and payments. Client form data: No client form data.

Google LLC (United States)

Google Sign-In for users who choose it; Google Analytics on our public website for visitors who accept analytics cookies. Client form data: No client form data.

What we never collect

- Wire instructions. TitleMagic has no feature to collect, store or send wiring instructions, so there is nothing in it to redirect. Forms carry a wire fraud advisory telling buyers to confirm any instructions by phone, using a number they already know.
- Payment card numbers. Subscription payments are entered on Stripe's hosted checkout, not on TitleMagic pages.

What we never email

- Full Social Security numbers, bank account numbers or routing numbers. Magic Link emails contain only the client's name, the form name, your company name, the link and its expiry date.
- Form answers in notifications. Notifications to processors say who signed and link to the dashboard.
- If you use "Send to file email", the summary leaves sensitive fields out entirely and the attached signed PDF masks them to their last four characters.

Contact

Security reports: security@gettittlemagic.com. Questionnaires and vendor reviews: support@gettittlemagic.com. Live status: <https://gettittlemagic.com/status>.