Security and data handling

Recce Room holds what a show keeps closest: unreleased scripts, schedules, crew lists, private homes, owners' tax and bank papers, deal terms. This is how the service handles that material today, written from what the software actually does, for a studio's IT security and procurement teams.

Everything below describes the service as it runs now. Where something isn't in place yet, it is listed under "Not in place yet" rather than left out. Recce Room holds no security certification (no SOC 2, ISO 27001 or TPN assessment) and doesn't claim one.

1. WHERE THE DATA LIVES	
Providers	The website and its server code run on Netlify. The database is Postgres, run by Neon. Files (photos, documents, PDFs) are kept in Cloudflare R2 object storage. Email goes through Resend, text messages through Twilio, payments through Stripe, and AI processing through Anthropic. All are United States companies; the privacy policy lists every provider.
Region	Data is stored with these providers in the United States and wherever they operate. There is no customer choice of region today.
Files are private	The storage bucket is private. Nothing in it has a public address: a file is reached only through a short-lived signed link the server issues after checking the person's access (most expire within 15 to 75 minutes), or, for encrypted files, is decrypted and sent by the server itself with no caching.
In transit	The site is served only over HTTPS; plain HTTP is redirected, and browsers are told to use HTTPS for a year (HSTS). Pages can't be framed by other sites, and file types can't be guessed by the browser. Files move to and from storage over HTTPS.

2. ENCRYPTION AT REST	
On top of the storage providers' own encryption of everything they hold, Recce Room encrypts its most sensitive material itself, with AES-256-GCM, before it reaches the database or storage. A database copy or a storage bucket on its own can't open these.	
Scripts and schedules	Every script revision, one-liner, Day out of Days, production calendar and shot list is encrypted with its own random key, and that key is locked with a master key. The script's breakdown (scene headings, characters) is encrypted the same way in the database.
Tax and bank papers	W-9s, ACH and direct-deposit forms, and certificates of insurance taken through an owner's or vendor's private link are each encrypted with their own key. Taxpayer ID numbers and bank routing and account numbers are encrypted in the database; only the last four digits are ever shown.
Crew and production papers	Call sheets, crew lists (and the phone numbers and emails read from them), timecards, show papers, safety bulletins, production company papers, and department files (SFX plans, set dressing, props, looks, department shares) are encrypted the same way.
Other sealed fields	Team chat messages (a key per show), a property owner's saved signature, two-step sign-in secrets, the tokens for services a team connects (DocuSign, Dropbox, SmugMug), and property owners' phone numbers and emails in the owner directory.
What relies on the provider's encryption only	Photos and video, floor plans, maps, blank and filled forms, signed agreements, permit papers, shared documents and scans from the phone app are stored in the private bucket without Recce Room's own extra layer. They are still private and reached only through access checks and short-lived links.
Keys	Encryption keys are held as secrets in the hosting environment, never in the code or the database. They are not in a dedicated key-management service, there are no customer-managed keys, and there is no scheduled key rotation (see "Not in place yet").

3. SIGNING IN	
Passwords	Stored only as bcrypt hashes. New accounts need at least 10 characters. Sign-in takes the same time whether or not the email has an account.
Sessions	A random token in a secure, HTTP-only cookie, kept on the server only as a hash. A session lasts 30 days. Signing out ends it. Every session (web and phone) ends when the password is reset, when someone is removed from a team, or when an account is locked or deleted.
Two-step sign-in	Available on every account, using any authenticator app (time-based codes), with ten single-use recovery codes. Each code works once. The account owner can see which team members have it on.

3. SIGNING IN (CONTINUED)	
Guessing limits	Sign-in stops after 10 failed tries per network address or per email in 15 minutes, two-step codes after 6, and password-reset requests are limited too. Network addresses are kept only as a keyed hash, and these records are cleared after two days.
Password reset	A single-use link that lasts one hour. Asking again cancels the earlier link. With two-step on, a reset doesn't sign anyone in.
The phone app	Signs in the same way and keeps its own key, stored on the server only as a hash, which lapses after 90 days without use and is removed at sign-out. Face ID, Touch ID and fingerprint unlock stay on the phone. Documents kept for offline use stay encrypted on the phone and are cleared at sign-out and at the end of the day.

4. WHO SEES WHAT	
Every account is closed to every other account, and inside an account each person sees only the shows they were invited to, with the access they were given.	
Accounts are separate	Each request is checked against the account and the show it belongs to. One subscriber's shows, people, papers and photos are never visible to another subscriber. (The one deliberate exception is the opt-in owner directory below.)
The Locations team	Legal papers (agreements, W-9s, insurance, permits) open only to the account owner and the people on that show's Locations list. Full tax IDs and the W-9 and bank files themselves open only to the account owner, Location Managers and Location Coordinators, and every opening is logged.
Departments and crew	Crew are invited to one show with a job title, and see only what that title's access boxes allow. Department titles get no money or legal access by default. The account owner can change any box, and removes someone's access at once.
Approvers	A spend needs two different people: the Location Manager and one of the UPM, Line Producer or Accountant. Approvers see what they're approving, never a tax ID.
Department photos	Pictures taken in the app are held for their department head until released, so not even the account owner sees them first.
Prices	Site fees and other costs show only to the account owner and the show's Locations team, never on crew pages or client view links.
Kill switch	The account's subscriber can cut off a show in one step: every crew member's access, invitations and the client view link end at once. Recce Room's operators can also lock an account or a person, which signs them out everywhere.
Recce Room staff	The terms of service treat a show's material as confidential: our people open it only when the account asks for help, to keep the service secure and working, or when the law requires it, and we tell the account owner first about a legal demand unless the law forbids it.

5. LINKS, WATERMARKS AND ATTACHMENTS	
Material leaves Recce Room mostly as private links rather than files, and every link is long, random and can't be guessed.	
Client view links	Open only with a password, a one-time code emailed to listed addresses, or (if the owner chooses) to anyone with the link. They can carry an end date, be turned off or replaced at any time, and every view is logged. An optional on-screen watermark shows the viewer's name and the date.
Gallery links	Open only with a one-time code sent by text or email, and end after 30 days. Markups are saved with the viewer's name and date drawn into the image.
Document links	Private document links end after 14 days; a W-9 or bank-form upload request after 21; a property owner's link two weeks after the show wraps (or 90 days) and opens only with an emailed code; a crew view link after 120 days unless changed. PDFs sent this way carry the recipient's name and email on every page.
Scripts	Every view of a script is stamped with the viewer's name, email and time on every page, and logged.
Wrap photos	Location photos in the wrap files that go to production are watermarked with the show's name across the whole frame.
Attachments	Tax and bank papers are never emailed, and signing and approval emails carry only a title and a link. Some things a user chooses to send do go as attachments: itineraries, lookbooks, overhead maps, permit applications sent to a permit office, and crew phone contacts sent as a contact file.

6. AUDIT TRAILS	
Signed documents	Each signed document has an audit page: how the signer was identified, when, and fingerprints (SHA-256) of the blank form, the version sent and the signed result, plus its approvals.
Approvals	Each approval or refusal is recorded with who, when, and a fingerprint of the exact version approved.
Opens and downloads	Script views, W-9 and bank-form openings, client view-link visits, gallery and crew-link opens, PDF-send opens and approved downloads are recorded.
Account events	An event log records actions across a show; kill-switch use, operator locks, link revocations, account erasures and every property-line owner lookup are logged.
Limits	These logs are ordinary database records, kept while the account exists. They are not yet write-once or tamper-evident, and there is no customer-facing export of the full event log yet.

7. AI	
Provider	Recce Room's AI features use Anthropic's Claude models through Anthropic's commercial API, under terms that don't let Anthropic train on the material. No other AI provider is sent customer material.
Only after approval	Reading a script into a detailed breakdown, reading crew lists, timecards and old crew maps, and tagging photos run only when the account approves an estimate for that job. The pages, images or text in that job are sent to Anthropic and the results come back to the show.
Small automatic uses	With AI switched on for the site, a few thumbnails of a gallery are sent to choose its cover photo, before-and-after photo pairs are checked, and the words typed into photo search are interpreted. User-started research (restaurant ideas, permit-office lookups) sends only the place and the question.
Never sent	Team chat is never sent to an AI model. Tax and bank numbers are never sent.

8. EMAIL AND TEXT MESSAGES	
Sending	Email is sent through Resend from Recce Room's own domain, as "<account> via Recce Room", with replies going to the account. Text messages go through Twilio, are kept short, and their contents and codes aren't written to logs.
What's in them	Emails are notices with a link back into Recce Room. They never contain tax IDs, bank details or script pages; a new script draft is announced with counts only. Some emails do name people and places (a permit application, a note someone left), because that is what they're for.
Incoming email	Call sheets emailed to a show's address are accepted only with the email service's verified signature, and their attachments are stored encrypted.

9. DELETION AND RETENTION	
Trash	Anything a customer deletes can be restored for 30 days, then a daily job removes it for good, files and all. The account owner can empty it sooner.
W-9s and bank forms	Kept five years, then deleted automatically, file and all.
Team chat	Deleted for everyone when the account owner wraps the show.
Trials	If a free trial ends without a subscription, its photos and videos are deleted 14 days later, after emailed warnings.
Closing an account	The account locks at once (nobody, including link holders, can open it) and every stored file and record is erased 30 days later. People who belong to no other account are anonymized. A record that the erasure happened is kept, with counts and nothing about the people.
Owners' removal requests	A property owner can ask for their details, floor plans or name on a parcel to be removed; we act within 48 hours and keep a do-not-add list.
Backups	The database provider keeps its own short point-in-time history, which is how a mistake at the database level would be undone. Recce Room has no separate backup copies of the database or files, and hasn't yet written down or tested a restore.

10. PRIVACY COMMITMENTS	
Whose data it is	A show's material belongs to the account that holds it. Recce Room acts on its behalf as a service provider and doesn't use it for its own purposes.
Never sold	Crew information is never resold. Recce Room sells no personal information, shows no advertising, and uses no tracking or advertising cookies.

10. PRIVACY COMMITMENTS (CONTINUED)	
Property owners	Property lines are shown to Locations teams only. Owner names from public records aren't stored for California or New Jersey. The pooled owner directory is opt-in by the account owner, entries carry no trace of who gave them, and owner phones and emails are sealed and reached only through an owner relay that asks the owner first. There is no bulk export, and lookups are logged and rate-limited.
Payments	Card payments happen on Stripe's own pages; Recce Room never receives a card number. Stripe's messages to Recce Room are checked for Stripe's signature.

NOT IN PLACE YET (ON THE ROADMAP)	NOT DONE
Certifications	No SOC 2 report, ISO 27001 certificate or TPN assessment, and none is under way. The studio package offers help with a studio's own security review (TPN).
Penetration test	No independent penetration test has been done yet.
Single sign-on	No SAML or OIDC single sign-on and no SCIM user provisioning. Signing in with Google, Apple or Microsoft accounts isn't built either. Single sign-on is planned for the studio package.
Required two-step	Two-step sign-in is optional for each person; an account owner can see who has it on but can't yet require it. There's no idle timeout on sessions and no "sign out of every device" button (a password reset does end every session).
Data residency	No choice of region; data is kept with US providers.
Key management	Keys aren't held in a dedicated key-management service or hardware module, there are no customer-managed keys, and there is no scheduled key rotation.
Encryption of everything	Photos, floor plans, forms, signed agreements and phone scans rely on the storage provider's encryption without Recce Room's own extra layer.
Tamper-evident logs	Audit logs are ordinary database records, not write-once, and there's no customer export of the full event log.
Backups and recovery	No separate backups beyond the database provider's point-in-time history, and no written, tested restore plan or recovery time objective.
Content Security Policy	The site sends no Content-Security-Policy header yet.
Written policies	No written information security policy, incident response plan, or vendor risk program yet, and no formal security training. The privacy policy commits to telling affected people about a breach as the law requires.
Automated checks	The automated test suite, type checks and linting must pass before every release goes live, but there's no automated dependency-vulnerability scanning yet.

Questionnaire answer sheet

Short answers to the questions a standard vendor security questionnaire (SIG-Lite or CAIQ style) usually asks. Each answer points to the numbered section in part 1 that backs it. "No" and "Not yet" are stated as such.

QUESTIONNAIRE

#	QUESTION	ANSWER	SEE
GOVERNANCE AND COMPLIANCE			
1.1	Do you hold SOC 2, ISO 27001 or a TPN assessment?	No. None yet.	§Gaps
1.2	Has an independent penetration test been done?	Not yet.	§Gaps
1.3	Do you have written security policies and an incident response plan?	Not yet as written documents. This packet and the privacy policy describe current practice; breaches are notified as the law requires.	§Gaps §10
1.4	Do you sell or share customer data for advertising?	No. Crew information is never resold; no advertising or tracking cookies.	§10
DATA LOCATION AND SUBPROCESSORS			
2.1	Where is customer data stored?	With US providers: Neon (database), Cloudflare R2 (files), Netlify (hosting). No region choice.	§1
2.2	Which subprocessors handle customer data?	Netlify, Neon, Cloudflare, Resend, Twilio, Stripe, Anthropic, Google Maps Platform, Fly.io (our map router), the US Census Bureau (address lookup), Apple and Google push. Listed in the privacy policy.	§1
2.3	Is customer data segregated between customers?	Yes, in the application: every request is checked against its account and show. Each account is closed to every other.	§4
ENCRYPTION			
3.1	Is data encrypted in transit?	Yes. HTTPS only, with HSTS; storage traffic over HTTPS.	§1
3.2	Is data encrypted at rest?	Yes, by the storage providers. In addition, scripts, schedules, tax and bank papers, crew lists, call sheets and chat are encrypted by Recce Room with AES-256-GCM. Photos, forms and signed agreements rely on the provider's encryption only.	§2
3.3	How are encryption keys managed?	Held as secrets in the hosting environment, per-file keys wrapped by a master key. No KMS or HSM, no customer-managed keys, no scheduled rotation.	§2 §Gaps
IDENTITY AND ACCESS			
4.1	Is multi-factor authentication supported?	Yes, authenticator-app codes with recovery codes. Optional per person; can't yet be required by the account.	§3 §Gaps
4.2	Do you support SSO (SAML/OIDC) and SCIM?	Not yet. Planned for the studio package.	§Gaps
4.3	How are passwords stored?	bcrypt hashes only; minimum 10 characters for new accounts; sign-in attempts rate-limited.	§3
4.4	Is access role-based and least-privilege?	Yes. Per-show invitations by job title with access boxes; legal and money access off for departments by default; tax IDs only for the owner and Location Managers and Coordinators.	§4
4.5	Can access be removed quickly?	Yes. Removing a person ends their sessions; the kill switch cuts off a whole show at once.	§4 §3
4.6	Who at the vendor can see customer data?	Only when the account asks for help, to keep the service secure and working, or when the law requires it. Confidentiality is in the terms of service.	§4
LOGGING AND MONITORING			
5.1	Are user actions logged?	Yes: signing, approvals, script views, tax-paper openings, link visits and downloads, kill-switch use and account events.	§6
5.2	Are logs tamper-evident and exportable?	Not yet. They are ordinary database records with no customer export of the full log.	§6 §Gaps

QUESTIONNAIRE (CONTINUED)			
#	QUESTION	ANSWER	SEE
DATA SHARING			
6.1	How is material shared outside the account?	Private, random links with codes or passwords and end dates; PDFs watermarked with the recipient; scripts stamped per viewer; views logged.	§5
6.2	Is sensitive data sent by email?	Tax and bank papers and script pages are never emailed. Some user-sent items go as attachments (itineraries, lookbooks, overhead maps, permit applications, crew contact files).	§5 §8
AI			
7.1	Is customer data used to train AI models?	No. AI runs through Anthropic's commercial API, which doesn't train on it.	§7
7.2	What data goes to the AI provider, and when?	Script, crew-list, timecard, map and photo reading only after an approved estimate; small automatic uses (cover photo, photo-pair check, search words). Chat, tax and bank numbers never.	§7
RETENTION AND DELETION			
8.1	Can deleted data be recovered, and when is it gone for good?	Restorable from the Trash for 30 days, then removed with its files.	§9
8.2	What happens to data when the customer leaves?	The account locks at once and everything is erased 30 days later; a record of the erasure is kept without personal details.	§9
8.3	How long are tax forms kept?	Five years, then deleted automatically.	§9
RESILIENCE			
9.1	Do you have backups and a tested recovery plan?	The database provider's point-in-time history only. No separate backups and no written, tested restore plan yet.	§9 §Gaps
APPLICATION SECURITY			
10.1	Do you use security headers and secure cookies?	HSTS, frame denial, no MIME sniffing, same-origin referrer; HTTP-only, secure cookies. No Content-Security-Policy yet.	§1 §3 §Gaps
10.2	Do you scan dependencies for vulnerabilities?	Not automatically yet. The test suite, type checks and linting must pass before every release.	§Gaps
10.3	Do you store payment card data?	No. Cards are taken on Stripe's own pages.	§10

Questions, a completed copy of your own questionnaire, or a call with the people who built Recce Room: info@recceroom.com, (213) 810-5115. Recce Room, Inc., 137 N Larchmont Blvd., Suite 800, Los Angeles, CA 90004.