Security and privacy at HelpCenter.io

Why HelpCenter.io

Your help center holds your company's knowledge, and sometimes information that isn't meant for everyone. Here's how HelpCenter.io protects it, and the controls you have over who can read and change what.

Infrastructure and encryption

- HelpCenter.io runs on Amazon Web Services (AWS).
- Your dashboard and your help center are served over HTTPS, and browsers are told to always use a secure connection.
- Custom domains get a free SSL certificate, issued automatically once your DNS record checks out.
- Your data is backed up several times a day. See Do you back up my content?

Your team's accounts

- Passwords are stored as secure hashes, never as plain text.
- Two-factor authentication adds a code from an authenticator app to every sign-in. See Turn on two-factor authentication.

- Repeated failed sign-in attempts are limited, and password reset links expire after 60 minutes.

- Everyone on your team has a role in each help center: Admin, Editor, Translator or Viewer, and the Owner has full control. Removing someone takes away their access immediately. See Roles and permissions.

- Only the account owner can see or change billing.

Who can read your help center

- **Public, Private or Password:** choose who can open your help center. New help centers start unpublished, so only your team sees them until you publish.

- **IP allowlist:** let in only the IP addresses you list.

- **Single sign-on (JWT):** readers sign in with your own login (Catalyst).

- **Embedding origins:** the widget and your embedded help center only load on the websites you list.

- **Article and category access:** keep single articles or whole categories private, or share an article by a secret link.

See Control who can see your help center.

What stays private

- Internal notes and team comments never appear on your help center.

- Drafts, AI drafts and staged changes (Catalyst, in early preview) stay in the dashboard until you publish them.
- Private and password-protected help centers aren't indexed by search engines and have no public MCP server.
- AI Answers only uses published articles the reader is allowed to see. See AI and your data.

API keys and connected apps

- API keys are either **Read only** or **Read & write**, and can read team notes only if you allow it. When you delete a key, requests that use it stop working immediately.
- A key keeps working after the person who created it leaves your team, so delete keys you no longer need.
- AI agents and other apps you connect can only reach the help centers you choose. Disconnect them at any time under **Connected Apps** in your account.

Payments

Card details go straight to our payment processor, Braintree, a PayPal service. HelpCenter.io doesn't store card numbers. See Are my payment details secure?

How we test

Our automated test suite includes security tests. They check, for example, that one customer's help center can't read or change another's data, and that attacks such as cross-site scripting, request forgery and SQL injection are blocked. We also check the software we build on for known vulnerabilities.

Questions or a security concern?

Email support@helpcenter.io. To have your account and its data deleted, write to us from the account owner's email address. For how we handle personal data, read our Privacy Policy.

Related articles

- Do you back up my content?
- AI and your data
- Turn on two-factor authentication
- Sign readers in with your own login (JWT SSO)