a. hub

AGENCY OPERATING SYSTEM · SECURITY

Security & Data Protection

YOUR DATA, WALLED OFF · ENCRYPTED AT REST & IN TRANSIT · AUDITED

a.hub is the operating system agencies run their whole business on, under their own brand. Because we run our own agency on it, we are the first to feel anything that breaks — so security is built in, not bolted on. This overview describes the controls that protect your agency's and your clients' data. Every item is live in the product today.

Per-workspace data isolation | AES-256 encryption at rest | TLS / HSTS in transit | Two-factor authentication | Immutable audit log | Read-only client portals | Per-agency, revocable integrations | Automated backups + recovery

01 Data isolation — every agency is an island

Your workspace is walled off from every other agency on a.hub. This is enforced in the data layer, not left to convention.

- ✓ Every record carries a workspace (agency) id.
- ✓ Every read is scoped to the signed-in agency and **fails closed** — if the scope is ever missing, the system returns nothing, never another tenant's data.
- ✓ It is enforced automatically: a build cannot ship an unscoped read or write — our CI checks block it before release.
- ✓ An automated cross-tenant probe signs in as one agency and attempts to reach another's data across dozens of pages; we also crawl the live product. These checks keep coming back clean — **zero cross-agency leaks across 43 pages**.

02 Encryption — at rest and in transit

Your credentials and traffic are encrypted end to end.

- ✓ API keys and connected-account tokens are encrypted at rest with **AES-256**. They are decrypted in memory only when a feature uses them, never written to logs, and never returned to the browser.
- ✓ All traffic runs over **TLS/HTTPS**, with HSTS (strict transport security) enforced.
- ✓ Passwords are hashed one-way with a strong algorithm — never stored in plain text.

03 Access & authentication

Access is verified on the way in and scoped once inside.

- ✓ **Two-factor authentication** is available on login.
- ✓ Role-based access — each person sees only what their role allows.
- ✓ Sessions carry an expiry and are re-verified against the account on every request.

04 Accountability — an audit log you can't edit

Sensitive actions are recorded in a way no one can quietly rewrite.

- ✓ Every meaningful action — finance, HR, provisioning, and any “view as” / impersonation — is written to an **immutable, insert-only** record.
- ✓ The log is append-only: entries can be read, never edited or deleted.

05 Client portals — strictly read-only

Your clients get a branded, view-only cockpit.

- ✓ A client sees only their own account — their reports, approvals, requests and invoices.
- ✓ Never another client, never your costs or margins, never an internal note.

06 Integrations & keys — you stay in control

You connect your own tools, and you can disconnect them at any time.

- ✓ Each agency connects its own accounts (QuickBooks, Meta, Google). Tokens are stored per-agency, encrypted, and never shared across agencies.
- ✓ We request the minimum access a feature needs and are read-only where possible.
- ✓ Any connection can be revoked from settings at any time; data already synced stays, nothing new is pulled.

07 Application & infrastructure hardening

The platform ships with defensive defaults and runs on managed enterprise cloud.

- ✓ Modern security headers on every response: HSTS, clickjacking protection, MIME-sniffing protection, a strict referrer policy and a locked-down permissions policy.
- ✓ Hosted on managed cloud infrastructure (enterprise providers) with **automated database backups and point-in-time recovery**.
- ✓ Every change ships through automated checks (types, the tenancy guardrails above, and tests) before it can reach production.

08 Your data is yours

You own your data and can take it with you.

- ✓ Export your data at any time.
- ✓ On offboarding, we export and then remove your data on request.

09 Responsible AI (Brand Brain)

The AI assists your team; it never acts on its own.

- ✓ The Brand Brain produces **drafts only** — a human always reviews and approves before anything is used.
- ✓ One client's brain is never used to inform another's; your content is not shared between clients.

WHERE WE ARE HONEST

We are **not** yet SOC 2 or ISO 27001 certified — formal certification is on our roadmap as we scale, and we won't imply otherwise. Until then, isolation is enforced in code, checked on every release, and backed by encryption, two-factor authentication and an immutable audit log. We're glad to complete your security questionnaire, sign an NDA, and give your team a live login to verify the controls first-hand. One deliberate boundary worth noting: a.hub records payroll as paid but **never moves money** — there is no bank transfer.

This overview describes a.hub's current security controls and is provided for evaluation. It is not a contractual commitment or warranty; specific commitments are set out in your service agreement. Last reviewed 2026-07-09.