Kaam360 security questionnaire answers

Version 2026-10 · 70 questions · kaam360.com/security

Answers to the questions larger buyers usually ask (in the style of SIG Lite and the Cloud Security Alliance CAIQ). Every answer describes Kaam360 as it is today. Answers marked Policy describe how the people who run Kaam360 work (written down in docs/security in the code repository); the others are enforced by the software or the set-up and can be checked in the code, which is on GitHub. Kaam360 has not yet been through an outside audit (SOC 2, ISO 27001) or an outside penetration test; this document does not claim otherwise.

Answers marked Policy describe how the people who run Kaam360 work (a written rule rather than something the software enforces). The written policies are in docs/security in the code repository and summarised on kaam360.com/security.

Company and scope

CO-1 **What is the service and how is it delivered?**
Kaam360 is a web application (projects, tasks, time, customers, sales, invoices, support desk, email marketing) used in the browser. It runs as one installation for all customers (multi-tenant) on a server rented by Kaam360, with each organization's data kept apart in the software.

CO-2 **Where is the data hosted?**
On a dedicated server rented from Velia (velia.net), running Windows Server with IIS and PostgreSQL, behind Cloudflare. Encrypted backup copies are stored with Backblaze B2. Country of the data centre: [owner to fill in].

CO-3 **Do you have a written information security policy, and who owns it?**
Policy
Yes. The policy set is in the code repository under docs/security (information security, access control, change management, incident response, backup and recovery, vendor management, data retention, acceptable use, business continuity). The business owner owns it and reviews it yearly.

CO-4 **Have you been audited (SOC 2, ISO 27001) or had an outside penetration test?**
Not yet. We keep a readiness checklist (docs/security/readiness-checklist.md) of what is in place and what is missing, and a written plan for commissioning an outside test. We will say on our public Security page when either has happened.

CO-5 **How many people have access to production systems?**
Policy
The business owner, plus the developers and platform administrators listed in the quarterly access review. The platform panel lists its administrators; GitHub lists repository access.

CO-6 **Can you sign a data processing agreement?**
Our Data processing page (kaam360.com/dpa) sets out the terms; a signed copy, including standard contractual clauses where needed, can be requested through Help & support.

Access control and authentication

AC-1 **How do users authenticate?**
Email and password (at least 10 characters on sign-up), optionally with two-step sign-in (TOTP authenticator app plus recovery codes). Organizations can use single sign-on with SAML 2.0 (Okta, Microsoft Entra ID, Google Workspace and other providers) or Google and Microsoft sign-in.

AC-2 **Can multi-factor authentication be enforced for all users of our organization?**
Yes. An organization administrator can require two-step sign-in for everyone; people without it are taken to set it up before they can do anything else. People who sign in through the organization's SAML identity provider are exempt because that provider's checks apply.

AC-3 **Do you support SSO, and can passwords be disabled?**
Yes. SAML 2.0 with signature, audience, recipient, age and one-time-use checks; email domains must be verified; an organization can make SSO the only way in, keeping named break-glass administrators; groups can be mapped to roles.

AC-4 **How are passwords stored?**
Hashed with ASP.NET Core Identity's PBKDF2 hasher with a per-password salt. They are never stored, logged or shown in readable form, and cannot be looked up by Kaam360 staff.

AC-5 **What protects against brute force?**
Five wrong passwords lock the account for 15 minutes. Sign-in attempts are also limited per network address (30 per 10 minutes), and password reset and sign-up requests are limited per address and per email.

AC-6 **Is there role-based access control?**
Yes. Built-in Admin, Manager and Employee roles, and organizations can create their own roles choosing exactly which rights each has. Project membership further limits what a person sees. Customer users (client portal) only see the projects they are given and only what they are allowed to do.

AC-7 **How are sessions managed?**
Cookies are HttpOnly, Secure and SameSite. The application session expires after 30 days without use (sliding); the platform panel after 2 hours; the client portal after 8 hours. Anyone can sign out at any time. Switching a person off signs them out within a minute.

AC-8 **Can access be restricted by network?**
Yes. An organization can list the IP ranges from which its people may use the application; anyone elsewhere sees an explanation instead of the page.

AC-9 **How is access to your own infrastructure controlled?**
Policy
The platform panel has its own sign-in with TOTP two-step; the server, GitHub and vendor accounts use personal accounts with two-step sign-in; the database user the site runs as is not a superuser. Access is granted by the owner for a named person and removed the same day someone leaves.

AC-10 **Do you review access periodically?**
Policy
Quarterly, using the template in docs/security/access-review-template.md, covering the platform panel, GitHub, the server, vendor accounts and secret rotation. Completed reviews are filed in the repository.

AC-11 **How are API credentials handled?**
API keys and OAuth tokens are random, shown once, and stored only as SHA-256 hashes with a short prefix for identification. OAuth 2.0 for connected apps uses PKCE, scopes and per-app consent; keys can be revoked by an administrator at any time. API calls are rate-limited and return standard rate-limit headers.

AC-12 **Is customer data accessible to your staff?**
Policy
Kaam360 staff do not open customers' workspaces. The platform panel shows organization-level facts only (plan, number of people, usage, support tickets). Any exception needs the customer's written request and is recorded.

AC-13 **Can administrators review and export who did what?**
Yes. Organization administrators can filter the activity log by kind, person and dates and download it as a CSV file; records are kept for 400 days.

AC-14 **How quickly is access removed when one of our people leaves?**
As soon as an administrator switches the person off: their session ends within a minute and they can no longer sign in. With SAML single sign-on and 'SSO only', removing the person in your identity provider also stops new sign-ins.

Data protection and encryption

EN-1 **Is data encrypted in transit?**
Yes. All connections use HTTPS (TLS) with a Let's Encrypt certificate on the server and Cloudflare in front; HTTP is redirected and HSTS is sent. Sign-in cookies are marked Secure. Connections to the mail server use TLS.

EN-2 **Is data encrypted at rest?**
Partly. Backups are encrypted with AES-256 (a passphrase only Kaam360 holds) before they leave the server, so Backblaze cannot read them. Secrets saved on the platform panel are sealed with the server's data-protection keys (DPAPI). Passwords, API keys and tokens are stored as hashes. The live database and uploaded files on the server are not encrypted by the application itself; whole-disk encryption of the server is [owner to confirm with the hosting provider].

EN-3 **What encryption algorithms and key management are used?**
TLS 1.2 and 1.3 at the edge; AES-256 for backups with a key derived from the passphrase; SHA-256 for stored credentials and tokens; PBKDF2 for passwords; ASP.NET Core Data Protection (keys stored on the server, protected with DPAPI) for sealed settings and signed links. The backup passphrase and vendor keys live only in the server's private settings file and the owner's password manager.

EN-4 **How is data of different customers separated?**
Every record carries its organization, and the data layer applies that filter to every query (EF Core global query filters) for the signed-in person's organization; uploaded files are stored in a folder per organization and handed out only after a permission check. The automated test suite checks before every release that one organization cannot read another's records.

EN-5 **Do you process payment card data?**
No. Payments are handled by Paddle (merchant of record, PCI DSS Level 1); card details are entered in Paddle's own form and never reach Kaam360.

EN-6 **Which third parties process customer data (sub-processors)?**
Velia (hosting), Cloudflare (DNS and edge), Backblaze (encrypted backups), Hostinger (email), Paddle (payments), Anthropic (only if an organization switches on the AI assistant, and then only the question, matching help pages and the asker's open task titles), GitHub (code and deployment, no customer data). The public list is at kaam360.com/dpa and is updated before any addition.

EN-7 **Can customers export their data?**
Yes. An administrator can download everything the organization has put in, as spreadsheets plus files, from Settings > Data & privacy. Data is also reachable through the API.

EN-8 **Can customers delete their data?**
Yes. An administrator can delete the whole organization; it is erased after a 14-day delay that can be cancelled. Backup copies rotate out within about 30 days. Individual people can be removed by an administrator.

EN-9 **Is customer data used for anything other than providing the service?**
No. It is not used for advertising, sold or used to train AI models. The AI assistant, if switched on, sends the question and a few matching items to Anthropic, whose commercial terms exclude training on the data.

EN-10 **Can we bring our own encryption keys (BYOK)?**
No. Customer-managed keys are not offered.

Application security and change management

AS-1 **Do you follow a secure development lifecycle?**
Policy
Every change goes through a branch and a pull request explained in plain language, the regression test suite (about 380 tests covering permissions, tenant isolation, billing, email, backups, the API and migrations) must pass before every push, and deployment is started by hand with a typed confirmation. Documentation is updated in the same pull request.

AS-2 **Is code reviewed before release?**
Policy
Yes, through the pull request on GitHub; the owner or a reviewer reads and merges it. Emergency fixes still go through a pull request and the tests, and are reviewed within three working days.

AS-3 **How do you deploy, and can you roll back?**
Nothing deploys automatically. The 'Deploy to production' GitHub workflow builds on GitHub, backs up the database on the server first, keeps the previous program folder, applies database migrations and waits until

the new version answers /health and confirms it can save. Roll back: redeploy the previous commit or restore the kept folder and pre-deploy database copy.

AS-4 **Do you keep a change and deployment history?**
Yes. GitHub keeps every pull request (who, what, when) and every deployment run; the running version is shown at kaam360.com/health.

AS-5 **Are environments separated?**
Development happens on developers' machines and scratch databases; the test suite runs against a copy, never the live database; the live site is one production environment. There is no shared staging server today.

AS-6 **How do you protect against the OWASP Top 10?**
Injection: all database access goes through Entity Framework Core with parameterised queries (no string-built SQL for user input). XSS: Blazor encodes output by default; the few places that render HTML are reviewed. CSRF: anti-forgery tokens on every form; API endpoints use bearer tokens and disable cookies. Access control: permission checks in the service layer, tested. Security headers: HSTS, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, frame-ancestors (clickjacking), Cross-Origin-Opener-Policy. SSRF: addresses typed by customers (webhooks, mail servers) must be public https hosts and are checked again at connection time.

AS-7 **How are uploaded files handled?**
Stored under a random name with a checked extension in a folder per organization, outside the web root, with per-organization storage limits; downloaded only after a permission check, with the original name in Content-Disposition and nosniff set so the browser never runs them.

AS-8 **Do you check dependencies for known vulnerabilities?**
Yes, with 'dotnet list package --vulnerable --include-transitive' during the internal security review (October 2026: one vulnerable component found and updated; every scanned project is now clean) and before releases. Automatic Dependabot alerts on GitHub are not switched on yet; that is a listed next step.

AS-9 **Do you perform security testing?**
An internal security review of authentication, authorisation, headers, rate limits, uploads, SSRF guards, SQL use and secrets was done in October 2026 (docs/security/internal-review-2026-10.md), with the findings fixed. Automated tests cover security headers, tenant isolation, permissions and rate limits. An outside penetration test has not been done yet; the plan for commissioning one is written.

AS-10 **Is there a public way to report vulnerabilities?**
Yes. The Security page asks reporters to use Help & support inside the app or the contact form, promises a reasonable time to fix before disclosure, and promises no action against good-faith reporters.

AS-11 **Do you have an API, and is it documented and rate-limited?**
Yes. API v1 (keys) and API v2 with OAuth 2.0 for connected apps, documented at kaam360.com/developers with OpenAPI. Keys and apps are limited per organization, scoped, rate-limited (429 with Retry-After) and revocable; webhooks are signed.

AS-12 **Are outgoing webhooks authenticated?**
Yes. Every webhook carries a timestamp and an HMAC-SHA256 signature made with a secret per webhook (headers X-Kaam360-Timestamp and X-Kaam360-Signature), so the receiver can check it came from Kaam360 and was not replayed. Webhook addresses must be public https addresses.

Logging, monitoring and incident response

IR-1 **What is logged?**
An activity log per organization: sign-ins and failed sign-ins, password changes, people added or switched off, rights and settings changes, data downloads, deletion requests and many business actions, with the actor, time and network address; kept 400 days; exportable as CSV by administrators. The platform panel has its own activity log. Server logs are written with Serilog. Passwords, codes and keys are never logged.

IR-2 **How do you monitor availability?**
A GitHub-hosted check asks the site's /health (which tests the database and the ability to save) and sign-in page every 5 minutes from outside our network and publishes the result to the public status page, which

stays up when the server is down. The nightly backup emails us on failure.

IR-3 **Do you have an incident response plan?**
Policy
Yes, docs/security/incident-response-plan.md: who leads, how customers are told (status page and emails), containment steps, legal notification deadlines, and a post-mortem within 10 working days.

IR-4 **How and when are customers notified of a breach?**
Policy
Affected organizations' administrators are told by email without undue delay and within 72 hours of us becoming aware, with what happened, which data, what we did and what they should do. This is promised on the Data processing page.

IR-5 **Is there a public status page and can we subscribe?**
Yes: the status page (linked from kaam360.com/status) shows current state, 90-day uptime, incidents and planned maintenance. Anyone can subscribe to incident emails with a double opt-in and unsubscribe with one click.

IR-6 **Have you had any security breaches in the last three years?**
No known breach as of October 2026. Any future incident will have a post-mortem filed in the repository.

IR-7 **Is access by your own staff to customer data logged?**
Kaam360 staff do not open customers' workspaces. Everything platform administrators do in the platform panel (for example suspending an organization, changing settings, posting incidents, making a backup) is recorded in the platform activity log with who, what and when.

Backup, recovery and business continuity

BC-1 **How often is data backed up and where?**
Every night (after 02:00 UTC): the whole database and every uploaded file, encrypted with AES-256 on the server, sent to a private Backblaze B2 bucket; the newest 30 copies are kept. The database is also copied before every deployment (newest 20 kept on the server). 'Back up now' is available in the platform panel.

BC-2 **Are backups tested?**
Policy
The 'PostgreSQL backup test' workflow backs up, restores into a scratch database and compares every table; policy is to run it every quarter and to do a full restore on a separate machine yearly with the restore tool, which refuses a wrong passphrase or a damaged file. The Go live page records that a restore was tested.

BC-3 **What are your recovery objectives?**
Policy
Recovery point: at most 24 hours (one night to the next). Recovery time: a damaged server rebuilt within one working day; a wrong deletion restored within hours. These are targets, not contractual guarantees.

BC-4 **Do you have a business continuity plan?**
Policy
Yes, docs/security/business-continuity.md: server loss (rebuild from backup with the setup script and redeploy), Cloudflare, Backblaze, Hostinger, Paddle and GitHub outages, and loss of the owner (emergency access to the password manager, which the owner still has to set up). There is no hot standby server; the honest recovery is a rebuild.

BC-5 **What uptime do you commit to?**
We publish measured uptime on the status page rather than a contractual SLA. Enterprise customers can ask for an SLA through sales.

BC-6 **Are backups stored in a different location from production?**
Yes. The encrypted nightly copies are stored with a different company (Backblaze B2), away from the hosting provider's server. The region of the bucket: [owner to fill in].

Vendor management, privacy and compliance

VM-1 **How do you assess vendors?**

Policy

Before adding a vendor that handles customer data, the owner reads its security and data-processing terms, records it in docs/security/vendor-management.md and updates the public Data processing page first; keys are limited to what the vendor needs; vendors are rechecked yearly.

VM-2 **Do your vendors hold recognised certifications?**

Cloudflare, Backblaze and GitHub publish SOC 2 reports; Paddle is PCI DSS Level 1. The hosting and email providers' assurances are to be filed by the owner (see vendor-management.md).

VM-3 **Will we be told before a new sub-processor is added?**

Policy

The Data processing page promises to update the list before adding another company that handles your organization's information. Customers who need to be told by email can ask for this in a signed DPA.

PR-1 **Do you comply with GDPR / applicable data protection law?**

We act as processor for our customers' data (controllers) under the Data processing terms at kaam360.com/dpa: processing only on instructions, confidentiality, sub-processor list, assistance with requests, breach notification, deletion or return at the end. The Privacy page covers our own processing (accounts, website visits, support). A signed DPA with standard contractual clauses can be requested.

PR-2 **What personal data do you hold about our users?**

Name, email, language, time zone, role, sign-in and activity records, and whatever the organization enters about them (for example time entries). Nothing is collected from users' devices beyond what the browser sends. The optional activity-tracking desktop app records only what the organization configures and is covered in its own guide.

PR-3 **Do you use cookies or trackers on the website?**

Only the sign-in cookie, the anti-forgery cookie and the language choice. Website visit counting is done by us without cookies or IP addresses; no advertising or analytics company is involved. Cloudflare passes the visit through.

PR-4 **How long do you keep data after a contract ends?**

When a subscription ends the workspace becomes read-only and nothing is removed, so the customer can export or resume. On deletion, erased after 14 days, out of backups within about 30 days. The activity log is kept 400 days; website visit counts 13 months (docs/security/data-retention-and-deletion.md).

PR-5 **Is data transferred outside our region?**

Data is kept on the rented server (country: [owner to fill in]) and with the vendors listed above, some of which are in the United States (Backblaze, Cloudflare, Paddle, GitHub, Anthropic). Standard contractual clauses are available on request.

PR-6 **How do you handle data subject requests (access, correction, deletion)?**

As processor, we pass a request from one of your people to your organization. Your administrators can correct a person's details, switch them off or remove them, and export all the organization's data; we help with anything they cannot do themselves.

People and physical security

HR-1 **Are staff trained in security?**

Policy

The people who run Kaam360 read and follow docs/security (acceptable use, incident response). There is no formal training programme yet; it is listed as missing in the readiness checklist.

HR-2 **Are background checks performed?**

Policy

No formal background checks. Access to production is limited to the owner and named people under the access-control policy.

HR-3 **What are the rules for staff devices?**

Policy

Screen lock, disk encryption and up-to-date software on any computer used for the server, GitHub or the platform panel; no customer data on laptops (acceptable-use policy).

HR-4 **Do people with access sign confidentiality agreements?**

Policy

Not yet as a formal step. The acceptable-use policy requires confidentiality; a one-page agreement for anyone given access is a listed next step in the readiness checklist.

PH-1 **What physical security protects the servers?**

The server is in the hosting provider's data centre (Velia); physical security is the provider's responsibility under its terms. The owner is to file the provider's security documentation (vendor-management.md).

PH-2 **How are secrets protected on the server?**

In a private settings file outside the code (never on GitHub, excluded by .gitignore) or sealed in the database with the server's data-protection keys, which Windows protects (DPAPI). The deployment never prints them.