Vendor Security Questionnaire

Service Desk Builder — AI Readiness Audit for Freshservice & Zendesk. Answers are true of our current setup; see servicedeskbuilder.com/security, /privacy, and /dpa.

COMPANY

What is Service Desk Builder?

Service Desk Builder is an early-stage software company providing an automated AI Readiness Audit for Freshservice and Zendesk service desks.

HOSTING

Where is the application hosted?

On Vercel's serverless infrastructure. Application data and product state are stored in Vercel KV (or equivalent managed key-value storage).

AUTHENTICATION

How is access to accounts controlled?

Authentication and account management are handled by Clerk. Team access uses organisation roles (Admin and read-only Viewer); write actions are restricted to Admins server-side.

API CREDENTIALS

Do you store our Freshservice/Zendesk API key?

No. The API key is held in server memory only for the duration of the audit or ticket-creation request. It is never written to any database, log file, cache, or persistent storage.

ACCESS SCOPE

What access does the audit use?

Read-only API access to count and measure configuration (categories, knowledge base, SLAs, routing, canned responses, ticket metadata). Audits make no changes.

WRITE ACCESS

Does the product ever write to our service desk?

Only the optional 'push tasks as tickets' feature, and only when explicitly enabled and confirmed per push. It creates remediation tickets you request; it never updates, closes, or reads other tickets.

TICKET CONTENT

Do you read or store ticket content?

No. We do not read or store raw ticket bodies, requester names, requester emails, or end-user contact details. Ticket description length is measured in memory and the text is immediately discarded.

DATA STORED

What customer data do you store?

Computed scores and metrics, audit history, connected platform and subdomain, limited category diagnostics, report state, client labels, MSP white-label assets, generated report outputs, and ticket IDs/URLs returned when you ask us to create tickets.

ENCRYPTION IN TRANSIT

Is data encrypted in transit?

Yes. All traffic is over TLS (HTTPS).

ENCRYPTION AT REST

Is data encrypted at rest?

Yes. Data is stored on encrypted, provider-managed infrastructure (Vercel / managed KV).

PAYMENTS

How are payments handled?

Payments are processed by Stripe. Card details are entered on Stripe's infrastructure and never touch our servers. We store billing and payment status only, not full card numbers.

SUBPROCESSORS

Who are your subprocessors?

Vercel (hosting/storage), Clerk (auth), Stripe (payments), Resend (transactional email), and Anthropic (optional AI remediation content). The Freshservice and Zendesk APIs are read during audits you initiate. A current list is available on request.

DATA RESIDENCY

Where is data processed, and how are transfers handled?

Data may be processed outside your region by the subprocessors above. Transfers rely on appropriate safeguards such as adequacy regulations, Standard Contractual Clauses, or the UK International Data Transfer Agreement.

DATA RETENTION

How long do you retain data?

Account and audit history are retained while your account remains active, unless you delete audits or request deletion. Anonymous product-usage event counters expire automatically.

DATA DELETION

How can we delete our data?

Email us at any time to request deletion. Some records may be retained where required by law or for fraud prevention.

LOGGING

Do logs contain sensitive data?

No. API keys and ticket content are never written to logs. Logs hold operational diagnostics only.

ACCESS MANAGEMENT

Who on your side can access customer data?

Access is limited to what is necessary to operate and support the Service. We are a small team and apply least-privilege and least-data principles.

BACKUPS

How are backups handled?

Backups and durability are managed by our infrastructure providers (Vercel / managed storage).

INCIDENT RESPONSE

Who do we contact about a security incident?

security@servicedeskbuilder.com. We respond within 2 business days and work with you on remediation.

VULNERABILITY DISCLOSURE

Do you have a responsible-disclosure process?

Yes. Report issues to security@servicedeskbuilder.com; please allow reasonable time to remediate before public disclosure.

SOC 2 / ISO 27001

Are you SOC 2 or ISO 27001 certified?

Not currently. We are an early-stage company; our controls are documented at /security and in our Privacy Policy and DPA. Not applicable at our current size.

PENETRATION TESTING

Do you perform penetration testing?

We do not currently commission formal third-party penetration tests. We rely on managed, regularly-patched provider infrastructure and minimal data collection. Not applicable at our current size.

COOKIES & TRACKING

Do you track users across sites?

No. We record anonymous product-usage events using a first-party session identifier only. We do not track across other websites and do not sell or share data with advertisers.

DPA

Is a Data Processing Addendum available?

Yes. Our DPA is published at /dpa, and a current subprocessor list is available on request.

SUB-TENANT ISOLATION

How is one customer's data isolated from another's?

Data is keyed per account owner and access is enforced by authenticated, server-side checks on every request.

AI PROCESSING

Is our data used to train AI models?

No. Optional AI remediation content is generated from structured issue metadata via Anthropic's API and is not used to train models.