

Data Handling

Measured against the Integrix codebase at commit `b1871d145`, 2026-10-19. Statements about our hosting provider are quoted from that provider's published documentation and are their assertion, not our measurement.

What Integrix holds

Integrix tracks IT integration work during a merger or acquisition. The data it stores is the working record of that program: applications, infrastructure, migration waves, tasks, decisions and sign-offs.

The database has 121 tables. The personal and identifying data they hold is workplace directory and asset information, in these classes:

Class	What it is	Where
Employee directory	Name, work email, UPN, phone, job title	<code>euc_master</code> , <code>workforce_roster</code> , <code>identity_users</code> , <code>team_members</code>
Directory scan results	UPN, display name, job title, device assignment	<code>ad_scan_results</code> , <code>intune_scan_results</code> , <code>device_fleet</code>
Mailbox records	Mailbox name, owner address	<code>mailbox_migration</code> , <code>shared_mailboxes</code>
Application accounts	Username and a salted script password hash	<code>coordinator_accounts</code> , <code>external_accounts</code> , <code>mgmt_accounts</code> , <code>team_accounts</code> , <code>tech_accounts</code>
Audit trail	Username, IP address, action, timestamp	<code>audit_log</code>
Network and asset identifiers	Device names, current and target IP addresses	<code>network_devices</code> , <code>network_tasks</code> , <code>infra_assets</code>

This list is read from the live database, not from the schema file in the repository, because a column can reach the live database through a migration script before the file is updated. The query we run is committed beside this document.

What Integrix does not hold

No column in the database holds a national identifier, date of birth, salary, payment card, bank account, health information, or any demographic or special-category attribute.

The exception, stated plainly. 59 columns named `notes` , across 59 tables, accept anything a user types, and description and comment fields add to that surface. Nothing stops someone

pasting sensitive information into a note. We do not scan those fields and we do not claim to.

Where it lives

One PostgreSQL database, hosted by Render in its Ohio region (AWS us-east-2) in the United States. The application and the database run on the same platform, in the same region. There is one production deployment.

Render states that its Postgres databases "are encrypted at rest using AES-256 data encryption," that "this encryption applies to both primary and replica instances, along with all backups," and that "external connections to your database are always encrypted using Render-managed TLS certificates." Render's security page lists SOC 2 Type 2 and ISO 27001 under Compliance. We have not read the reports, so we cite the listing rather than assert the attestations.

Traffic to `getintegrix.com` is HTTPS. HTTP redirects to HTTPS. HSTS is set to one year including subdomains. `X-Frame-Options: DENY`, `X-Content-Type-Options: nosniff`, `Referrer-Policy: strict-origin-when-cross-origin` and a `Content-Security-Policy` that forbids framing are present. These were read from live response headers on 2026-10-20. The session cookie is `Secure`, `HttpOnly` and `SameSite=Lax`; that is set in the application's production configuration, because a visitor who has not signed in is sent no cookie to read.

Database link. The application connects to its database over Render's private network, in the same region, and requires TLS on that link (`sslmode=require`). Render states that internal connections "optionally support TLS encryption using self-signed certificates," so the link is encrypted but the certificate is not verified. This is Render's internal network; traffic never leaves the platform. Certificate verification matters on public links, and the public link to this database is blocked.

Who can reach it

Access to the Integrix hosting account is limited to one person, with multi-factor authentication enabled.

Application accounts authenticate against salted scrypt hashes. No plaintext password is stored. A session expires after 30 minutes without activity. A password reset is performed by an Integrix coordinator and is written to the audit log; there is no self-service reset. Application accounts do not yet offer multi-factor authentication. It is on our plan, and this document will say when it ships.

Render is our sole hosting provider and therefore our processor. Render publishes its own subprocessor list, which we cite rather than summarize. It names four entries, each listed for "Hosting / Cloud Platform": Amazon Web Services, Google Cloud Platform, Cloudflare and ClickHouse Inc. All four are located in the United States.

Isolation

Between customers. Every engagement and every management account belongs to one company. A request from a company's account for another company's engagement returns a not-found page, and the attempt is written to the audit log. This holds for the engagement page, every workstream page and every data endpoint under them. It is enforced in one place in the code, before any route runs, and a test that stands up a second company and attempts to cross runs on every build.

Between engagements. Every login below coordinator is scoped to a single engagement. That scoping was tested directly: 95 cross-engagement attempts by three trust classes against a second live engagement, including 17 positive controls, changed zero rows, measured across 101 tables before and after.

The coordinator. One coordinator account exists. It belongs to Integrrix, is the only account that can reach more than one company, and is the account that creates engagements, creates and resets user accounts, and deletes engagements. No customer holds a coordinator account.

Appointment links. Integrrix sends end users a scheduling link containing a random token. Anyone holding the link can view, reschedule or cancel that appointment without logging in, which is what makes it usable by people who have no account. Tokens come from a cryptographic random source. A coordinator can revoke one. If your organization requires appointment access to sit behind a login, tell us before an engagement begins.

Artificial intelligence

Integrrix ships an optional assistance feature that calls Anthropic. It is inactive in production because no API key is configured. Activating it is a deliberate configuration change by Integrrix. No other AI vendor is called by Integrrix code. When the feature is inactive the interface labels its fallback output as simulated; a user is always told which is which.

Backups

Integrrix performs no backup of its own on the production backend. Render takes continuous backups of the database and can restore it to any point in the past 3 days, into a new database instance; it also produces logical exports, retained for seven days. A restore was tested on 2026-10-19 (the move rehearsal).

Logging

The platform writes application access and error logs. Render retains them for 7 days on our workspace plan. Render publishes no statement of which of its staff can read customer logs. We cannot answer that part today.

Contractual position

Integrix runs on Render's Hobby workspace, governed by Render's Terms of Service. Render publishes a Data Processing Addendum; its published page does not state which accounts it covers or how it is entered into, and we have not signed it. **We are not currently party to a Data Processing Agreement with our hosting provider.** That means we hold no contractual commitment from Render on breach notification timing, no Standard Contractual Clauses for EU or UK transfers, no contractual deletion timeline, and no audit rights. The practices described above are Render's published commitments to the market. If a Data Processing Agreement is a requirement for your organization, tell us and we will put one in place before an engagement begins.

Our commitments

Incident history. No security incident has affected Integrix or its data.

Deletion on request. On written request, Integrix deletes an engagement and all associated records within 30 days. Deletion removes every row in every table that carries the engagement's id, 102 of the 103 such tables at this commit, in one transaction. The exception is the audit log, which also carries the id but is deliberately retained.

Retention. Engagement data is retained for the term of the agreement and for 90 days after it ends, then deleted.

Incident response. Integrix acknowledges a reported security issue within 24 hours and provides an initial assessment within 72 hours. Contact: hello@getintegrix.com.

What we cannot answer yet

Which of our hosting provider's staff can read customer logs, and whether our hosting provider holds the attestations its security page displays. These are gaps in what our hosting provider publishes. We have named them here rather than answer around them, and this document is reissued when any of them closes.

Every factual claim here carries one of three kinds of support. Claims about our own code are re-derivable from the repository at the commit named above. Claims about our hosting platform are quotations from that vendor's published pages, read by a person on 2026-10-19. The rest are statements Integrix makes about its own account, deployment and history, which a reader cannot verify from either source: our plan tier, our conclusion that no Data Processing Agreement is in place, the configuration of this installation, and our incident history. The undertakings under "Our commitments" are promises about our own conduct, and they bind us.

Richard W Bowles

Founder, Integrix

2026-10-19