Document Navigation

ZephyrCart Intranet

- **News**
  - **Stripe Tax integration partnership**
  - **All-hands recap — May 15**
  - **ap-singapore is now GA**
  - **Platform update — May rollups**
  - **Friday-afternoon shipping window — opt-out next sprint**
- **Policies**
  - **Code of conduct**
  - **Data handling**
  - **Incident response**
- **Onboarding**
- **Team Handbook**

Data handling

How customer data moves, who can touch it, and what we never do with it.

Classification

Every piece of data we handle falls into one of four buckets:

Class	Example	Storage	Access
Public	Marketing copy, API spec	Anywhere	Everyone
Internal	This intranet, OKRs	SSO-gated tools	All employees
Confidential	Customer email, order data, payment metadata	Tenant region only	Role-gated, audited
Restricted	PAN, CVV (not stored), employee compensation	Vault, KMS-encrypted	Two-person rule, logged

What stays in the tenant's region

A tenant's `Confidential` data does not leave its home region. There is no cross-region read replica of customer PII. Telemetry that flows centrally is de-identified at source and listed explicitly:

- Request counts, latencies, error rates, by route + status
- Aggregate billing totals, by tenant id (not by customer id)
- Webhook delivery success rates, by endpoint host (not by URL path)

What does **not** flow centrally: customer emails, names, addresses, order line items, payment tokens, IP addresses.

Access requests

Customer-data access for support requires:

1. An open support ticket from the customer's verified contact.
2. A manager approval click in the access tool. Approvals expire after 24 hours.
3. The query runs against the tenant's region. The audit log captures who, when, what, why.

Raw HTML passes through the renderer — this paragraph demonstrates that.

What we never do

- Sell, lease, share, or otherwise transmit customer data to third parties for marketing.
- Train models on identifiable customer data. (Aggregate, anonymised telemetry is fair game for internal product analytics.)
- Store full card numbers (PAN). Stripe holds the cards; we hold a tokenised handle.

In a breach

The first action is the incident response runbook. The second is the legal hold and notification — Legal owns this and will direct.

Audits

We run a third-party penetration test annually (currently with Trail of Bits) and an internal red-team exercise quarterly. Findings land in the security channel within 30 days of the engagement closing.