

COMPLIANCE & SECURITY · TEMPLATE

Data Handling and Classification Policy Template

For founders and operations leaders who need a clear, adoptable standard for how data is stored, shared, accessed, and retired.

How to use this: Define your classification tiers first, then map where sensitive data currently lives before setting handling rules for each tier.

Classification Tiers

Define what falls into each tier for your business specifically, using real examples, not abstract categories.

Tier	Examples for Our Business	Who Can Access	Handling Rule
Public			No special handling required
Internal			Standard access controls, no external sharing
Restricted			Encryption, minimal access, no copying into unapproved tools

Where Sensitive Data Actually Lives

Where is customer personal data (names, emails, addresses) stored?

Where is customer payment or financial data stored, and who has access?

Where are credentials, API keys, and secrets stored?

What data do support and success teams handle that may include sensitive information?

What data do we collect that we no longer have a clear business reason to keep?

Storage and Sharing Rules

- ☐ Restricted data is never stored in general-purpose tools not approved for it (personal drives, chat exports, spreadsheets).
- ☐ Restricted data is never shared externally without an approved, secure method.
- ☐ Access to restricted data is logged or at minimum limited to a named, small group.
- ☐ New tools or vendors are checked against this policy before sensitive data is put into them.
- ☐ Support and sales teams have clear guidance on what customer data can and cannot be pasted into internal tools.

Retention and Retirement

Set a default retention period for each data type and an actual mechanism for deleting it.

Data Type	Retention Period	Deletion Method	Owner
Customer account data (active)			
Customer account data (post-cancellation)			
Support ticket contents			
Financial / payment records			
Logs and analytics data			

Adoption and Review

- ☐ Policy has been shared with the whole team, not just engineering or leadership.
- ☐ New hires are walked through data classification during onboarding.
- ☐ Policy is reviewed at least annually or when a major new tool/data type is introduced.
- ☐ A named owner is responsible for keeping this policy current.