Interoperability & Portability Policy

Version 4

REZOLVE.ai

Document Information

Name of the document	Interoperability & Portability Policy
Release date	23-May-2025
Owned by	Mayank Baghel
Governed by	Udaya Bhaskar Reddy

Revision History

Version No	Version Date	Details of Change
1	21-May-2025	Initially Drafted
2	22-May-2025	Final
3	25-July-2025	Document information Updated
4	29-May-2026	Reviewed and updated

Reviewer and Approver

Name	Title	Comments	Date Reviewed
Mr.Udaya Bhaskar Reddy	Co-Founder & CTO	Approved	04-June-2026

Contents

1. Purpose

To define the principles, practices, and technical controls that ensure our SaaS platform supports secure interoperability between internal and external systems and maintains full customer data portability.

2. Scope

This policy applies to:

- All internal services communicating over APIs
- Customer-facing APIs and interfaces
- Data import/export workflows
- Environments promoting from dev → staging → production

3. Policy Statements

3.1 Communications Between Application Services

- All services must communicate via standardized protocols (HTTPS, REST/gRPC).
- APIs must be defined using OpenAPI 3.x with published schemas.
- All inter-service traffic must be encrypted using TLS 1.2+.

3.2 Information Processing Interoperability

- Data formats exchanged must follow JSON schema
- UTF-8 encoding is required.
- Compatibility with 3rd party platforms is validated during onboarding.

3.3 Application Development Portability

- All apps must support promotion across environments using Helm.
    - Terraform wherever possible
- Configuration is environment-variable based, with secrets from Azure Key Vault.
- Deployment artifacts are containerized and registry-based.

3.4 Information/Data Portability & Exchange

- APIs provide structured export of tenant data.
- Customers can self-initiate data exports in JSON/CSV via REST API or SFTP
- Data integrity and completeness are verified with checksum or schema validation.
- Persistence policies are defined per T&Cs.

3.5 Policy Review and Updates

- This policy is reviewed annually by the security and platform teams.
- Changes require documentation and approval from engineering leadership.

Data Offboarding SOP

Step	Action	Owner
1	Receive contract termination request	Customer Success
2	Confirm offboarding date and export request	Customer Success
3	Provide data export via API or secure SFTP (JSON/CSV)	DevOps
4	Retain copy for 30 days (configurable per T&Cs)	SRE
5	Purge tenant-specific data from DB, logs, backups	Platform Ops
6	Log deletion event and update audit record	Security Ops

All offboarding events are logged. Customers may receive a purge confirmation upon request.

Technical Architecture Overview

Domain	*Solution*
API Design	OpenAPI 3.0 with Redoc UI
Schema Interop	JSON schema registry maintained in Git
Auth & Security	OAuth2/JWT, TLS 1.2+, Azure API Management
Data Access	REST APIs with role-based access, export endpoints
Inter-service Comms	REST with TLS;
CI/CD	Jenkins + Helm for deployment portability
Secrets	Azure Key Vault, encrypted transit/storage
Monitoring	Loki + Grafana; traces via Tempo
Contract Termination	Data format: JSON/CSV; retention: 30 days; deletion: audit-logged

NOTE – Next review cycle for this policy is **March 2027**.
Management can review the policy at any time and can make changes depending on the situation.

All documents related to policies and procedures - any reference to Actionable Science is as good as Rezolve.ai.