

TCP-HOS-001

Data Residency & Hosting Statement

Document Reference: TCP-HOS-001

Document Title: Data Residency & Hosting Statement

Owner: SOSME Technology

Classification: Public

Version: 1.0

Hosting Overview

Item	SOSME Commitment
Primary Hosting Strategy	Saudi-first cloud infrastructure
Customer Data Ownership	Always owned by the customer
Encryption	In transit and at rest
Backups	Automated and encrypted
Business Continuity	Enterprise continuity and disaster recovery procedures
Data Portability	Customer data export supported
Regulatory Alignment	Designed to support Saudi and applicable international requirements

1. Purpose

At SOSME, protecting customer information is a fundamental principle of our Business Operating System.

This Data Residency & Hosting Statement explains where customer information is hosted, how it is protected, how backups are managed, and the principles governing data residency and data sovereignty across the SOSME Platform.

2. Our Hosting Philosophy

SOSME is designed as an enterprise-grade cloud platform built on the following principles:

- ◆ Security by Design
- ◆ Privacy by Design
- ◆ Saudi-first cloud strategy
- ◆ High Availability
- ◆ Business Continuity
- ◆ Customer Data Ownership
- ◆ Enterprise Scalability

Our hosting architecture is designed to support organizations ranging from startups to large enterprises while maintaining high standards of security, resilience, and operational reliability.

3. Primary Hosting Region

SOSME adopts a **Saudi-first hosting strategy**.

Where commercially and technically available, customer production environments are hosted within the **Kingdom of Saudi Arabia** to support local data residency expectations and national digital transformation initiatives.

For customers operating in other jurisdictions, additional hosting regions may become available subject to:

- ◆ Customer requirements

- ◆ Regulatory obligations
- ◆ Commercial availability
- ◆ Infrastructure readiness

4. Cloud Infrastructure

SOSME utilizes enterprise-grade cloud infrastructure provided by internationally recognized cloud service providers.

The hosting infrastructure is selected based on:

- ◆ Security
- ◆ Reliability
- ◆ Scalability
- ◆ Regulatory alignment
- ◆ Business continuity capabilities

Cloud providers may be updated over time as part of SOSME's continuous improvement strategy without affecting customer ownership of data.

5. Data Residency

Customer data is processed and stored within the hosting region selected for the customer's environment.

SOSME does not intentionally transfer customer business data across international borders unless:

- ◆ required to provide contracted services;
- ◆ requested or approved by the customer;

- ◆ required by applicable law or regulatory authorities.

Where cross-border processing is necessary, SOSME implements appropriate contractual, technical, and organizational safeguards.

6. Customer Data Ownership

Customer data always remains the property of the customer.

SOSME does not acquire ownership of customer information, business records, documents, financial data, employee information, or operational data processed through the platform.

SOSME acts solely as the technology platform and service provider responsible for securely hosting and processing customer data in accordance with applicable agreements.

7. Data Protection

Customer information is protected through multiple layers of security including, where applicable:

- ◆ Encryption during transmission
- ◆ Encryption at rest
- ◆ Role-Based Access Control (RBAC)
- ◆ Multi-Factor Authentication (MFA)
- ◆ Continuous monitoring
- ◆ Audit logging
- ◆ Secure software development practices
- ◆ Regular security updates

Further information is available in the SOSME Security Statement.



8. Backup & Recovery

SOSME maintains encrypted backup processes designed to support business continuity and disaster recovery.

Backup activities include:

- ◆ automated scheduled backups;
- ◆ encrypted backup storage;
- ◆ controlled restoration procedures;
- ◆ periodic recovery validation.

Backup retention periods may vary depending on:

- ◆ subscription plan;
- ◆ customer contractual requirements;
- ◆ regulatory obligations.

9. Business Continuity

SOSME maintains business continuity and disaster recovery procedures designed to minimize service disruption.

These procedures include:

- ◆ infrastructure redundancy;
- ◆ backup restoration capability;
- ◆ operational recovery planning;
- ◆ incident response procedures.



Additional information is available in the Business Continuity Statement.

10. Data Portability

Customers may export their business information in accordance with their subscription agreement and applicable contractual terms.

Export capabilities may include:

- ◆ accounting records;
- ◆ customer data;
- ◆ inventory;
- ◆ employee information;
- ◆ reports;
- ◆ documents;
- ◆ configuration data.

SOSME is committed to supporting customers throughout onboarding, operation, and offboarding processes.

11. Compliance

SOSME designs its hosting and operational practices to support applicable regulatory and cybersecurity requirements, including, where applicable:

- ◆ Saudi Personal Data Protection Law (PDPL)
- ◆ Saudi cybersecurity requirements
- ◆ applicable privacy regulations

- ◆ contractual customer obligations

Compliance capabilities continue to evolve as the platform expands into new markets.

12. Continuous Improvement

SOSME continuously evaluates new hosting technologies, cloud regions, infrastructure enhancements, and security capabilities.

Hosting architecture may evolve over time to improve:

- ◆ performance;
- ◆ resilience;
- ◆ availability;
- ◆ regulatory alignment;
- ◆ customer experience.

Any material changes affecting customer hosting arrangements will be communicated through appropriate customer communication channels.

Contact

For questions regarding data residency, hosting architecture, or information security, please contact:

Security & Compliance Team

✉ security@sosme.ai