

SOSME SECURITY STATEMENT

Framework: SOSME Enterprise Trust Framework

Document ID: TCP-SEC-001

Version: 1.0

Effective Date: [01.01.2025]

Last Updated: [01.01.2025]

Security at SOSME

At SOSME, security is one of our core commitments.

Organizations rely on SOSME to manage business operations, financial information, documents, workflows, and Artificial Intelligence. Protecting that trust is fundamental to everything we build.

Our security program is designed to safeguard the confidentiality, integrity, and availability of our platform while supporting business continuity, regulatory compliance, and responsible innovation.

This Security Statement provides an overview of our security principles and practices. It is intended to promote transparency without disclosing confidential technical information that could compromise the security of our platform or our customers.

Security at a Glance

Our security program is built on five commitments.

 Security by Design

 Protection of Customer Information

 Identity & Access Management

 Continuous Monitoring & Security Assurance

 Business Continuity & Operational Resilience

Trust by Design

Trust is embedded into the design, engineering, operation, and continuous evolution of the SOSME Platform.

Our engineering and operational practices are guided by five foundational principles.

Security Governance

Security governance is established through the SOSME Enterprise Governance Standards and is supported by documented policies, operational standards, risk management practices, and continuous assurance activities.

Security by Design

Security considerations are integrated throughout the platform lifecycle—from architecture and software development to deployment, operations, and continuous improvement.

Privacy by Design

Privacy considerations are incorporated into our products, processes, and data handling practices.

AI by Design

Artificial Intelligence capabilities are developed and operated in accordance with the SOSME Enterprise Artificial Intelligence Governance Framework (EGS-011).

Compliance by Design

Compliance requirements are incorporated into platform capabilities and operational processes rather than added afterwards.

Business Continuity by Design

Operational resilience and recovery planning are considered throughout the design and operation of our services.

1. Protecting Customer Information

Protecting customer information is one of our highest priorities.

SOSME implements technical and organizational measures designed to safeguard information throughout its lifecycle.

Our approach includes:

- ♦ protecting information during transmission and storage;
- ♦ controlling access to customer information based on authorized roles;

- ◆ logical separation of customer environments where applicable;
- ◆ appropriate data retention and deletion practices;
- ◆ data minimization principles where applicable; and
- ◆ continuous review and improvement of security controls.

Customers remain responsible for ensuring that information uploaded to the platform is accurate, lawful, and appropriate for their intended business purposes.

2. Identity & Access Management

Access to SOSME is designed around the principles of identity verification, least privilege, and accountability.

Our security approach includes:

- ◆ user authentication;
- ◆ role-based access controls;
- ◆ secure credential management;
- ◆ session protection;
- ◆ support for Multi-Factor Authentication (MFA), where available;
- ◆ support for Single Sign-On (SSO), where available; and
- ◆ periodic review of privileged access.

Customers are responsible for managing user access and permissions within their own organizations.

3. Secure Engineering

Security is integrated throughout our software development lifecycle.

Our engineering practices include:

- ◆ secure architecture and design;
- ◆ secure coding practices;
- ◆ peer code review;
- ◆ security testing;
- ◆ controlled software releases;
- ◆ vulnerability management; and

- ♦ continuous improvement of development practices.

As technology and cybersecurity risks evolve, SOSME continually reviews and enhances its engineering and security practices.

4. Security Controls

SOSME maintains a security program that includes administrative, technical, and operational controls designed to protect our platform and customer information.

These controls include, where applicable:

- ♦ Identity and Access Management
- ♦ Multi-Factor Authentication support
- ♦ Protection of information during transmission and storage
- ♦ Secure software development practices
- ♦ Security logging and monitoring
- ♦ Vulnerability management
- ♦ Periodic vulnerability assessments
- ♦ Penetration testing
- ♦ Backup and disaster recovery procedures
- ♦ Change management
- ♦ Incident response processes
- ♦ Continuous security improvements
- ♦ Security configuration management
- ♦ Secure secrets and key management

For security reasons, specific technical implementations are not publicly disclosed.

5. Infrastructure Security

SOSME is designed to operate on secure cloud infrastructure with multiple layers of protection.

Our infrastructure security practices include:

- ♦ secure environment configuration;
- ♦ network protection;

- ♦ controlled administrative access;
- ♦ infrastructure monitoring;
- ♦ regular maintenance; and
- ♦ operational resilience.

Infrastructure architecture continues to evolve as the platform grows and security requirements mature.

6. Monitoring, Detection & Incident Response

We continuously monitor our platform to help identify operational issues, unusual activity, and potential security events.

Where a security incident occurs, established incident management procedures are followed to:

- ♦ assess the event;
- ♦ contain potential impact;
- ♦ investigate the cause;
- ♦ restore affected services;
- ♦ communicate with affected customers where appropriate; and
- ♦ implement corrective improvements.

Security incidents are managed in accordance with our internal governance processes and applicable legal or contractual obligations.

Incidents are prioritized based on severity, business impact, and customer risk.

7. Business Continuity & Disaster Recovery

Operational resilience is an integral part of our security program.

Our continuity practices include:

- ♦ backup management;
- ♦ recovery planning;
- ♦ disaster recovery procedures;
- ♦ resilience planning;
- ♦ periodic review of continuity arrangements; and

- ♦ continuous improvement of operational readiness.

Additional information is available in the **TCP-SVC-001 Business Continuity Statement**.

8. Artificial Intelligence Security

Artificial Intelligence capabilities, including YARA AI, is developed and operated in accordance with SOSME's security, privacy, and responsible AI principles.

Our approach includes:

- ♦ protection of information processed by AI features;
- ♦ governance of AI capabilities;
- ♦ human oversight where appropriate;
- ♦ monitoring of AI functionality; and
- ♦ continuous improvement of AI security and governance.

For more information, please refer to the **SOSME Yara AI Responsible Use Policy** and the **SOSME AI Transparency Statement**.

9. Security Assurance & Continuous Improvement

Security is an ongoing commitment.

SOSME continually evaluates and strengthens its security posture through governance, operational monitoring, and security assurance activities.

Our security program includes:

- ♦ ongoing risk assessments;
- ♦ periodic vulnerability assessments;
- ♦ penetration testing;
- ♦ secure software development reviews;
- ♦ monitoring of security events;
- ♦ review of security controls;
- ♦ independent security assessments, where appropriate; and
- ♦ continuous improvement initiatives.

As SOSME grows, we intend to expand our security assurance program and pursue additional certifications and independent assessments aligned with customer, regulatory, and industry expectations.

10. Compliance & Governance

Our security practices are designed to support alignment with recognized laws, standards, and industry frameworks, including:

- ◆ Saudi Personal Data Protection Law (PDPL);
- ◆ applicable ZATCA requirements;
- ◆ NIST AI Risk Management Framework (AI RMF);
- ◆ OWASP Secure Development practices; and
- ◆ future alignment with ISO/IEC 27001, SOC 2 , ISO 22301, and NCA Essential Cybersecurity Controls (ECC)

11. Shared Responsibility Model

Maintaining a secure environment is a shared responsibility.

SOSME Responsibilities	Customer Responsibilities
Secure platform infrastructure	Manage user accounts and permissions
Platform security controls	Protect user credentials
Application security	Secure endpoint devices
Platform monitoring	Configure user access appropriately
Backup and disaster recovery	Maintain the quality and legality of uploaded information
Secure software updates	Train users and follow internal security policies
Incident response	Promptly report suspected security incidents
Platform availability	Business continuity planning

Working together helps maintain a secure, resilient, and trusted operating environment.

Need Help?

If you have questions about our security practices or wish to report a security concern, please contact the SOSME Security Team using the contact information available on our official website.

If you believe you have identified a security vulnerability, please refer to our **Vulnerability Disclosure Policy**.

Our Security Commitment

Security is more than technology—it is a continuous commitment.

We continuously strengthen our platform through responsible engineering, sound governance, ongoing monitoring, security assurance, and a culture of continuous improvement.

Our objective is to provide a trusted operating environment where organizations can confidently manage, automate, and grow their businesses.

Thank you for trusting SOSME.

Business. Rebuilt.

Related Documents

- ◆ TCP-SVC-001 – Business Continuity Statement
- ◆ TCP-SEC-001 – Vulnerability Disclosure Policy
- ◆ TCP-AI-002 – AI Transparency Statement
- ◆ TCP-PRI-001 – Privacy Policy
- ◆ TCP-AI-001 – Responsible Artificial Intelligence Policy
- ◆ SOSME Acceptable & Responsible Use Policy
- ◆ LEG-004 – Terms of Use
- ◆ LEG-002 – Master Subscription Agreement

The latest versions of all SOSME Trust Center documents are available through our official website.