

SOSME – FREQUENTLY ASKED QUESTIONS (FAQ)

Framework: SOSME Enterprise Trust Framework

Document ID: TCP-REF-001

Version: 1.0

Last Updated: [01.01.2025]

Welcome to the SOSME Trust Center FAQ.

This page answers common questions about our security, privacy, Artificial Intelligence, operational resilience, and governance. It complements our Trust Center policies and statements and is intended to provide a simple overview of how SOSME protects our customers, their information, and their business operations.

Security

1. How does SOSME protect customer information?

Protecting customer information is one of SOSME's highest priorities. Our security program combines administrative, technical, and operational controls designed to safeguard the confidentiality, integrity, and availability of customer information. This includes identity and access management, secure engineering practices, monitoring, vulnerability management, backup procedures, and continuous improvement of security controls. Security is embedded throughout the lifecycle of the SOSME Platform as part of our Security by Design approach.

2. How is access to the SOSME Platform secured?

SOSME uses identity verification, authentication, role-based access controls, and the principle of least privilege to help ensure users can only access information appropriate to their responsibilities. Where available, Multi-Factor Authentication (MFA) is supported to strengthen account security. Customers are responsible for managing their own users, permissions, and internal access policies.

3. How does SOSME manage security incidents?

SOSME maintains incident management procedures designed to identify, assess, contain, investigate, and resolve security incidents. Where required by law or contractual obligations, affected customers will be informed of relevant incidents. Following each significant incident, we review the root cause and implement improvements to strengthen our security posture.

4. How can I report a security vulnerability?

If you believe you have identified a security vulnerability affecting SOSME, we encourage you to report it responsibly using the security contact details available on our website. Please provide sufficient information to help us understand and reproduce the issue. We appreciate responsible disclosure and investigate all legitimate reports in accordance with our TCP-SEC-002 – Vulnerability Disclosure Policy.

Privacy

5. What personal information does SOSME collect?

The information we collect depends on how you interact with our Services. It may include contact details, account information, business information you choose to provide, technical information such as browser and device details, and information necessary to deliver AI-enabled features. Full details are available in our Privacy Policy.

6. How is my information protected?

SOSME applies appropriate technical and organizational measures to help protect personal and business information throughout its lifecycle. These measures include access controls, secure development practices, monitoring, backup procedures, and ongoing security improvements. We continuously review our practices to address evolving risks and regulatory expectations.

7. How can I exercise my privacy rights?

Depending on applicable law, you may request access to your personal information, ask for corrections, request deletion where appropriate, withdraw consent where processing is based on consent, or exercise other available privacy rights. Requests may be submitted using the contact information provided in our Privacy Policy.

Artificial Intelligence

8. What is Yara AI?

Yara AI is the native Artificial Intelligence layer of the SOSME Operating System. Rather than operating as a standalone chatbot, Yara AI is embedded throughout the platform to help users analyze information, automate work, improve productivity, and support better business decisions while operating within the permissions assigned to each user.

9. Does Yara AI replace human decision-making?

No. Yara AI is designed to assist people—not replace them. AI-generated outputs should always be reviewed before being relied upon for important financial, legal, operational, or strategic decisions. Responsibility for business decisions remains with the customer and its authorized users.

10. How does Yara AI use customer information?

Yara AI processes only the information necessary to provide the requested functionality within the user's authorized environment. Customer information is handled in accordance with the SOSME Privacy Policy, security controls, and applicable legal requirements. SOSME is committed to protecting customer information when AI features are used.

11. How does SOSME govern Artificial Intelligence?

Yara AI operates under a governance framework built on human oversight, accountability, transparency, privacy, security, and continuous improvement. Our approach aligns with the principles described in the TCP-AI-001 – Responsible Artificial Intelligence Policy and TCP-AI-002 – AI Transparency Statement

Reliability & Operations

12. How are backups and disaster recovery managed?

SOSME maintains backup, recovery, and operational resilience practices designed to support service continuity and restore operations following significant disruptions. Our approach is based on continuous improvement and periodic review. Additional information is available in the TCP-SVC-001 – Business Continuity Statement

13. How does SOSME maintain platform availability?

SOSME continuously monitors its platform and maintains operational processes designed to support reliable service delivery. We regularly review infrastructure, software, and operational practices to improve resilience, performance, and customer experience while minimizing disruption during maintenance or platform updates.

🏛️ Governance & Legal

14. Which regulations and standards does SOSME support?

SOSME designs its platform and governance practices to support alignment with applicable laws and recognized industry frameworks, including the Saudi Personal Data Protection Law (PDPL), applicable ZATCA requirements, the NIST AI Risk Management Framework (AI RMF), and OWASP Secure Development practices. We also maintain a roadmap toward additional internationally recognized assurance standards, including ISO/IEC 27001, ISO/IEC 27701, ISO 22301, SOC 2, and the NCA Essential Cybersecurity Controls (ECC), as our platform and business continue to mature.

15. Where is customer data hosted?

SOSME supports different deployment models to meet customer, regulatory, and business requirements. Depending on the selected deployment option, customer information may be hosted within customer-managed environments or on secure cloud infrastructure operated by approved service providers.

Where applicable, hosting arrangements are designed to support compliance with relevant legal, contractual, and regulatory requirements, including data residency obligations. Customers with specific hosting or regulatory requirements are encouraged to discuss these needs with SOSME during implementation.

16. Does SOSME encrypt customer information?

Yes. SOSME applies appropriate technical and organizational measures to help protect customer information during transmission and storage, where applicable. Encryption is one of several security controls used to safeguard the confidentiality, integrity, and availability of information.

Our security program also includes identity and access management, secure software development practices, monitoring, vulnerability management, backup procedures, and continuous improvement of security controls. Additional information is available in the **TCP-SEC-001 – Security Statement**.

17. How often are Trust Center documents updated?

SOSME periodically reviews its Trust Center documentation to ensure it remains accurate, relevant, and aligned with applicable legal, regulatory, security, and business requirements. Documents may be updated whenever there are significant changes to our platform, governance framework, security practices, privacy commitments, Artificial Intelligence capabilities, or applicable laws and industry standards.

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

18. Can customers request additional security or compliance information?

Yes. Customers undergoing procurement, security reviews, regulatory assessments, or due diligence may request additional information regarding SOSME's security, privacy, governance, or compliance practices. Where appropriate, additional documentation may be provided under applicable confidentiality or non-disclosure arrangements (NDAs) to protect sensitive security and operational information

19. Where can I find SOSME's Trust Center documents or request additional information?

The SOSME Trust Center provides access to our public policies, security statements, AI governance documents, privacy information, and legal resources. If you require additional documentation for procurement, due diligence, or compliance purposes, please contact the SOSME Trust Team using the contact details available on our official website. Where appropriate, additional information may be shared under applicable confidentiality arrangements.

Need More Information?

If your question is not answered here, please contact the appropriate SOSME team through the Trust Center:

- ◆ Security

- ◆ Privacy
- ◆ AI Governance
- ◆ Legal & Compliance
- ◆ Customer Support
- ◆ Sales
- ◆ Trust & Compliance

We're committed to providing clear, transparent, and timely responses to help you evaluate and use SOSME with confidence.

Business. Rebuilt.

Related Documents

- ◆ TCP-GOV-001 – Governance & Compliance Framework
- ◆ TCP-SEC-001 – Security Statement
- ◆ TCP-SEC-002 – Vulnerability Disclosure Policy
- ◆ TCP-PRI-001 – Privacy Policy
- ◆ TCP-PRI-002 – Cookies & Similar Technologies Policy
- ◆ TCP-AI-001 – Responsible Artificial Intelligence Policy
- ◆ TCP-AI-002 – AI Transparency Statement
- ◆ TCP-GEN-001 – Acceptable Use Policy
- ◆ LEG-002 – Master Subscription Agreement
- ◆ LEG-004 – Terms of Use

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

For additional information, visit the SOSME Trust Center.