

SOSME BUSINESS CONTINUITY STATEMENT

Framework: SOSME Enterprise Trust Framework

Document ID: TCP-SEC-003

Version: 1.0

Effective Date: [01.01.2025]

Last Updated: [01.01.2025]

Business Continuity at SOSME

At SOSME, operational resilience is an essential part of the trust our customers place in us.

Organizations depend on SOSME to support critical business processes, financial operations, workforce management, and intelligent automation. We recognize the importance of maintaining service availability and recovering effectively from unexpected events.

This Business Continuity & Disaster Recovery Statement provides an overview of our approach to maintaining resilient operations and restoring services when disruptions occur.

For security reasons, this document provides a high-level overview and does not disclose confidential operational procedures.

Continuity at a Glance

Our continuity program is built around five commitments.

-  Operational Resilience
-  Data Protection & Backup
-  Disaster Recovery
-  Continuous Monitoring
-  Continuous Improvement

Business Continuity by Design

Business continuity is considered throughout the lifecycle of our platform.

Our objective is to:

- ♦ minimize service disruption;
- ♦ protect customer information;

- ♦ recover services in a controlled manner;
- ♦ continuously improve operational resilience;
- ♦ support timely communication with customers during significant operational disruptions; and
- ♦ support customer confidence during unexpected events.

1. Operational Resilience

SOSME designs and operates its services with resilience in mind.

Our operational practices include:

- ♦ resilient cloud infrastructure;
- ♦ controlled operational processes;
- ♦ service monitoring;
- ♦ planned maintenance activities;
- ♦ change management;
- ♦ capacity planning;
- ♦ resilience testing; and
- ♦ periodic review of operational risks.

Our objective is to reduce the likelihood and impact of service interruptions.

2. Data Backup

Protecting customer information is a critical component of our continuity program.

Our practices include, where appropriate:

- ♦ regular backup of critical platform data;
- ♦ secure storage of backup information;
- ♦ verification of backup processes;
- ♦ protection of backup integrity;
- ♦ periodic verification of backup restorations; and
- ♦ periodic review of backup procedures.

Backup strategies continue to evolve as our platform and customer requirements grow.

3. Disaster Recovery

Despite careful planning, unexpected events may occur.

SOSME maintains disaster recovery capabilities designed to support the restoration of services following significant operational disruptions.

Our disaster recovery approach includes:

- ♦ recovery planning;
- ♦ restoration procedures;
- ♦ infrastructure recovery;
- ♦ validation of recovered services;
- ♦ recovery objectives are periodically reviewed and refined based on operational requirements; and
- ♦ post-incident review and improvement.

Recovery priorities are determined according to business impact and operational requirements.

4. Incident Management

Where a significant operational incident occurs, SOSME follows established incident management procedures designed to:

- ♦ identify the incident;
- ♦ assess potential business impact;
- ♦ coordinate response activities;
- ♦ restore affected services;
- ♦ communicate with affected customers where appropriate; and
- ♦ review lessons learned to improve future resilience.

5. Testing & Continuous Improvement

Business continuity is not a one-time activity.

SOSME periodically reviews and evaluates its continuity and recovery capabilities through activities such as:

- ♦ continuity planning reviews;
- ♦ recovery exercises;

- ♦ operational assessments;
- ♦ risk evaluations;
- ♦ tabletop exercises;
- ♦ disaster recovery simulations; and
- ♦ improvement initiatives.

The scope and frequency of these activities are determined based on operational needs, platform evolution, and risk assessments.

6. Business Impact Assessment

SOSME periodically evaluates critical business services and operational dependencies to help prioritize recovery efforts and continuously improve operational resilience. Recovery priorities are determined according to business impact and service criticality.

7. Customer Responsibilities

Business continuity is a shared responsibility.

Customers are encouraged to:

- ♦ maintain appropriate business processes;
- ♦ manage user access responsibly;
- ♦ retain copies of critical business records where appropriate;
- ♦ maintain their own endpoint security; and
- ♦ establish internal continuity arrangements that support their business operations.

8. Shared Responsibility Model

SOSME Responsibilities	Customer Responsibilities
Operate and maintain the platform	Maintain internal business continuity plans
Maintain backup and recovery capabilities	Protect endpoint devices and local environments
Monitor platform availability	Manage user access and credentials
Respond to operational incidents	Validate critical business data
Restore platform services following disruptions	Maintain internal operational procedures
Continuously improve resilience	Report operational issues promptly

Operational resilience is achieved through collaboration between SOSME and our customers.

9. Continuous Improvement

Operational resilience evolves alongside our platform.

We regularly review our continuity practices, technology, governance, and operational procedures to strengthen our ability to respond to changing business needs and emerging risks.

Need Help?

If you have questions regarding our business continuity or disaster recovery practices, please contact the SOSME Support Team using the contact details published on our official website.

Our Commitment

Business continuity is about more than recovering systems—it is about maintaining the confidence our customers place in us.

We are committed to strengthening the resilience of our platform, protecting customer operations, and continuously improving our ability to respond to change.

Thank you for trusting SOSME.

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-AI-001 – Responsible Artificial Intelligence Policy
- ◆ TCP-AI-002 – AI Transparency Statement
- ◆ LEG-004 – Terms of Use

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