BUSINESS CONTINUITY & DISASTER RECOVERY POLICY

MISIXS, LLC
Version 1.1 - Approved by GRC
Effective Date: January 2, 2026

Contents

1. Objective

The objective of this policy is to provide guidelines for MISIXS, LLC's business continuity and disaster recovery. The document prescribes the requirements to plan for recovery during disasters so that business commitments to customers can be met.

This policy recognizes that MISIXS operates multiple brands with different operational maturity levels and business continuity requirements. This policy establishes baseline principles while allowing brand-specific implementations appropriate to each brand's service level commitments and operational stage.

2. Scope

This document is applicable to all processes and operations within MISIXS, LLC and all brands operating under MISIXS, LLC, including the RuleFirst platform and any other current or future branded offerings.

This policy applies to:

- All staff members, contractors, and service providers who support MISIXS operations
- All information systems, infrastructure, and data processing activities
- All brands, products, and services offered under MISIXS, LLC
- Third-party service providers and subprocessors engaged to support the Platform and Services

Brand-Specific Scope:

Different MISIXS brands have different business continuity and disaster recovery approaches based on their operational maturity, customer commitments, and service level requirements. See Section 4 for brand-specific details.

3. Policy Statement

MISIXS, LLC is committed to ensuring appropriate levels of service continuity to its customers. Continuity of operations in a secure manner shall be planned for and embedded in the organization's business continuity management and disaster recovery planning activities, with implementation approaches tailored to each brand's operational requirements and customer commitments.

MISIXS recognizes that:

- **Production platforms** serving customers under contractual service level agreements require robust business continuity and disaster recovery capabilities
- **Experimental and research brands** may operate under best-effort recovery models appropriate to their stage of development
- **Custom and enterprise deployments** may have customer-specific business continuity requirements built into deployment plans

- **Third-party infrastructure providers** play a critical role in disaster recovery for cloud-based services

4. Brand-Specific Business Continuity Approaches

MISIXS operates multiple brands with different operational maturity levels and business continuity requirements. This section describes the business continuity approach for each brand category.

4.1 RuleFirst Platform

Service Level: Production platform serving customers under contractual agreements

Business Continuity Approach:

The RuleFirst platform relies primarily on third-party infrastructure providers for disaster recovery capabilities, including:

- **Cloud Infrastructure:** AWS (Amazon Web Services) provides underlying infrastructure redundancy, backup, and disaster recovery capabilities
- **Managed Services:** Database services, storage services, and compute services leverage provider-native backup and recovery features
- **Third-Party Subprocessors:** Communication providers, AI model providers, and other subprocessors maintain their own business continuity capabilities

MISIXS Responsibilities:

- Monitor third-party provider service level agreements and disaster recovery commitments
- Maintain documented procedures for service restoration leveraging third-party capabilities
- Coordinate with third-party providers during disaster recovery scenarios
- Communicate with customers regarding service disruptions and recovery timelines
- Maintain backups of critical configuration data and customer data where applicable

Customer Responsibilities:

- Customers are responsible for maintaining their own backups of data they control
- Customers should review third-party provider SLAs and disaster recovery capabilities
- Customers may implement additional backup and recovery measures as needed for their business requirements

4.2 Custom Solutions and Enterprise Deployments

Service Level: Custom deployments with customer-specific requirements

Business Continuity Approach:

For Statement of Work (SOW) engagements, custom solutions, and enterprise deployments, business continuity and disaster recovery requirements are built into the deployment plan and documented in the applicable agreement.

Implementation:

- Business continuity requirements are assessed during the engagement planning phase
- Recovery time objectives (RTO) and recovery point objectives (RPO) are defined based on customer requirements
- Disaster recovery capabilities are designed and implemented as part of the solution architecture
- Testing and validation procedures are documented in the deployment plan
- Ongoing maintenance and review schedules are established

Documentation:

Each custom deployment shall have documented business continuity and disaster recovery procedures appropriate to the customer's requirements and the solution architecture.

4.3 SecretAILabs and Adventures Brands

Service Level: Experimental, research, and development brands

Business Continuity Approach:

SecretAILabs and RuleFirst Adventures brands operate experimental and research-focused services that are not yet at a stage to offer scalable continuity and recovery commitments.

Best-Effort Recovery:

- These brands operate under a best-effort recovery model
- Services may experience extended downtime during disaster scenarios
- Data recovery is attempted on a best-effort basis but is not guaranteed
- Users of these services should not rely on them for mission-critical operations
- Users should maintain their own backups of any critical data

Disclosure:

Users of experimental brands are informed of the best-effort recovery model through:

- Terms of Service disclosures
- Service documentation
- User communications

Future Evolution:

As experimental brands mature and transition to production service levels, business continuity and disaster recovery capabilities will be enhanced accordingly, and this policy will be updated to reflect the new service level commitments.

4.4 Other MISIXS Brands

For brands not specifically listed above, the business continuity approach shall be determined based on:

- Operational maturity and service level commitments
- Customer requirements and contractual obligations
- Regulatory and compliance requirements
- Risk assessment and business impact analysis

The appropriate business continuity tier (production, custom, or best-effort) shall be documented and communicated to users.

5. Information Security Aspect of Business Continuity Management

5.1 Information Security Continuity

5.1.1 Planning Information Security Continuity

The organization-wide information security processes shall include information security requirements to help ensure that confidentiality, integrity, and availability of critical information assets shall be preserved even in the event of a business disruption or disaster.

MISIXS shall identify recovery guidelines that can be taken as a baseline reference to classify mission-critical systems and develop recovery and restoration plans appropriate to each brand's service level commitments.

A strategy plan shall be developed for the overall business continuity/disaster recovery approach. Information security controls applicable during business-as-usual scenarios shall remain relevant even during disaster scenarios. All exceptions shall need approval from the Information Security Officer and senior management.

The organization ensures ICT readiness through the implementation of appropriate disaster recovery and business continuity measures, including regular data backups, system redundancy, and failover capabilities where applicable to the service level. Critical systems are protected by automated monitoring, incident response procedures, and recovery strategies that ensure appropriate levels of availability. These measures are regularly reviewed for continuous improvement and updated to maintain resilience and availability of essential services in alignment with compliance requirements and customer commitments.

Third-Party Provider Reliance:

For services that rely on third-party infrastructure providers (such as the RuleFirst platform):

- MISIXS shall review and document third-party provider business continuity and disaster recovery capabilities
- MISIXS shall monitor third-party provider service level agreements and performance
- MISIXS shall maintain procedures for coordinating with third-party providers during disaster scenarios
- MISIXS shall communicate third-party provider capabilities and limitations to customers

5.1.2 Implementing Information Security Continuity

MISIXS shall ensure that an adequate framework is in place to prepare for, mitigate, and respond to a disruptive event using personnel with the necessary authority, experience, and competence, appropriate to the service level commitments of each brand.

MISIXS shall identify personnel with the necessary responsibility, authority, and competence to manage an incident and maintain information security.

MISIXS should consider the development and approval of comprehensive and well-documented plans, response strategies, and recovery procedures to effectively manage and mitigate the impact of any potential disruptive event, with the level of detail and testing appropriate to the service level commitments.

5.1.3 Verify, Review & Evaluate Information Security Continuity

Information security controls for business continuity sites and systems shall be reviewed and verified where applicable. Business continuity plans shall be tested and updated regularly to ensure they are up to date and effective, with testing frequency appropriate to the service level commitments.

The roles and responsibilities for both information systems' contingency planning and recovery shall be reviewed and updated at least annually.

Brand-Specific Review:

- **Production platforms:** Annual review and testing of business continuity procedures
- **Custom deployments:** Review and testing per customer agreement requirements
- **Experimental brands:** Review as operational maturity evolves

5.2 Redundancies

MISIXS shall identify business requirements for the availability of information systems appropriate to each brand's service level commitments.

Redundant components or architectures shall be considered wherever availability cannot be guaranteed using the existing systems architecture and where appropriate to the service level commitments.

Redundant information systems shall be tested to ensure the successful failover from one component to another where such redundancy is implemented.

Third-Party Provider Redundancy:

For services relying on third-party infrastructure providers, redundancy is primarily provided by:

- Cloud provider multi-availability zone deployments
- Managed service provider backup and replication features
- Geographic distribution of infrastructure where appropriate

6. Document Security Classification

Company Internal (please refer to the Data Classification Policy for more details, if available).

7. Non-Compliance

Compliance with this policy shall be verified through various methods, including, but not limited to, automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, which may include termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

8. Responsibilities

The designated Information Security Officer or equivalent role is responsible for approving and reviewing this policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

Specific Responsibilities:

- **Information Security Officer:** Overall authority for business continuity policy and standards
- **Operations Teams:** Implementation and maintenance of business continuity measures appropriate to each brand
- **Engineering Teams:** Design and implementation of redundancy and recovery capabilities
- **Customer Success Teams:** Communication with customers regarding service disruptions and recovery

- **Third-Party Management:** Monitoring and coordination with infrastructure providers and subprocessors

Contact Information:

For business continuity policy questions and incident coordination:

Email: privacy@misixs.com

Mailing Address: MISIXS, LLC 970 Nolder Drive Lancaster, Ohio 43130 United States

9. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization, brand service levels, or third-party provider capabilities.

10. Version History

Version	Status	Log	Date
1.1	Current	Initial policy version for MISIXS, LLC	January 2, 2026

END OF BUSINESS CONTINUITY & DISASTER RECOVERY POLICY