INCIDENT MANAGEMENT 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 a framework within which information security events and incidents associated with information systems are communicated in a timely manner and necessary corrective actions are taken.

This policy operationalizes the incident response procedures described in Section 12 of the Data Processing Agreement and supports MISIXS, LLC's commitment to detect, investigate, and respond to Personal Data incidents and security incidents affecting the Platform and Services.

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 have access to MISIXS information systems
- All information security incidents and Personal Data incidents affecting MISIXS systems, customer data, or business operations
- All subprocessors and third-party service providers engaged to support the Platform and Services
- All digital and non-digital assets that play a role in the creation, storage, transmission, and disposal of information

3. Policy Statement

Security incidents are irregular and anomalous conditions that cause - or may lead to - service degradation, loss of sensitive data, outages, or any form of reduced operational status. These situations require quick human intervention to avert disruptions or restore operational status.

This document offers guidance and establishes methods for handling and managing incidents for staff or incident responders who believe they have discovered or are responding to a security incident.

MISIXS, LLC maintains procedures designed to detect, investigate, and respond to Personal Data incidents. Upon becoming aware of a Personal Data incident affecting Customer Data, MISIXS shall notify the affected customer without unreasonable delay and provide information reasonably available to support the customer's response.

4. Information Security Incident Management

4.1 Responsibilities and Procedures

An incident management procedure shall be created to define procedures and responsibilities to ensure quick, effective, consistent, and orderly responses to information security incidents.

There shall be responsible personnel appointed for:

- Ensuring that all employees, contractors, customers, and third parties are aware of incident reporting and communication channels
- Investigation and coordination of reported information security incidents and security weaknesses
- Tracking closure of incidents and corrective and preventive actions
- Coordinating with customers regarding Personal Data incidents as required by the Data Processing Agreement

Incident Reporting Contact:

All security incidents and Personal Data incidents must be reported immediately to:

Email: privacy@misixs.com **Subject Line:** Security Incident Report

4.2 Reporting Information Security Events and Incidents

MISIXS management shall establish appropriate channels through which information security incidents can be reported promptly upon discovery.

All information security incidents shall be recorded in an information security incident database.

The details of the steps to be followed for reporting an incident shall be communicated to all employees and contractors of the company.

Incident reporting and management procedures shall be made available for easy access and reference for reporting security incidents and weaknesses by users.

A monitoring mechanism shall be set up for proactive monitoring of intrusions, attacks, and frauds.

Personal Data Incident Notification:

Upon becoming aware of a Personal Data incident affecting Customer Data, MISIXS shall notify the affected customer without unreasonable delay. Notification shall include information reasonably available at the time to support the customer's response, including:

- Description of the nature of the incident
- Categories and approximate number of data subjects affected
- Categories and approximate number of Personal Data records affected
- Likely consequences of the incident
- Measures taken or proposed to address the incident and mitigate harm
- Contact information for further inquiries

4.3 Assessment of and Response to Information Security Incidents

All information security incidents that are reported shall be assessed and classified as per the classification criteria mentioned in the incident management procedure.

The assessment and classification of incidents shall be maintained for future reference to allow easy identification and avoid false positives.

A response plan and strategy for the appropriate handling of security incidents shall be formulated, which covers the incident cycle from identification to root cause analysis to resolution.

Incidents shall be communicated to users impacted as per legal, regulatory, and contractual agreements. For Personal Data incidents affecting Customer Data, notification shall be provided without unreasonable delay in accordance with the Data Processing Agreement.

The overall response to reported incidents shall include the identification of corrective action where important.

Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction. MISIXS, LLC is governed by the laws of the State of Ohio, and evidence handling shall comply with Ohio legal requirements.

4.4 Learnings from Security Incidents

Analysis shall be carried out for information security incidents and shared with the appropriate authorities periodically.

Knowledge gained from the resolution of security events shall be used to reduce the likelihood of similar incidents in the future and help limit the impact of incidents.

Continuous Improvement:

MISIXS shall track root causes, implement corrective actions, and improve processes so the same type of incident becomes less likely over time. Reasonable steps shall be taken to remediate incidents and mitigate further harm.

5. Document Security Classification

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

6. 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.

7. 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 incident management policy, procedures, and continuous improvement
- **Incident Response Team:** Investigation, containment, remediation, and documentation of security incidents
- **Customer Success Team:** Coordination with customers regarding Personal Data incidents affecting Customer Data
- **Legal and Compliance:** Ensuring incident response complies with legal, regulatory, and contractual obligations
- **All Staff Members:** Prompt reporting of suspected security incidents or weaknesses

Contact Information:

For incident reporting, policy questions, and incident-related inquiries:

Email: privacy@misixs.com

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

8. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization.

9. Version History

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

END OF INCIDENT MANAGEMENT POLICY