Incident Response Policy

Version 1.1
Effective Date: 6/21/2023

Revision History

Revision	Date	Description of changes	Reviewer(s)
0.1	5/11/23	Initial Draft	Chase Johnston, VerSprite
1.1	6/21/2023	Adopted	Marcy Johnson, Inline Data Systems

Table of Contents

Introduction

The Incident Response Policy will establish the rules and requirements for identifying, investigating, validating, prioritizing, and responding to information security incidents. This policy is for all system and individual users of the company IT assets, information assets, and/or facilities, including but not limited to employees, contractors, vendors, and agents operating on behalf of Inline Data Systems (Inline).

Purpose

The purpose of this policy is to outline expectations and accountability while adhering to industry standards when responding to information security incidents, toward protecting the confidentiality, integrity, and availability of IT assets, information assets, and company reputation.

Roles and Responsibilities

The head of IT at Inline is responsible for ensuring the appropriate resources, processes, people, and technology are deployed to enable this policy.

The Incident Manager is appointed by the head of IT at Inline and is responsible for assessing and responding to a reported incident, and providing updates to the **head of IT** and Board of Directors.

Incident Management

Identification and Investigation

An incident is any unplanned interruption to an IT service or reduction in the quality of an IT service. Security incidents at Inline are identified in a number of ways, including, but not limited to:

1. User reporting of security violations, system weaknesses, or policy violations;
2. Automated system alerts as well as monitoring of both system-generated and manually generated logs; or
3. Notification from vendors or software providers of recently discovered or known system weaknesses, vulnerabilities, or other related issues.

The suspected security incident should be escalated to the Incident Manager, who investigates the incident to determine its validity. Results of the investigation are documented in the **Incident Report.**

Classification and Prioritization

Incident response will be managed based on the level of severity of the incident. The purpose of this phase is to determine the level of severity of the incident by estimating its impact on or threat to the operation or integrity of the company and its information. It determines the priority for handling the incident, who manages the incident, and the timing and extent of the response.

Upon escalation of an incident, the priority of the incident should be validated, prior to response determination or notifications of either additional personnel or any external entities.

Rating	Priority	Description
High	Resolve Immediately	The incident adversely impacts, or has a high probability of impacting, a system or service critical to the operation of the company or threatens to have a significant adverse impact on company systems, employees, or customers.
Medium	Immediate Focus - Second Only to Critical Items (within 5 days)	The incident adversely impacts a non-critical system, or moderately impacts, or has a probability of threatening to impact, systems, employees, or customers.
Low	Short-term mitigation – Scheduled in with business functions and/or funding (within 30 days)	The incident adversely impacts a very small number of systems, employees, or customers and/or has low risk of spread.
N/A	None	Used for events initially suspected to be IT security incidents, however upon investigation no evidence of a security is found.

Response and Containment

Upon incident confirmation, the Incident Manager will initiate an incident response to contain the impact and prevent further damage. The response will vary depending on the nature of the incident, but will aim to isolate the incident, preserve any log data and other relevant information for further forensic analysis, and identify and eradicate the root cause of the incident.

Reporting and Documentation

The Incident Manager must document all incidents, actions taken, decisions made, and lessons learned in the Incident Register. The Incident Report will be used for post-incident review and improvements, and for compliance and audit purposes.

The Incident Manager will work with the **head of IT with Inline** and External Legal Counsel to determine notification requirements with customers and state/federal regulatory authorities.

Compliance

This Incident Response Policy addresses the following security requirements:

- **SOC 2:** CC5.3 Control Activities

Enforcement

Violations of this Incident Response Policy will be reviewed by the appropriate Inline team and Inline management and may result in disciplinary action in accordance with this Program, Inline's information security policies and procedures, and human resources policies.

Policy Review

The **Incident Manager** shall review this Incident Response Policy and the security measures defined herein at least annually, or whenever there is a material change in Inline's business practices that may reasonably implicate the business risk tolerance. Inline must retain documentation regarding any such program review, including any identified gaps and action plans.