SUPPLIER SHIELD

Incident Management Procedure

Table of Contents

1. Purpose

The objective of this Security Incident Management procedure is to define how:

- Information security events and system weaknesses that could lead to information security incidents are identified, qualified, communicated, and escalated in a timely manner.
- We manage information security incidents by detecting, assessing, classifying, handling, and recovering them.

This document outlines the Supplier Shield™ Incident Management Procedure. It is intended for external audiences requiring visibility in our Incident Management Framework. While the structure, processes, and response teams are presented, Supplier Shield™ reserves the right to omit confidential information that may compromise the employees, stakeholders, or company's security and privacy.

Supplier Shield™ has developed and launched a comprehensive Incident Management Procedure. This initiative provides a clear strategy and framework for managing incidents impacting information security. The procedure includes a structured set of requirements for establishing response teams and implements clear processes for execution, coordination, and recovery.

2. Scope

The Incident Management Procedure applies to all business events and incidents that may affect Supplier Shield's operations, customers, or personnel. These events include, but are not limited to, cybersecurity incidents, technological failures, natural disasters, human error, pandemics, and civil unrest, or any other regionally significant occurrences that could impact business continuity. The program includes:

- Supporting systems such as applications and cloud databases,
- Personnel, including employees, contractors, and critical third-party partners.
- Processes, procedures and other relevant documented information.

3. Definitions

Term/Abbreviation	Definition
Availability	Characteristic of the information by which authorized persons can access when it is needed.
Confidentiality	Characteristic of the information by which it is available only to authorized persons or systems.
Disruption	An incident, whether anticipated or unanticipated, that disrupts the normal course of operations at an organization's location.
Event	A security event is an attempt to breach security policies and countermeasures.
Incident	An information security incident is a successful breach of security policies and countermeasures. An information security incident may impact the availability, confidentiality, and integrity of data and IT systems.
Incident Management	Incident management comprises the overall organizational and technical process of preparation and response to suspected or confirmed security incidents to minimize the impact and support the recovery of the business services.
Integrity	Characteristic of the information by which it is changed only by authorized persons or systems in an allowed way.
Managed Security Service Provider (MSSP)	A third-party organization that delivers cybersecurity services to businesses.

4. Roles & Responsibilities

Incident Response Team (IRT)

- The Incident Response Teams will be assembled whenever a medium- or high-security incident happens. The IRT Security Team is composed of the CEO, ISO, IT Specialist, and may include external experts and additional internal support based on incident type.

Chief Executive Officer (CEO):

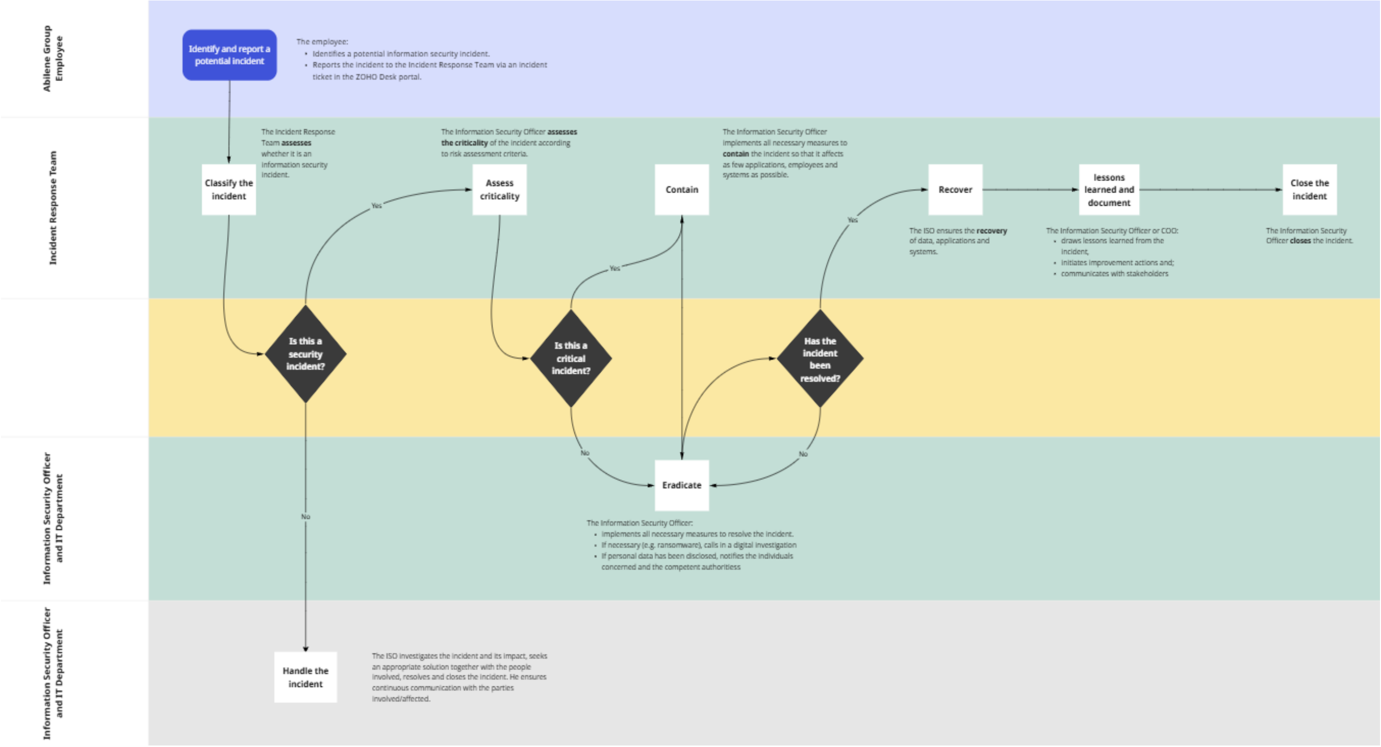
- Responsible for leading the incident investigation and response, and impact assessment and classification.

Information Security Officer (ISO):

- Supports COO in evidence collection, classification, and remediation tasks. May lead if delegated by the COO.

5. Incident Management Controls

a. Incident Management Life cycle


Abilene Group Employee
Incident Response Team
Information Security Officer and IT Department
Information Security Officer and IT Department
Identify and report a potential incident
Classify the incident
Is this a security incident?
Yes
No
Assess criticality
Is this a critical incident?
Yes
No
Contain
Eradicate
Has the incident been resolved?
Yes
No
Recover
lessons learned and document
Close the incident
Handle the incident

The employee:

- Identifies a potential information security incident.
- Reports the incident to the Incident Response Team via an incident ticket in the ZOHO Desk portal.

The Incident Response Team **assesses** whether it is an information security incident.

The Information Security Officer **assesses the criticality** of the incident according to risk assessment criteria.

The Information Security Officer implements all necessary measures to **contain** the incident so that it affects as few applications, employees and systems as possible.

The ISO ensures the **recovery** of data, applications and systems.

The Information Security Officer or COO:

- draws lessons learned from the incident,
- initiates improvement actions and;
- communicates with stakeholders

The Information Security Officer **closes** the incident.

The Information Security Officer:

- implements all necessary measures to resolve the incident.
- If necessary (e.g. ransomware), calls in a digital investigation
- If personal data has been disclosed, notifies the individuals concerned and the competent authoritiess

The ISO investigates the incident and its impact, seeks an appropriate solution together with the people involved, resolves and closes the incident. He ensures continuous communication with the parties involved/affected.

b. Incident Detection & Prioritization

We detect events through multiple channels, such as employee reports, vulnerability scans, and vendor alerts. Relevant events are recorded, analyzed, and classified within our ticketing portal by the Incident Response Team (IRT) to determine whether they qualify as incidents. The classification considers potential impacts on confidentiality, integrity, availability, financial exposure, and reputation. The table below defines the severity levels applied during a cyber incident.

Impact	Low	Moderate	Significant	Severe
Value	1	2	3	4

c. Containment, Remediation & Recovery

Phase	Description
1. Containment	Based on the type of incident, the IRT: - proceeds to immediate containment (e.g., shutting down a system, disconnecting it from a network, disabling certain functions, etc.). - Implement short-term fixes (e.g., firewall rules, access restrictions) to stop the spread while root cause analysis continues. - Notify relevant internal stakeholders and, if applicable, external parties and suppliers.
2. Remediation	The IRT eliminates the root cause and any residual threats to prevent recurrence (e.g. deleting malware, disabling breached user accounts, identifying and mitigating all vulnerabilities that were exploited, etc.).
3. Recovery	The IRT restores systems to normal operation, confirms that the systems are functioning normally, and remediates vulnerabilities to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, etc.

d. Lessons Learned

The IRT initiates a post-incident review within 10 working days of incident closure. Severe incidents require a formal meeting chaired by the CEO, including participation from executive management. Lessons learned for other incidents may be conducted through appropriate channels, depending on the severity of the incident and the specific needs identified during the response, including:

- Structured debrief involving system and process owners.
- Informal review within the IRT to update quick response checklists.

e. Forensic

The IRT documents all actions, timestamps, and personnel involved throughout the incident in our ticketing portal.

When forensic analysis is required, the IRT activates the MSSP under contract to collect and analyze volatile data (e.g., memory dumps, logs, and system states) and other relevant information prior to remediation.

6. Document Control

a. Approval

This version is validated as of 01.11.2025 and supersedes all previous versions. For further information, please contact us via email: request@suppliershield.ch.

Title	**Incident Management Procedure**
Approved By	Alexis Hirschhorn – CEO
Date of Approval	15.10.2025
Version Number	1.6

b. Version History

Version	Date	Reason for Amendment
V1.0	09.05.2022	Initial version
V1.1	15.05.2022	Modified and approval
V1.2	10.04.2023	Minor changes
V1.3	23.04.2024	Minor changes
V1.4	15.03.2024	Minor changes
V1.5	28.04.2025	Review and modified
V1.6	15.10.2025	Review and modified