Date	Name	Role	Change	Version
Wed Aug 06 2025	Tim Murnaghan	CTO	Approved	V1.0

Incident Management Policy

1. General

1.1 Integrum ESG (“the Company”) must establish a clear process for managing information security incidents. This includes defining effective incident management procedures, assigning roles and responsibilities, and ensuring effective communication.

1.2 The Incident Management Policy and Procedure (“the Policy”) determines information security incident management methods, including effective identification, repairs, investigation, prevention, and follow-up actions.

1.3 This Policy addresses limited information security incidents and does not go into the severe incidents that could shut down the activities of the Company. For severe incidents, see the Company’s Disaster Recovery and Business Continuity Plan.

2. Purpose and Scope

2.1 The purpose of this Policy is to provide clear guidance on identifying and managing information security incidents. It outlines the steps to take when an incident occurs, ensuring a quick and effective response to minimise damage and prevent future issues.

2.2 This Policy outlines specific responsibilities for the Company’s Incident Response Team, detailing the processes they must follow to assess, contain, investigate, and resolve security incidents.

2.3 If a security incident involves a breach of personal data, the relevant legal and compliance personnel will be informed. They will help manage the response to the incident and ensure proper communication both inside and outside the Company.

3. Definitions

3.1 **Customer:** an individual or business that purchases the Company’s services.

3.2 **Employee**: includes full-time and temporary employees, contractors, and consultants of the Company.

3.2 **Personal Data**: any data that can be used, directly or indirectly, to identify an individual.

3.3 **Personal Data Breach:** when personal data held by the Company is processed, disclosed, or accessed in an unauthorised or unlawful way, destroyed, lost, or altered.

3.4 **Security Incident:** an irregular or adverse event that occurs to user data or personal data, or that involves the availability and integrity of the Company's systems or networks. Examples of security incidents may include;

3.4.1 Loss or theft of data, or equipment (personal or Company-owned) on which data is stored;

3.4.2 Personal Data breaches;

3.4.3 Breach or loss of confidential data;

3.4.4 Denial of Service (DoS) and Distributed Denial of Service (DDoS);

3.4.5 Hacking attacks;

3.4.6 Malware activity such as trojan horses, viruses, and worms;

3.4.7 Human error or employee negligence;

3.4.8 Attempted fraud involving electronic or physical systems and functions; and

3.4.9 Suspected impropriety by the user, service provider, or vendor.

3.5 **Incident Response Team**: personnel from the Company responsible for responding to and managing security incidents.

3.6 **User:** any individual who is authorised to use the Company's services, or has access to any of the data managed by the Company.

4. Responsibilities

4.1 The responsibility to follow this Policy applies to all Company employees.

4.2 The CISO is responsible for developing, maintaining, and implementing this Policy.

5. Document Ownership

5.1 The Policy Owner is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the Company's review requirements. A current version of this document is available to all members of staff in the company Shared Drive, Folder, etc.

Incident Management Procedure

6. Procedure Overview

6.1 As part of the Company's information security training, employees will learn how to recognise potential security incidents. If an employer suspects or identifies a security incident, they must immediately report it to the Incident Response Team who will determine if a security incident has occurred.

6.2 If a security incident is confirmed, then the Incident Response Team will take the following immediate actions:

6.2.1 perform further tests to clarify the scope of the event and the damage caused to the Company's systems; and

6.2.2 Take immediate action to contain the event and limit the damage to the Company's systems. The Incident Response Team will manage the incident in cooperation with relevant employees in the Company. They will seek to minimise the damage caused due to the event and act as quickly as possible to restore Company operations.

6.3 In the case of a data breach where the Company is required to inform law enforcement authorities, the Incident Response Team must retain evidence of the event and notify the relevant law enforcement authorities according to the notification procedure and relevant regulations.

6.4 After handling the security incident, the Incident Response Team, and the relevant employees, will investigate the cause. The goal is to understand what happened and find ways to prevent similar security incidents in the future. The findings will be recorded using an incident management form (see Annexure A).

6.5 The Incident Response Team will be responsible for tracking the implementation of the corrective actions and assessing how effective they are. The Incident Response Team will inform the Company of any issues in managerial review meetings.

7. The Security Incident Response Process

7.1 The response process consists of three phases; (1) identification phase, (2) assessment phase, and (3) response phase.

7.2 **Identification**: The security incident is recognised, reported to, and confirmed by the Incident Response Team.

7.3 **Assessment**: The Incident Response Team analyses the security incident for the possible causes. The assessment should include the following steps;

7.3.1 Record the date and time when the security incident was discovered, and the date and time when the response efforts begin.

7.3.2 Alert the Incident Response Team responsible for managing the security incident.

7.3.3 Establish a reporting and communication channel.

7.3.4 Document everything that was done and everyone who was contacted regarding the security incident (i.e. who discovered it, who reported it, to who was it reported, what type of breach occurred, what was stolen, how was it stolen, and what systems were affected).

7.3.5 Assess priorities and risks based on what is known about the security incident.

7.3.6 Classify the security incident as one or more of the following;

7.3.6.1 Virus Security Breach;

7.3.6.2 Personal Data Breach;

7.3.6.3 Distributed Denial of Service; or

7.3.6.4 Unauthorised use of an employee's credentials.

7.3.7 Assign and establish team roles and responsibilities concerning the management of the security incident.

7.4 **Response**: The Incident Response Team responds to each type of security incident accordingly.

7.5 If a security incident involves a personal data breach, the Company will follow the steps outlined below under 'Personal Data Breach'.

8. Classification of Security Incidents and Their Response Protocols

The below outlines the different security incidents and the response protocols for each.

8.1 Virus Security Breach

8.1.1 The Incident Response Team alerts management of the security incident.

8.1.2 The Incident Response Team informs employees who use infected devices that resources will not be available.

8.1.3 A security incident case ticket is opened in the Company's security incident management application with a description of the security incident. All logs reviewed during the security incident will be attached to the ticket as evidence.

8.1.4 Infected systems are taken off the network, and virus scans are run to evaluate a complete diagnostic of the network.

8.1.5 All servers are diagnosed to determine if the breach has penetrated other areas of the network.

8.1.6 Infected systems are fixed and tested to make sure they are running properly.

8.1.7 Cleaned servers are reintroduced into the network for normal operation.

8.1.8 Once the security incident is resolved, inform employees that resources are available again.

8.1.9 Document the breach and resolution in the security incident case ticket.

8.1.10 Close the security incident case ticket.

8.2 Personal Data Breach

8.2.1 The Incident Response Team alerts management of the personal data breach.

8.2.2 The Incident Response Team determines the type and amount of personal data potentially exposed.

8.2.3 Open a security incident case ticket.

8.2.4 Interview those involved in discovering the personal data breach.

8.2.5 Analyses the personal data breach to determine the root cause.

8.2.6 Fix the issue that caused the breach and prevent further possible damage.

8.2.7 Stop additional loss by isolating the impacted system and its services.

8.2.8 Replace affected machines with clean ones.

8.2.9 Change all passwords and use separate passwords for different accounts and services.

8.2.10 Warn employees to be aware of any suspicious queries from third parties, which could be related to the breached data (e.g. ‘phishing’ attacks).

8.2.11 Engage in specialised privacy legal counsel to determine the legal and contractual notification obligations.

8.2.12 The Incident Response Team must review and evaluate:

8.2.12.1 The types of personal data that were breached;
8.2.12.2 The regulations governing the specific personal data beach;
8.2.12.3 Whether the breach is likely to result in a high risk to a data subject’s rights and freedoms; and
8.2.12.4 The security measures that were implemented and applied to the personal data affected by the breach.

8.2.13 Notify affected data subjects of the breach.

8.2.14 Document the breach and resolution in the security incident case ticket.

8.2.15 Close the security incident case ticket.

8.3 Distributed Denial of Service

8.3.1 Open a security incident case ticket.

8.3.2 Notify affected users.

8.3.3 Isolate the compromised system from the rest of the network.

8.3.4 Enable alternative communication channels for the process that is under attack.

8.3.5 Find the source of the attack.

8.3.6 Ensure that impacted services can be operational again.

8.3.7 Inform users of reintroducing suspended services, applications, and modules.

8.3.8 Document the breach and resolution in the security incident case ticket.

8.3.8 Close the security incident case ticket.

8.4 Unauthorised Use of an Employee's Credentials

8.4.1 Open a security incident case ticket.

8.4.2 Notify the employee.

8.4.3 Suspend the employee's account in the relevant management system.

8.4.4 Analyse the user's actions during the attack by reviewing network and local logs to identify what was attacked, and investigate the source of the employee's credentials and how they were misused.

8.4.5 Undo malicious actions made by the user.

8.4.6 Document the breach and resolution in the security incident case ticket.

8.4.7 Close the security incident case ticket.

8.5 General Security Incident

8.5.1 The Incident Response Team alerts management [and legal] of the security incident.

8.5.2 Open a security incident case ticket.

8.5.3 Prepare an assessment of the security incident's effect on external partners, vendors, and customers.

8.5.4 Set a deadline to fix the issue if it can't be solved immediately.

8.5.5 Fix any damage, identify and address vulnerabilities, and prepare a summary report. Document the breach and resolution in the security incident case ticket.

8.5.6 Close the security incident incident case ticket.

9. Reporting Security Incidents

9.1. Users must immediately report irregular or suspicious activities in their accounts and working environments. Examples of irregular or suspicious activities include:

9.1.1 A user is locked out of their account or device unexpectedly without reason;

9.1.2 The fingerprint function on a user's device is not functioning;

9.1.3 A user's device (e.g. laptop, smartphone, tablet) containing Company data is lost or stolen (personal or company-owned);

9.1.4 Signs of unknown activity are observed, such as unknown files in the file directories and unexplained changes to desktop settings;

9.1.5 An employee is suspected or found to have violated information security procedures;

9.1.6 There is suspicion that Company information has been or may be damaged, disclosed, modified, or deleted; and

9.1.7 Detection of attempted or successful unauthorised access to a system or its data.

9.2. When a security incident is detected, a Security Incident Report Form or a Corrective Action Form must be completed and submitted to the [CISO].

9.3 The Company must request information from its cloud service provider to enable the Company to do the following:

9.3.1 To report an information security event it has detected to its cloud service provider;

9.3.2 The cloud service provider to receive reports regarding an information security event detected by the cloud service provider; and

9.3.3 The Company to track the status of a reported information security incident.

9.4 Annually, the [CISO] must report to the [CEO], as part of the management review, about all critical security incidents, their impact, and the actions taken to prevent similar incidents in the future.

10. Solving Security Incidents

10.1 The security incident handling procedure will include the following stages.

10.2 **Immediate response**:

10.2.1 If a security incident is in progress, immediate steps must be taken to block the incident and the attacker, to prevent further damage.

10.3 **Information gathering**:

10.3.1 Information about the incident must be collected using internal and external sources

10.3.2 Necessary evidence must be collected and documented in case legal action is taken.

10.3.3 All evidence must be backed up to ensure availability and integrity.

10.4 **Analysis and tracking**:

10.4.1 The [CISO], in consultation with other entities, must analyse the incident and identify and track the following;

10.4.1.1 The source of the incident;

10.4.1.2 Systems involved in the incident, both attacked and in danger of an attack.

10.4.1.3 Potential impact on the confidentiality, integrity, and availability of the information systems and information of the Company and customer data;

10.4.1.4 Current status of the incident; and

10.4.1.5 Corrective measures that need to be taken.

10.5 **Response plan (remediation)**:

10.5.1 The possible scenarios of security incidents and instructions for handling them must be defined.

10.6 **Repair and recovery**:

10.6.1 Execute the response plan. The [CISO] will be responsible for organising the response to the attack and for coordinating recovery activities.

10.7 **Notification of stakeholders**:

10.7.1 The [Support Team] must notify the customers of the breach.

10.8 **Feedback and lessons learned**:

10.8.1 After an incident has ended and the systems have returned to normal activity, the [IT Manager] must check the faults that enabled the incident.

10.8.2 The [IT Manager] must gather feedback from all the relevant parties.

10.8.3 The [CISO] and [IT Manager] must conclude and define measures to prevent future incidents.

10.9 **Implementing corrective and preventative measures**:

10.9.1 Restore damage that was not fixed when the incident was handled;

10.9.2 Instal relevant patches and software updates;

10.9.3 Implement security controls and software updates;

10.9.4 Make enhancements or amendments to relevant security procedures;

10.9.5 Distribute the conclusions and instructions for preventing similar attacks with the relevant parties; and

10.9.6 Where the incident is caused by an internal employee, [HR] will handle disciplinary actions based on the severity of the violation; and

10.9.7 Take legal action against external offenders where necessary.

11. Escalation Procedure

11.1 When a security incident becomes a serious threat and requires extra handling beyond the usual response plan, the escalation procedure must be followed. An incident is escalated when standard response steps are insufficient to contain or resolve it. The escalation procedure follows the [Information Security Policy].

11.2 The escalation procedure is initiated by the personnel who determine that the incident cannot be resolved through the standard procedure.

11.3 Escalation rules should be clearly defined to ensure the incident is resolved quickly and effectively.

Annexure A: Security Incident and Corrective Action Form

Incident Date: [*insert*]

Report No.: [*Insert*]

Incident Description: [*Insert*]

Immediate action taken to respond to the incident:

- Status
- Schedule
- Responsibility
- Action description

Cause of the incident:

Corrective actions taken to prevent the incident from taking place in the future:

- Status
- Schedule
- Responsibility
- Action description

Effectiveness of the corrective action:

- The date for the effectiveness check
- The due date for the effectiveness check
- Effectiveness check results

Date: [*insert*]

Name: [*insert*]

Signature: [Insert]