	No of Pages	1 of 5
	Document Classification:	Internal
	Effective Date	1 Aug 2025
INFORMATION SECURITY DISCIPLINARY PROCESS	Doc No	ISMS-PPL-03
	Revision	1.0

AMENDMENTS LOG

Revision History

Version	Revision Author	Reviewer / Approver	Date	Summary of Changes
1.0	Nor Asfiah Binte Jamalludin (ISMS MR)	James Chia (CEO)	1 Aug 2025	Initial Release



	No of Pages	2 of 5
	Document Classification:	Internal
	Effective Date	1 Aug 2025
INFORMATION SECURITY DISCIPLINARY PROCESS	Doc No	ISMS-PPL-03
	Revision	1.0

TABLE OF CONTENTS

PURPOSE	3
SCOPE	3
REFERENCE	3
RESPONSIBILITIES & AUTHORITIES	3
EMPLOYEE DISCIPLINARY PROCESS	3
1. General Principles	3
2. Process Steps	4
2.1 Information Security Breach	4
2.2 Investigation	4
2.3 Results of Assessment	5
2.4 Appeal	5

	No of Pages	3 of 5
	Document Classification:	Internal
	Effective Date	1 Aug 2025
INFORMATION SECURITY DISCIPLINARY PROCESS	Doc No	ISMS-PPL-03
	Revision	1.0

PURPOSE

This disciplinary process is intended for use in the event that an information security breach has occurred. Before following this procedure, a full investigation should be carried out to establish the facts of the breach and to ensure that any disciplinary action is justified. This investigation must be documented.

It is intended that this process will ensure fair and proportionate treatment of employees and will take into account the following factors:

- The nature of the breach
- The effect of the breach on the organization
- The clarity of the procedures involved
- The amount and quality of the training received by the employee
- Whether the employee has committed a security breach before
- Any relevant legal factors
- Whether the offense was intentional (malicious) or unintentional (accidental)

SCOPE

This control applies to all employees of the organization.

REFERENCE

ISO/IEC 27001 Standard Annex A 6.4 Disciplinary Process

RESPONSIBILITIES & AUTHORITIES

Top Management has the prime responsibility and approval authority for this control.


HR is responsible to ensure that the employee disciplinary process for any information security breach is carried out as per this procedure.

EMPLOYEE DISCIPLINARY PROCESS

1. General Principles

The following general principles apply to the disciplinary process set out in this document:

- The disciplinary process will be triggered by HR and will involve the immediate superior of the employee concerned, the MR, IT, DPO and the management, if necessary.

	No of Pages	4 of 5
	Document Classification:	Internal
	Effective Date	1 Aug 2025
INFORMATION SECURITY DISCIPLINARY PROCESS	Doc No	ISMS-PPL-03
	Revision	1.0

- The process will allow for proportionate action depending on the severity of the information security breach.
- The process will allow for graduated action in the event of repeated breaches by the same individual.
- The process will be carried out in a timely manner in accordance with business needs.
- A fair investigation of both sides will be allowed and meetings will be held at times that do not unreasonably favour either party.
- The employee will have the right to appeal at each stage of the process.
- The details of the breach and the progress of the disciplinary process will be documented by HR and will be regarded as confidential.
- The identity of the individuals subject to disciplinary action should be protected.
- Any person can report a breach to the MR. The individual who reports a breach (whistle-blower) should be protected. The individual subject to disciplinary action and other employees who are not authorized to do investigation will not be informed of who reported the breach, where appropriate and as requested by the whistle-blower.

2. Process Steps

2.1 Information Security Breach

The process is initiated by the detection of an information security breach. This may be a relatively minor event such as the unauthorised use of someone else's user account or something more major such as the deliberate theft of confidential information or unauthorised disclosure of personal data that is likely to cause significant harm. Also, violation of policies on information security or non-fulfilment of the user's information security responsibilities shall be regarded as cause for disciplinary action.


The handling of the breach itself will be according to the procedures set out in *ISMS-ORG-10 Information Security Event & Incident Management*.

2.2 Investigation

At an appropriate time after the information security breach has occurred, an investigation will be arranged by HR to establish:

- The circumstances of the breach, including date, time, sequence of events, information, type of personal data, and systems affected
- The root cause of the breach
- The immediate effect of the breach on the organization
- Whether existing policies and procedures were followed
- If not, then whether the breach would have been avoided if existing policies and procedures had been followed
- The individuals involved

The results and conclusions of the investigation will be documented.

	No of Pages	5 of 5
	Document Classification:	Internal
	Effective Date	1 Aug 2025
INFORMATION SECURITY DISCIPLINARY PROCESS	Doc No	ISMS-PPL-03
	Revision	1.0

2.3 Results of Assessment

In the event that the investigation concludes that there may be a case for disciplinary action against one or more individuals, an assessment will be carried out to decide the next steps. The participants in this assessment should include:

- The individual's immediate superior
- The HR, MR and other person(s) primarily responsible for the investigation e.g., IT
- The Data Protection Officer (DPO) for data breach
- The Management, for dismissal actions

The individual employee may be requested to participate in parts of the assessment, if appropriate. In some circumstances it may be appropriate to suspend the employee whilst the assessment is taking place.

The outcome of the assessment will be a decision regarding which of the following actions to take:

Severity of violations	Disciplinary Actions
Minor	This includes violation such as responding to a phishing email. 1 st offense: counselling by HR / MR 2 nd offense: warning letter from HR 3 rd offense: may lead to permanent loss of access to system or termination.
Major	This includes deliberate action to obtain gain or cause harm. May lead to permanent loss of access to system or termination.

The action should be communicated to the employee by HR.

2.4 Appeal

In the event that the employee wishes to exercise a right to appeal this must be notified in writing to HR within two weeks of the disciplinary decision.

An appeal hearing will be held. The result of the appeal will be communicated to the employee in writing by HR.