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

TABLE OF CONTENTS

PURPOSE

This document provides guidelines concerning how information security events are recognized within the organisation and a decision made about whether they should be considered to be information security incidents and managed accordingly.

DEFINITIONS

Information security events are commonly defined as "any change of state that has significance for the management of information security".

A **weakness or vulnerability** refers to a flaw in the asset or control that can leave it open to attack. It may refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information exposed to a threat.

A **threat** refers to a potential cause of an unwanted incident, which can result in harm to a system or organization.

An **incident** is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

SCOPE

This control applies to all systems and processes that constitute the organization's information assets, including the people who have access to information.

REFERENCE

ISO/IEC 27001 Standard	Annex A 5.24 Information security incident management planning and Preparation Annex A 5.25 Assessment and decision on information security events Annex A 5.26 Response to information security incidents Annex A 5.27 Learning from information security incidents Annex A 5.28 Collection of evidence

RESPONSIBILITIES & AUTHORITIES

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

The Incident Response Team (IRT) shall be alerted on the events that are likely to be flagged up and be able to recognize which ones genuinely represent information security incidents. This also encompasses being notified of weaknesses / vulnerabilities that may leave information exposed to a threat. The IRT is responsible to assess which ones need to be handled and which ones are just noise. This could be the

difference between feeling continuously swamped and successfully protecting your organization from attack.

For events, vulnerabilities or weaknesses involving personal data, the Data Protection Officer (DPO) must be alerted and shall take part on the assessment and management of the said events and weaknesses.

PROCEDURE

1 Reporting Weakness, Vulnerabilities & Threats

All personnel must promptly report known or suspected security weaknesses, vulnerabilities, or threats to IT or MR via email or verbally. If personal data is involved, the MR collaborates with the DPO.

IT, MR and if personal data is involved, the DPO:

- Assess and document the issue
- Update the risk register if necessary
- Ensure controls are implemented or enhanced
- Verify remediation effectiveness

System Admins are responsible for reviewing and applying required patches and updates.

2 Event Management

2.1 Detection and Notification

Security events may be detected through:

- Automated monitoring (e.g., SIEM, system agents, local event logs)
- Manual reporting (e.g., staff, customer support tickets, authorized messaging tools)

Customer-related events are triaged by Support; all others are assessed by the Information Response Team (IRT).

2.2 Event Assessment

Events are categorized based on significance:

- **Informational:** No action needed (e.g., successful logins, backups).
- **Warning:** Requires monitoring; thresholds may soon be exceeded.
- **Exception:** Indicates abnormal behaviour, potential impact, or policy breach.

Key indicators of an exception include:

- Malicious activity
- Involvement of personal or classified data
- Breach of security policy
- High impact or potential escalation

Exceptions are treated as incidents.

2.3 Correlation and Response

Events are correlated via:

- Local device logs
- Remote monitoring systems (e.g., SIEM)

Based on correlation, responses include:

- **Automated actions** (e.g., reboot, lockout)
- **Human alerts** for manual intervention
- **Escalation** to incident or change management, if applicable

2.4 Review and Optimization

Significant events are reviewed to:

- Ensure proper handling
- Identify trends
- Refine event filtering and alerting rules to maintain an effective signal-to-noise ratio

2.5 Event Closure

Events may close automatically (e.g., system recovers and logs resolution) or remain open until manual action is taken.

- **Informational:** Logged only
- **Warnings:** Monitored or resolved
- **Exceptions:** Managed as incidents per incident response procedure

3 Incident Management

When an incident is detected, the Information Response Team (IRT) conducts an initial impact assessment to determine:

- Affected systems and assets
- Type and scope of data compromised (including personal data, if applicable)
- Business impact and affected units
- Likely cause and duration

3.1 Impact Assessment

This impact assessment should estimate:

- The extent of the impact on IT infrastructure.
- The information assets that may be at risk or have been compromised
- For compromised personal data, the types of personal data that have been compromised and the volume of affected individuals
- The likely duration of the incident i.e., when it may have begun
- The business units affected and the extent of the impact to them
- Initial indication of the likely cause of the incident

3.2 Incident Classification and Prioritization

Incidents are prioritised based on impact:

Incident Type	Priority	Target Response	Description
Major Incident	P1 - High	Within 24 hours	Major incident that results in significant disruption to the business. Examples: • Malware has been detected and is spreading across the company's systems • Unauthorized access has been detected to significant amounts of confidential data • Platform is unavailable to customers / users due to a possible denial of service • Reportable data privacy breach - The compromised personal data is likely to result into harm to individuals (regardless of the number) OR affects 500 or more individuals (regardless of the types of personal data)
Minor Incident	P2 - Medium	Within 2 working days	Localised disruption / inconvenience affecting a few users only. Examples: • Single system unavailable • Virus alert on a single computer • Unauthorized access has been detected to data of lower sensitivity • Non-reportable data breach

The IRT Lead decides whether to activate the incident response process, assemble the team, and escalate as needed (e.g., authorities, partners). This is likely to be the case for all "P1" priority incidents. For "P2" priority incidents, the IRT Lead may decide if there is a need to assemble the team and activate this procedure, where deemed appropriate.

3.3 Activating the Incident Response

Guidelines for whether this procedure should be initiated for any particular incident of which the IRT Lead has been notified are if any of the following applies:

- there is evidence of deliberate human interaction for malicious purposes
- there is significant actual or potential disruption to business operations
- there is obvious potential for the situation to worsen if not appropriately addressed
- the actual or potential impact on the organization is significant
- a set of behaviours known to be malicious is displayed
- there is any other reason to be suspicious

In the event of disagreement or uncertainty about whether or not to activate this procedure, the decision of the IRT Lead will be final.

If it is decided not to activate this procedure, then a plan should be created to allow for a lower-level response to the incident within normal channels. This may involve just documenting action plans and timelines by the action owners in the organisation's the incident logging system.

If the incident warrants the activation of this procedure, the IRT Lead will start to assemble the IRT.

3.4 Assemble the IRT

The IRT will generally consist of the following people in the roles specified, although the exact make-up of the team will vary according to the nature of the incident.

Role	Main role holder	Responsibilities
IRT Lead	CEO	● Decides whether or not to initiate a response ● Assembles the incident response team ● Overall management of the incident response team ● Acts as interface with the board and other high-level stakeholders ● Final decision maker in cases of disagreement ● Prepares for meetings and takes record of actions and decisions
DPO	Appointed DPO	● Ensure effective management of data protection risks ● Be involved in the management of all incidents which relate to the processing of personal data (data privacy breach) ● Ensure the timely identification and recording of data privacy breaches ● Ensure that data protection legislation, regulation and practice are followed ● Provide advice in respect of data protection arrangements ● Act as a contact point for supervisory authorities and individuals and ensure timely notification to required

		parties, taking into account the applicable legislation and/or regulation
HR	Operations Lead	● Responsible for ensuring internal communications are effective ● Manage staff welfare
Communications	Marketing Lead	● Decides the level, frequency and content of communications with external parties such as the media ● Defines approach to keeping affected parties informed e.g., employees, customers
IT	Technical Lead	● Provides input on technology-related issues ● Assesses the extent and impact of the incident ● Liaises with the IRT on an on-going basis to provide updates and answer any questions required for decision-making by the IRT on information technology arrangements required

The table below shows who is either Responsible (R), Accountable (A), Consulted (C), or Informed (I) at different stages of the procedure.

Task	**IRT Lead**	**Tech**	**DPO**	**Comms/HR**	**User**
Incident detection	A/R	R	I	I	R
Impact Assessment	A/R	R	R	I	I
Assemble incident response team	A/R	C	C	C	I
Containment	A/R	R	C	I	I
Investigation and collection of evidence	A/R	R	C	I	C
Eradication	A/R	R	C	I	I
Recovery	A/R	R	C	I	I
Monitoring	A/R	R	R	I	I
Communication	A/R	C	C	R	I
Notification	A/R	C	R	C	I
Post-incident review	A/R	R	R	C	C

3.5 Incident Response Phases

3.5.1 Containment

Immediate steps are taken to limit the spread and impact of the incident (e.g., network isolation, account disabling, firewall rule changes).

Refer to Annex A for the possible containment for the different types of potential information security incidents.

3.5.2 Investigation and Evidence Collection

The IRT gathers data to determine the root cause and scope. The evidence will be kept in a safe place where it cannot be tampered with and a formal chain of custody established. The evidence may be required:

- For later analysis as to the cause of the incident
- As forensic evidence for criminal or civil court proceedings
- In support of any compensation negotiations with software or service suppliers

Audit logs may be examined to piece together the sequence of events; care should be taken that only secure copies of logs that have not been tampered with are used.

Particularly (but not exclusively) if foul play is suspected in the incident, accurate records must be kept of the actions taken and the evidence gathered in line with digital forensics guidelines. The main principles of these guidelines are as follows:

Principle 1 – Don't change any data. If anything is done that results in the data on the relevant system being altered in any way then this will affect any subsequent court case.
Principle 2 – Only access the original data in exceptional circumstances. A trained specialist will use tools to take a bit copy of any data held in memory, whether it's on a hard disk, flash memory or a SIM card on a phone. All analysis will then take place on the copy and the original should never be touched unless in exceptional circumstances e.g., time is of the essence and gaining information to prevent a further crime is more important than keeping the evidence admissible.
Principle 3 – Always keep an audit trail of what has been done. Forensic tools will do this automatically but this also applies to the first people on the scene. Taking photographs and videos is encouraged as long as nothing is touched to do it.
Principle 4 – The person in charge must ensure that the guidelines are followed.

Note: If it is judged to be likely that digital evidence will need to be collected that will later be used in court, precautions must be taken to ensure that such evidence remains admissible. This means that relevant data must not be changed either deliberately or by accident. It is recommended that specialist advice should be obtained at this point.

3.5.3 Eradication

The extent of the incident and the knock-on implications should be ascertained before any kind of eradication can be determined. Actions to fix the damage caused by the incident must be put through as an emergency change. These actions should be aimed at fixing the current cause (e.g., deleting the malware) and preventing the incident from re-occurring. Any vulnerabilities that have been exploited as part of the incident should be identified.

Depending on the type of incident, eradication may sometimes be unnecessary.

3.5.4 Recovery

Systems are restored to operational status, ensuring vulnerabilities are mitigated. Recovery actions may include restoring from backup, password resets, and configuration changes.

3.5.5 Incident Monitoring and Communication

Ongoing monitoring ensures containment and recovery are effective. Internal and external communications are coordinated by the MR, with support from HR and DPO as required.

In case enquiries from media are received, no members of staff should give an interview with the media unless this is pre-authorised by CEO. In drafting a statement for the media, the following guidelines should be observed:

- Personal information should be protected at all times
- Stick to the facts and do not speculate about the incident or its cause
- Ensure legal advice is obtained prior to any statements being issued
- Try to pre-empt questions that may reasonably be asked
- Emphasise that a prepared response has been activated and that everything possible is being done

3.5.6 Notification

The organisation will always comply in full with applicable legal and regulatory requirements regarding incident notification and will carefully assess any offerings to be made to parties that may be impacted by the incident.

Where a personal data breach has occurred, it shall be assessed by the DPO whether it is likely to result in significant harm or impact to the affected individuals, and how many individuals are affected. Significant harm could include physical, psychological, emotional, economic and financial harm, as well as harm to reputation and other forms that a reasonable person would identify as a possible outcome of a data breach.

Where a data breach is assessed to be likely to result in significant harm / impact to the Individuals or of a significant scale (e.g., involves 500 or more Individuals), the DPO shall conclude that the data breach is notifiable to PDPC (Singapore) and to the affected Individuals.

Note: All data privacy breaches are essentially information security breaches, but not all information security breaches can be classified as data privacy breaches. Only those incidents that involve personal data are considered as data privacy breaches (which is also referred to as "data breach"). Refer to Annex B for the summary of the personal data breach notification points.

3.5.7 Post-Incident Activities

The IRT Lead will decide, based on the latest information from the members of the team, the point at which response activities should be ceased and the IRT stood down. Note that the recovery and execution of plans may continue beyond this point but under less formal management control.

This decision will be up to the IRT Lead's judgement but should be based upon the following criteria:

- The situation has been fully resolved or is reasonably stable

- The pace of change of the situation has slowed to a point where few decisions are required
- The appropriate response is well underway and recovery plans are progressing to schedule
- The degree of risk to the business has lessened to an acceptable point
- Immediate legal and regulatory responsibilities have been fulfilled

All actions taken as part of standing down should be recorded in the IRT meeting minutes. After the IRT has been stood down, the IRT Lead will hold a debrief of all members ideally within 24 hours. The relevant records of the incident will be examined by the IRT to ensure that they reflect actual events and represent a complete and accurate record of the incident. Any immediate comments or feedback from the team will be recorded.

A more formal post-incident review will be held at a time to be decided by top management according to the magnitude and nature of the incident. This may be through the quarterly information security meetings or through an arranged meeting depending on urgency and shall cover knowledge obtained from the incidents that will help avoid its recurrence and can be used to strengthen and improve the information security controls including root cause analysis, impact analysis, corrective measures to prevent recurrence, and lessons learned from operational and policy related issues, resource related issues, employee related issues and management related issues among others that the IRT has experienced.

ATTACHMENTS

Annex A Containment for Different Types of Potential Incidents
Annex B Data Breach Notification (where personal data is involved)

FORM

ISMS-ORG-10-F1 Event / Incident Log

Annex A – Containment for Different Types of Potential Incidents

This section describes the possible containment for different types of potential incidents. The IRT shall ensure that the containment actions are carried out as soon as possible from the time the incident has occurred.

Situation	Symptoms	Cause	Containment
Operating system failure	System is unable to boot	Kernel-related issues	If equipment is a node part of the cluster, then turn off the node; Otherwise switch to redundant secondary. Reinstall operating system; and restore from backup.
Security breach detected	Excessive failed logon attempts	Unauthorized user attempting to gain access to the system	Trace the source of the logon attempts and take actions accordingly
	Excessive attempts to escalate privileges	Unauthorized user attempting to attain higher level of privileges	Trace the source of the excessive attempts and take actions accordingly
	Denial of service attack	Malicious attempt to take down the system	Locate source of attack and block it
	Unauthorized physical access of equipment	Malicious attempt to gain physical access to equipment	Perform thorough inventory check. Escalate and inform relevant parties, including making a police report.
	Malware found	System or security engineer to investigate	Isolate the system. Attempt to remove the malware. Find and stop the spread.
	Sensitive data reported stolen	Unauthorized attempt to steal sensitive data	Isolate the system. Attempt to locate source of entry. Escalate and inform relevant parties, including making a police report.

Situation	Symptoms	Cause	Containment
	Unauthorized access or change or deletion of data	Unauthorized attempts to manipulate with the data in system	Isolate the system. Attempt to identify the data affected and locate source. Escalate and inform relevant parties, including reporting to SingCERT.
	Any other suspicious response from the system	System and security engineer to investigate	Isolate the system. Investigate thoroughly.

Annex B – Singapore Data Breach Notification

Point 1: When to notify PDPC?

The DPO will notify the PDPC of a data breach that is:

- Of a significant scale (i.e., data breach involves personal data of 500 or more Individuals); or
- Likely to result in significant harm or impact to the Individuals to whom the information relates.

  Note: Significant harm could include physical, psychological, emotional, economic and financial harm, as well as harm to reputation and other forms that a reasonable person would identify as a possible outcome of a data breach.

Point 2: How soon does the DPO need to notify PDPC?

As soon as practicable, and in any case no later than 3 calendar days from the day it determines a notifiable data breach has occurred.

Point 3: How should the DPO notify PDPC?

Report to PDPC via https://eservice.pdpc.gov.sg/case/db. For urgent notification of major cases, organization may also contact PDPC at +65 6377 3131 during office hours.

Point 4: What details does the DPO need to include in the notification to PDPC?

- Facts of the data breach – summary of the facts that the organisation has managed to establish thus far, on a best effort basis
- Approximate number of Individuals and types of personal data affected by the data breach; and
- If not intending to notify affected Individuals, brief justification for the organisation's reliance on any applicable exception(s) (refer to point #9)
- Chronology of how the organisation first became aware of the data breach
- Where there is a delay in the notification of the data breach to the PDPC, the reasons for the delay and the supporting evidence
- Plans for managing the data breach
- Whether the breach has already been rectified
- Contact details of the person (DPO) whom PDPC can contact for further information or clarification

Where specific information of the data breach is not yet available, the DPO should send an interim notification based on the most accurate information available at the point in time that the notification is made.

Point 5: When to notify affected Individuals?

Where required (refer to point #9 for exceptions), the organisation should notify the affected individuals of a data breach that is likely to result in significant harm or impact to them at the same time or after notifying the PDPC.

Point 6: How soon does the organisation need to notify affected Individuals?

After notification to PDPC.

Point 7: How should the organisation notify affected Individuals?

The organisation should adopt the most effective way to reach out to them, taking into consideration the urgency of the situation and number of Individuals affected (e.g., emails, telephone, social media).

Notification should be simple to understand, specific and provide clear instructions on what Individuals can do to protect themselves.

Example:
Call and notify affected individuals: "Hi (name), I am calling from <organisation name>. On (date), we first became aware that a data breach has occurred and unfortunately, your personal data such as (e.g., name, medical history, etc) has been leaked to a website. We take this matter very seriously. The confidentiality of your personal data is of utmost importance to us. While we have reported the case to the police and Personal Data Protection Commission (PDPC), please help us protect yourself by <changing your password, cancelling your credit card and monitoring your account for any unusual activities>. We are doing all we can to recover your data and will keep you updated on the status."

Point 8: What details does the organisation need to include in the notification to affected Individuals?

- Background information on how and when the data breach occurred
- Types of personal data involved
- Data breach management and remediation plan – what the organization has done or will be doing in response to the risks brought about by the data breach
- Potential harm that the Individuals might suffer from the breach
- Steps that the Individuals might take to prevent any potential misuse of his/her personal data, or to reduce the significant harm arising from the data breach
- Contact details of the DPO and how affected Individuals can reach the organisation for further information or assistance (e.g., contact numbers, email addresses)

Where specific information of the data breach is not yet available, the organisation should send an interim notification based on the most accurate information available at the point in time that the notification is made.

Point 9: Exceptions to Obligation to Notify Affected Individuals of a Data Breach that is Likely to have a significant harm to them

The organisation may decide not to notify affected Individuals (but it is still required to notify PDPC) if:

- it is able to take action which renders it unlikely that any significant harm will result to an affected Individuals (remedial action exception)
- there are appropriate technological measures applied to the personal data before the data breach which renders the personal data inaccessible or unintelligible to an authorized party (technological protection exception)

- the PDPC or law enforcement agencies may also direct the organisation not to make notifications (such directions would occur where notification may compromise ongoing investigations, or where there are overriding national security or national interests)

In the event that the PDPC determines that the exception does not apply, the organisation would be required to notify the affected Individuals of the data breach.

Point 10: Who else to notify?

Where the organisation is a Data Intermediary (data processor) engaged by the client who is the Data Controller (e.g., the organisation is processing / hosting data on behalf of the client), it will not notify PDPC and/or affected individuals, and will instead notify the affected client about the facts of the data breach, the containment and recovery measures as well as the status, and if there are actions that the client need to take to lessen the possible impact of the breach, and the DPO contact details, as soon as it is discovered (preferably within 24 hours) so that the affected client (a.k.a. Data Controller) can take appropriate actions. The notification to the affected client shall be guided by the contract between them and the organisation where it should specify how the organisation will provide the information necessary for the affected client to fulfil their obligation to notify relevant authorities.

Where the organisation is governed by a sectoral regulator, it may also need to concurrently notify the appropriate regulatory body, or according to the timeframes under their respective requirements or other written law.

If approached by the Media

Spokesperson (Communications Lead) to provide a holding statement. For example, *"We take this matter very seriously as confidentiality of our customers' personal data is of utmost importance to us. We are reaching out to affected customers whose personal data may have been affected at the earliest possible time."*