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

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.

TABLE OF CONTENTS

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.

PURPOSE

This document describes how threat intelligence will be gathered, processed and reported within the organisation to provide awareness of the organisation's threat environment so that appropriate mitigation actions can be taken.

SCOPE

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

REFERENCE

ISO/IEC 27001 Standard Annex A 5.7 Threat Intelligence

RESPONSIBILITIES & AUTHORITIES

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

The Management Representative shall ensure that information relating to information security threats are collected and analysed to produce threat intelligence, and that appropriate mitigation actions are taken.

PROCEDURE

1. Threat Intelligence Levels

The collection, processing and reporting of threat intelligence is vital to the organisation's ability to assess risk and react to the threats it faces to its information security management. Threat intelligence is gathered and reported at three levels; strategic, tactical and operational. These levels are described below:

Level	Description
Strategic	High-level trends about attackers, motivations, and industry-wide risks.
Tactical	Known attacker methods, tools, and vulnerabilities relevant to our systems.
Operational	Real-time indicators of compromise (IoCs) or active threats to our systems.

2. Process Steps

This process sets out the major steps involved in collecting and processing intelligence about threats at the strategic, tactical and operational levels. Each step is described in the following sections.

2.1 Define context and identify information sources

Focus on threats relevant to:

- Our industry
- Tools and platforms we use
- Clients and services we provide

Use trusted and open sources, such as:

- Security vendor bulletins
- Open threat intel platforms
- Regulatory authorities and special interest groups advisories

2.2 Collect and review information

Relevant information will then be collected from the identified sources by whatever method is appropriate (for example, download a report, request for information, subscription to a news feed / email alerts).

2.3 Analyse and act

The information must be stored appropriately and its source clearly recorded to prepare it for analysis including corroborating information with the aim to produce a Threat Intelligence Report at least quarterly.

The Threat Intelligence Report should be relevant to the protection of the organisation and insightful, providing the organisation with an accurate and detailed understanding of the threat landscape.

The collected information must be analysed to define its relevance to, and implications for, the organisation. At the tactical and operational levels, this may include comparing information received from external sources with information available from internal systems, such as event logs to investigate any existing impact to the organisation such as breach.

2.4 Report and communicate

Once sufficient analysis of threat intelligence has been carried out, the resulting information must be presented in an actionable form in the Threat Intelligence Report so the organisation can act on the information quickly and effectively.

Where appropriate, reports from third parties (e.g., independent providers or advisors, government agencies or collaborative threat intelligence groups) particularly at the strategic level may be distributed in their published form. However, analysis should reflect clear guidance about the relevance of such reports to the organisation.

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.

Threat Intelligence Report should be distributed to all areas of the business that may be affected by their contents. This will usually be during the information security quarterly meetings where it will be communicated to the following:

- Top management (mainly for strategic level reports)
- Risk management team so it can be included in the organisation's risk assessment
- Information security steering committee responsible for the application of controls so it can be an additional input to technical preventive and detective controls like intrusion detection system, or anti-malware solutions
- Where appropriate, the organisation may share the information with other organisations (e.g., clients, suppliers) on a mutual basis in order to improve overall threat intelligence

Where Threat Intelligence Report refer to a potentially urgent threat, additional methods of communication which would be timelier will be arranged e.g., ad hoc meetings. Feedback should be requested on each report in order to improve aspects such as format, timeliness and contents.

FORMS

ISMS-ORG-03-F1	Threat Intelligence Report
ISMS-ORG-03-F2	Authorities and Special Interest Group Contact List

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.