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

The purpose of this procedure is to describe the process for conducting internal audit of the organisation's Information Security Management System (ISMS).

SCOPE

This procedure applies to internal audits intended to ensure that the ISMS is effectively implemented and maintained, and conforms to specified requirements or audit criteria.

REFERENCE

ISO/IEC 27001 Standard   9.2 Internal Audit

DEFINITION

Internal Audit	A systematic and independent evidence gathering used to provide input for management review and to declare that the organisation meets specified requirements (audit criteria).
Audit Criteria	Reference point to which audit evidence is compared against to determine how well they are being met.
Audit Evidence	Includes records, factual statements, and other verifiable information that is related to the audit criteria being used.
Audit findings	Result from a process that evaluates audit evidence and compares it against audit criteria.

Types of Audit Findings:

1.	Conformity (C)	Fulfilment of a specified requirement
2.	Nonconformity (NC)	Non-fulfilment of a specified requirement
3.	Opportunity for Improvement (OFI)	A situation or condition that may be weak, cumbersome, redundant, overly complex, or in some other manner, may offer an opportunity to improve the current system or prevent future problems.

Correction	Any action that is taken to eliminate a nonconformity but do not address root causes to prevent recurrence of a nonconformity.
Corrective Action	Steps that are taken to eliminate the root causes of existing nonconformities in order to prevent recurrence.

RESPONSIBILITIES & AUTHORITIES

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

The Management Representative is responsible to ensure that internal audits are conducted at planned intervals. Responsibilities for Internal Auditors and Auditees are detailed below.

PROCEDURE

1.   This procedure addresses the internal audit of the ISMS at least once every calendar year. At the call of top management or the MR, internal audits may be conducted more frequently based on performance and results observed during the previous audits.

2.   The MR works with the internal auditor(s) to prepare the *ISMS-PR-03-F1 Internal Audit Plan.*

   2.1   The plan includes all areas of the organisation, and is based on the status and importance of the area/process being audited.

   2.2   Other considerations include the results of previous audits and changes impacting the organisation.

   2.3   The plan identifies when the audits will take place and what areas to be audited.

   - Each area/process is audited a minimum of 1 time per year.
   - The MR assigns trained internal auditor(s), independent of the area/process to be audited. External auditors may be engaged to carry out the internal audit of the organisation, if necessary.
   - The assigned internal auditor confirms the audit schedule with the assigned auditee(s).

3.   The assigned internal auditor(s) review previous audit reports for the area. All corrective actions from the previous audits that require follow-up are identified and checked by the assigned internal auditor.

4.   The assigned auditor performs the internal audit according to the *ISMS-PR-03-F2 Internal Audit Checklist.*

   4.1   Compliance to the information security management system requirements and to the ISO/IEC 27001 Standard is determined through observation, interview and review of documented information using the internal audit checklist as a guide.

   4.2   A process approach is used by following the steps from start to finish, or from finish to start, and covering all the processes related to the work area being audited.

   4.3   Notes are taken to provide ample details in the event that a nonconformity is noted and can be readily located for corrective action.

4.4 Auditors document the audit findings on the internal audit checklist whether it is a conformity (C), nonconformity (NC), or opportunity for improvement (OFI).

5. At the conclusion of the audit, the auditor discusses the audit findings to the auditee(s) to agree on and write up correction(s) and corrective action(s), whichever is applicable. The assigned auditor prepares the *ISMS-PR-03-F3 Internal Audit Report.*

6. The auditee(s) are responsible for identifying the root cause and completing the internal audit report with correction(s) and corrective action(s), whichever is applicable. Reference shall be made to *ISMS-PR-05 Control of Nonconformity and Corrective Action*. The identified actions shall be implemented as agreed at the post-audit discussion with the auditor.

7. The assigned auditor shall verify the actions taken on the agreed target date to ensure that the problem has been corrected and root cause has been addressed effectively by the implemented corrective actions to prevent it from recurring again. If the actions taken are deemed effective as aforementioned, the NC or OFI can be considered closed. If not effective, the auditor shall recommend alternative actions to close out the NC or OFI.

8. The MR puts all records into the internal audit file:

8.1 The records included are the internal audit plan, checklist and the report complete with the actions taken for any NC and OFI.

8.2 The results of the internal audit are presented for discussion during the Management Review.

FORMS

ISMS-PR-03-F1   Internal Audit Plan
ISMS-PR-03-F2   Internal Audit Checklist
ISMS-PR-03-F3   Internal Audit Report