Internal Audit Report

A. Audit Details

Audit Date(s):		**Report Date:**	
Prepared by:			
Audit Location(s):			
Auditor(s):			
Audit Participants:			
Scope Statement:			

B. Management Summary

[Summarize the findings of the audit, such as in the example below]

This internal audit covered all the elements of the Information Security Management System (ISMS) in line with the ISO/IEC 27001:2022 Standard, and the controls set out in its Annex A with the organisation's Statement of Applicability.

In general, it was found that a good level of support is in place for the ISMS and top management is adequately committed to its success. Documented information was found well maintained and easily retrievable. Roles and responsibilities relevant to information security are clearly understood and fulfilled.

There are 1 nonconformity (NC) and 1 opportunity for improvement (OFI) noted during the internal audit. These areas should be addressed for continual improvement purposes.

C. Audit Criteria and Reference Documents

ISO/IEC 27001:2022, the International Standard for ISMS was used as the basis of the audit criteria. The organisation's documented ISMS was verified to see how the requirements of the Standard are applied. Compliance with applicable legal and other requirements was also assessed.

D. Audit Objectives

In line with the requirements of the standards, the overall objectives of this internal audit are to provide information on whether the organisation's ISMS:

- Conforms to:
  - the organisation's requirements for its established ISMS; and
  - the requirements of the ISO/IEC 27001 International Standard.

- Is effectively implemented and maintained.

E. Status of NCs and OFIs Raised at Last Statement

[Describe status of audit findings from previous year. Examples are given below]

As at the date of this audit, the status of the nonconformities raised at the last assessment was as follows:

Ref.	Description	Type	Actions	Status
NC-01	Resources not discussed at management review	Nonconformity	Minutes of latest management review show resources are now discussed	Closed
NC-02	Information security incident not handled according to procedures	Nonconformity	Additional procedural training has now been delivered	Closed

F. Audit Findings

[Describe the findings of the audit in the areas covered. Examples are given below]

Details of audit findings and evidences have been documented in the internal audit checklist. The audit was done based on sampling check.

There are 1 nonconformity (NC) and 1 opportunity for improvement (OFI) noted during the internal audit as detailed below:

Ref.	NC-01
Type	Nonconformity
Area	Policy and objectives
Clause	5.2 Policy 6.2 Information security objectives and planning to achieve them
Description	Information security policy does not include objectives or a framework for setting them. Objectives have not been set.
Requirements	*Top management shall establish an information security policy that:* *a) is appropriate to the purpose of the organization* *b) includes information security objectives or provides the framework for setting information security objectives* and *The organization shall establish information security objectives at relevant functions and levels.*
Evidence	The policy does not include the required sections and no objectives were evidenced.

Ref.	OFI-01
Type	Opportunities for Improvement
Area	Leadership and commitment
Clause	5.1

Description	Top management could make more use of team meetings to emphasize the importance of the information security management system.
Requirements	*Top management shall demonstrate leadership and commitment with respect to the information security management system by:* *d) communicating the importance of effective information security and of conforming to the information security management system requirements*
Evidence	Minutes of team meetings showed that top management had not attended any within the last 6 months