Information Security Management System Manual

HT-ISMS-MN-03

Document Control

Document Title	Information Security Management System (ISMS) Manual		
Document Id	HT-ISMS-MN-03		
Version		**Date of Release**	
Classification	Internal	**Location**	Intranet / Confluence
Author(s)	**Name**		
	Designation		
Reviewer(s)	**Name**		
	Designation		
Approver(s)	**Name**		
	Designation		

Revision History		
Version	**Date of Release**	**Description of Change**
1.0		Initial version

Document Distribution			
Name	**Department**	**Designation**	**Company**
Employee1	Operations	Vice President	HackTech
Employee2	IT	System Admin	HackTech

1. Overview

HackTech Technologies Pvt Ltd, a cutting-edge technology solution vendor, providing solutions for a dynamic environment where business and technology strategies converge. Our aim is to develop new products & services for implementing prudent business and technology strategies in today's dynamic digital environment.

2. Information Security Management System (ISMS)

HackTech is committed to maintaining the protecting the information and information processing assets of the organization. To achieve this, the organization has embarked upon a program to develop an Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2022 in adherence to all applicable legal and regulatory requirements.

3. Objective

The objective of this document is to guide the organization to define a management system that ensures information security requirements are addressed and Information Security into the Organization's processes. The directions contained in this document apply to organization's users which include Employees, Contractors, Vendors, and any associated person.

4. Context of Organization

4.1. Understanding the Organization and its context

HackTech has determined the Internal and External Issues including Climate Change that can affect achievement of the intended outcome of Information Security Management System.

Refer section 'Internal & External Issues' in document "Context & Scope of the Organization".

4.2. Understanding the needs and expectations of interested parties

HackTech has determined the interested parties that are relevant to Information Security Management System and also the requirements of these parties with respect to information security by ISMS. Determining the scope of Information Security Management System

4.2.1. Scope

Provision of Information Security Management System for the organization which provides various services to customers, including support functions and the interfaces established with third party service providers.

Refer section 'Scope' in document "Context & Scope of the Organization"

4.3. Information Security Management System

This ISMS Manual provides the documented framework required for establishing, implementing, maintaining and continually improving the Information Security Management System of HackTech, in accordance with the requirements of ISO/IEC 27001:2022. The ISMS manual is supported by appropriate policies, procedures and other documented information as required by the standard or as determined by the organization to be necessary to fulfil the requirements of the standard.

5. Leadership

5.1. Leadership and commitment

Top management of HackTech is represented by CEO; are committed to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the ISMS. The top management will inculcate an organization culture to ensure that the ISMS requirements are embedded as part of the HackTech's processes.

5.2. Policy

The top management has established the Information Security Policy that is appropriate to the purpose of the organization and has also identified objectives to support achievement of these policies. These policies would ensure that applicable legal, regulatory and contractual requirements are met, and the Organization provides the required focus for continual improvement.

5.3. Organization roles, responsibilities and authorities

Top management of HackTech has established the responsibilities, and authorities for roles relevant to information security and communicated to respective employees.

6. Planning

6.1. Actions to address risks and opportunities

6.1.1. General

Organization has considered the internal and external issues identified, the needs and expectation of interested parties that are relevant, when planning for the Information Security Management System.

6.1.2. Information security risk assessment

Organization has defined and established information security risk assessment methodology. The methodology includes:

- Criteria for acceptance of risk

6.1.3. Information security risk treatment

Organization has defined and established an information security risk treatment process which is documented as part of Risk assessment methodology, the details are available below:

Refer document “Risk Assessment Methodology”.

6.2. Objectives and planning to achieve them

Organization has established information security objectives at different functions and levels.

These objectives support the achievement of the information security policies. The objectives are measurable and have been communicated to the relevant people involved. The objectives have been formulated taking into consideration the applicable information security requirements and the results of risk assessment and risk treatment. Changes to these objectives will be reviewed and approved by the Top Management.

6.3. Planning of Changes

HackTech will plan the changes to the ISMS as required by the Standard and Business, Customer and Statutory requirements and also as an outcome of Audits & Risk Assessments from time to time. The methodology for major changes will be a Project based change post approval from Management. For minor changes either an MR may be called or mail approval taken and ratified in the next MR.

7. Support

7.1. Resources

Organization has determined and provided the required resources for establishing, implementing, maintaining and continual improvement of Information Security Management System.

7.2. Competence

The necessary competence of persons working under HackTech's control that affects ISMS performance has been determined and maintained. The gap analysis for various individuals performing these roles are carried out once a year or as and when new person joins. Necessary training or mentoring is provided to bridge the identified gaps. Records of competency assessment and fulfilment of gaps are maintained.

Refer document “ISMS Competency Matrix”

7.3. Awareness

HackTech ensures that the resources working under its control are aware of:

- The information security policies

7.4. Communication

HackTech has determined requirements for internal and external communication relevant to Information Security Management System including:

- on what to communicate.
- when to communicate.

7.5. Documented Information

7.5.1. General

The documented information maintained by HackTech for the ISMS includes the following:

- Documented information required by ISO 27001:2022 standard.

7.5.2. Creating and updating

All ISMS documents are protected and controlled by the HackTech policy covering the following:

- Document Approval prior to issue

7.5.3. Control of documented information

All records required for the ISMS are maintained to meet the HackTech operational requirements and the effective operation of the ISMS. Records are controlled as per the guidelines documented in Document Control Procedure.

8. Operation

8.1. Operation planning and control

HackTech has identified and controlled the processes that are needed to meet information security requirements, by having documented Standard Operating Procedures (SOP).

8.2. Information security risk assessment

HackTech has formulated and implemented a risk assessment methodology for reviewing risks at a planned interval of 6 months or as and when significant changes are proposed to occur.

8.3. Information security risk treatment

HackTech has formulated and implemented a risk treatment process as part of the risk assessment methodology, to mitigate the risks identified during the risk assessment process.

9. Performance evaluation

9.1. Monitoring, measurement, analysis and evaluation

To evaluate the effectiveness of the ISMS, HackTech has determined:

a) what needs to be monitored and measured?
b) methods for monitoring, measuring, analyzing and evaluating to ensure valid results.

9.2. Internal Audit

General

The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:

Internal Audit Program

- ISMS audits will be performed in HackTech at least once in six months to review Information Security Management System

Conforms to

- HackTech's own requirements for its Information Security Management System; and
- The requirements of ISO 27001:2022 standards are effectively implemented and maintained.

HackTech will:

- Plan, establish, implement and maintain audit programme(s), including the frequency methods, responsibilities, planning requirements and reporting. The audit programme(s) will take into consideration the importance of the processes concerned and the results of previous audits.

9.3. Management review

General

The top management the organization will review the ISMS at planned intervals (once in six months) to ensure its continuing suitability, adequacy, and effectiveness. This includes assessing opportunities for improvement and requires changes to be clearly documented and records maintained as per defined departmental procedures.

Management Review Inputs

The Management review will include consideration of:

a) The status of action from previous management reviews.
b) Changes in external and internal issues that are relevant to the Information Security Management System;

Management Review Results

The results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system

The output from the management review includes any decisions and actions related to the following:

- Improvement of the effectiveness of the ISMS.
- Issues closed.

10.Improvement

10.1. Continual Improvement

HackTech strives to continually improve the effectiveness of the ISMS using the information security policy, incident investigation results, audit results, analysis of monitored events and management review feedback

10.2. Non-Conformity and Corrective Action

When a Nonconformity occurs, organization will:

a) react to the nonconformity, and as applicable:

1) take action to control and correct it.

2) deal with the consequences.