



# Context and Scope of the Organization

---

HT-ISMS-MN-01

Author- Saurav Chaudhari

## CONFIDENTIALITY

This document is prepared by HackTech. All rights are reserved. No part of this document may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying without the written permission of HackTech. If this copy of the document is a hard copy, it is likely to be an obsolete version. Please check with the author of this document, to ensure that you are referring to the current version.

## Table of Contents

Document Control .....	2
1. Purpose .....	3
2. Context of the Organization .....	3
2.1. Internal & External Issues .....	3
2.1.1. External Issues .....	3
2.1.2. Internal Issues .....	3
2.2. Interested Parties .....	4
2.2.1. Internal .....	4
2.2.2. External .....	4
2.3. Scope .....	4
2.3.1. Location .....	4
2.3.2. Activities .....	4
2.3.3. Information .....	4
3. ISMS .....	5
4. Reference .....	5

## Document Control

<b>Document Title</b>	Context and Scope of the Organization		
<b>Document Id</b>	HT-ISMS-MN-01		
<b>Version</b>		<b>Date of Release</b>	
<b>Classification</b>	Internal	<b>Location</b>	Intranet / Confluence
<b>Author(s)</b>	<b>Name</b>		
	<b>Designation</b>		
<b>Reviewer(s)</b>	<b>Name</b>		
	<b>Designation</b>		
<b>Approver(s)</b>	<b>Name</b>		
	<b>Designation</b>		

Revision History		
<b>Version</b>	<b>Date of Release</b>	<b>Description of Change</b>
1.0		Initial version

Document Distribution			
<b>Name</b>	<b>Department</b>	<b>Designation</b>	<b>Company</b>
Employee1	Operations	Vice President	HackTech
Employee2	IT	System Admin	HackTech

## 1. Purpose

The purpose of this document is to record the Context and Scope of the organization (HackTech) for the information security management system (ISMS) based on ISO 27001:2022 standard.

## 2. Context of the Organization

### 2.1. Internal & External Issues

HackTech has determined internal and external issues that are relevant to its purpose and that affects its ability to achieve the intended outcomes of its ISMS.

#### 2.1.1. External Issues

- **Maintaining Compliance:** HackTech has the responsibility to comply with applicable legal, regulatory and contractual requirements.
- **Climate change:** Climate change modeling and research rely heavily on vast amounts of data to predict trends, impacts, and mitigation strategies. These data sets are often stored and shared through digital platforms, making them susceptible to cyberattacks, manipulation etc. Similarly, climate change also increases the vulnerability of many critical infrastructures which are digitized and susceptible to cyber-attacks. HackTech has the following practices to cope with climate change and reduce the carbon footprint
  - Adopting Remote Work
    - HackTech encourages remote work as it minimizes the need for daily commutes, reducing transportation emissions. It also reduces energy consumption in the office, as fewer people working in the building means less heating, cooling, and lighting is required. Hybrid & remote work arrangements have decreased the company's physical office space needs, cutting down on overheads.
  - Cloud Based Solutions for Efficiency
    - All the development servers within HackTech are on the Cloud leveraging the cloud-based infrastructure from providers that operate on renewable energy. Cloud computing has reduced the need for physical hardware, lowered energy costs, and ensured efficient use of resources.
  - Go Paperless
    - HackTech primarily is a paperless office which is an effective way to cut down on resource waste. Invoicing with customers is digitized, document sharing, and internal communications has eliminated paper waste and reduced storage needs, which is in alignment with eco-friendly principles.

#### 2.1.2. Internal Issues

- **Web Application Security:** Our business is dependent on the web application/s which can be a potential target for hackers as it is published on the internet.

## 2.2. Interested Parties

HackTech has determined the interested parties relevant to its ISMS including their needs and expectations.

### 2.2.1. Internal

Interested Party	Needs & Expectations
Management	The reputation of the company and its management could be questioned if there is a security breach.

### 2.2.2. External

Interested Party	Needs & Expectations
Customers	<ul style="list-style-type: none"><li>• Maintaining data security.</li><li>• Compliance to the applicable legal &amp; regulatory requirements.</li><li>• Availability of Service</li><li>• Adherence to contract</li><li>• Adherence to Information Security requirements</li><li>• Meeting Service Level Agreements</li><li>• Cooperation for audits</li><li>• Ontime communication of changes</li><li>• Reporting of any InfoSec / Data breaches as applicable</li></ul>

## 2.3. Scope

The scope for the Information Security Management System (ISMS) is:

*Design, Development, Implementation and Support of Software Applications and Products.*

*This is in accordance with the Statement of Applicability version 0.0 DATE.*

### 2.3.1. Location

Office location

### 2.3.2. Activities

Activities undertaken to provide the solutions are grouped into the following areas:

Core Operations

- Software Development

Support Functions

- IT Support

### 2.3.3. Information

The ISMS protects information held and processed, which includes:

- End Customer Information
- Product Information

### 3. ISMS

HackTech Technologies has established and implemented an Information Security Management System (ISMS). As an organization, we are maintaining and continually improving the same, in accordance with the requirements of ISO 27001:2022 standard.

### 4. Reference

- ISO 27001:2022 – Clauses 4.1, 4.2, 4.3 and 4.4