**<Company Logo>**

**<Company Name>**

**Information Security Management System**

**ISMS Scope Document**

|  |  |
| --- | --- |
| **Information Classification** | Internal |
| **Distribution** | Internal Distribution |
| **Access** | Internal Use Only |

**Contents**

[**Document Control Information 3**](#_heading=h.30j0zll)

[**Revision Chart 3**](#_heading=h.1fob9te)

[**1.**](#_heading=h.2et92p0) **Introduction 4**

[**2.**](#_heading=h.1t3h5sf) **External and Internal Issues 4**

[**3.**](#_heading=h.17dp8vu) **Requirements of interested parties 4**

[**4.**](#_heading=h.26in1rg) **Business 5**

[**5.**](#_heading=h.35nkun2) **Scope of the ISMS 5**

[**6.**](#_heading=h.2jxsxqh) **Exclusion 7**

[**7.**](#_heading=h.z337ya) **ISMS Scope Statement 7**

[**8.**](#_heading=h.1y810tw) **Note: 8**

# Document Control Information

|  |  |
| --- | --- |
| Document Name | ISMS Scope Document |
| Document Number |  |
| Current Version |  |
| Last Updated |  |
| Document Storage |  |
| First Published |  |
| Document Owner |  |
| Classification |  |
| Approved By |  |
| Review Due Date |  |

# Revision Chart

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Author | Description of Changes |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Introduction

This document defines the scope of the Information Security Management System for the organization.

This document sets out those parts of the organization for which ISMS compliance in line with ISO/IEC 27001:2013 – Information technology — Security techniques — Information Security Management Systems — Requirements is sought to be accomplished.

This document also provides some background information on the characteristics of the business, and its overall aims and objectives with respect to information security, to set the context for the establishment of ISO/IEC 27001:2013 compliant ISMS.

While determining the scope of ISMS, the organization has considered the external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome of the ISMS along with the requirements of interested parties relevant to information security.

# External and Internal Issues

The Major Issues which might affect the intended outcome of Information Security Management System are:

1. Lack of Top Management Commitment
2. Lack of Resources (both personnel and infrastructure)
3. Lack of Security Awareness

# Internal issues

With regard to the <Company Name> business itself, there are a number of relevant internal issues.

These include but not limited to

1. Uncertainties in employee relations
2. Significant organizational changes
3. Location moves
4. Company financial performance
5. Company culture
6. Resources and knowledge of the organization
7. Governance and organizational structure
8. Adopted standards and models
9. Contractual relationships

These general internal issues will be considered in more detail as part of the risk assessment process.

# External issues

With regard to the external environment in which [Organization Name] operates, there are a number of relevant external issues.

1. These include but Not Limited to:
2. Political
3. Government policy changes
4. Government instability
5. Unrest in countries in which the organization operates
6. Trade restrictions and tariffs
7. Economic
8. Prevailing economic climate
9. Interest and inflation rates
10. Supplier failure
11. Lack of customer demand
12. Increasing globalization of supply and/or demand
13. Increasing competition
14. Social
15. Changing demographics
16. Population growth changes
17. Social attitudes
18. Technology
19. Pace of innovation
20. Supporting technologies and infrastructure
21. Automation and artificial intelligence
22. Legal
23. Potential legislative changes
24. Regulatory changes
25. Data protection
26. Environmental
27. Climate change
28. Fire, flood, earthquake etc.
29. Pollution]

These general external issues will be considered in more detail as part of the risk assessment process.

# Requirements of interested parties

The requirements of the interested parties listed in the above section relevant to information security are to:

1. Meet the Legal, Regulatory and Contractual Obligations/Requirements of The organization.
2. Ensure Continual Improvement of Information Security Management System.
3. Maintain Confidentiality, Integrity and Availability of the Information and Information Processing Facilities at The organization.

The following are defined as interested parties that are relevant to the ISMS:

1. **•** Shareholders
2. • Board of Directors
3. • Suppliers
4. • Customers
5. • Regulatory bodies
6. • Customer user groups
7. • Employees of the organization
8. • Contractors providing services to the organization
9. • National or local government organizations
10. • Emergency services
11. • Trade associations and industry bodies
12. • Trade unions
13. • General public
14. • Investors
15. • Distributors
16. • Competitors
17. • Media
18. • Neighbours
19. • Dependents of employees

Applicable legal and regulatory requirements arise from the following:

1. Data Protection Regulation
2. Financial Services legislation
3. Consumer protection legislation

# Business

<Company Name> is a technology consulting and services company with nearly a decade of expertise in various focus areas: Storage, Cloud Computing, Virtualization, Software Development, DevOps, Enterprise Apps, Embedded Systems, Testing, and Test Automation.

<Company Name> help customers achieve their business goals of increased productivity, scalability and cost reduction. Our engagement models are designed to take care of customer’s requirements, letting them focus on business critical activities.

# Scope of the ISMS

INFORMATION SECURITY MANAGEMENT SYSTEMS COVERING SOFTWARE DEVELOPMENT PROJECTS, SUPPORTING PROCESS LIKE INFRASTRUCTURE, FINANCE, HUMAN RESOURCES AND ADMINISTRATION

The organization gives paramount importance to the organization’s Information and opts to build Information Security Management System (ISMS) in line with the global ISO/IEC 27001:2013 to demonstrate their commitment in protecting the organization’s Information.

* **The scope of Information Security Management Systems (ISMS) extends to the following departments of <Company Name> , <Location>:**

1. Software development projects
2. Human Resource (HR)
3. Administration (Admin)
4. Finance Department
5. IT Services & Support – Infrastructure; in accordance with the <Company Name>-ISMS- DOC-SOA Statement of Applicability.xlsx

* **Locations under the scope**

Chennai

<Company Name>

<Company Address>

Pune

<Company Name>

<Company Address>

**Pune Scope**

“INFORMATION SECURITY MANAGEMENT SYSTEMS COVERING SOFTWARE DEVELOPMENT PROJECTS, SUPPORTING PROCESS LIKE INFRASTRUCTURE, HUMAN RESOURCES AND ADMINISTRATION”

* **Logical Perimeter**

The information security management system would govern the networks and technologies at above locations.

* **Assets**

Following assets cover under the ISMS Scope;

1. Information Assets (Digital) which covers data files, E-Mails, system documentation, user manuals, training material and operational or support procedures or process document etc
2. Paper documents which covers contracts, SLA, guidelines and company documentation.
3. Software Assets which covers application software, system software, development tools and utilities. Such as .net framework, SQL, Trend Micro etc
4. Entire network and Hardware Assets such Core Routers, Switches, PC’s etc
5. Media Assets such as Tape Drives, CDs
6. Supporting Utility Assets such as HVAC, Access Control System
7. People (Employees, Temp Staff and Contract Personnel)
8. Company’s Reputation (Brand Value)

# Exclusion

* **Department / Team wise Exclusion :-** All other departments excluding Scope List
* **Location wise Exclusion :-** Bangalore
* **Control wise Exclusion**

A.14.2.7 Outsourced development

# ISMS Scope Statement

“INFORMATION SECURITY MANAGEMENT SYSTEM COVERING SOFTWARE DEVELOPMENT PROJECTS SUPPORTING PROCESS LIKE IT INFRASTRUCTURE, FINANCE, HUMAN RESOURCES AND ADMINISTRATION DEPARTMENTS”.

# Note:

The scope statement has been defined, so as to provide maximum flexibility after adapting. The scope will be reviewed and appropriate changes will be incorporate based on the Business needs.

**End of Document**