Contents

[1. Purpose 5](#_Toc78901736)

[2. Scope 5](#_Toc78901737)

[3. Responsibilities 5](#_Toc78901738)

[4. ISMS Policy 6](#_Toc78901739)

[**4.1 Information security requirements** 6](#_Toc78901740)

[**4.2 Approach to managing risk** 6](#_Toc78901741)

[**4.3 Human resources** 7](#_Toc78901742)

[**4.4 Improvement of ISMS** 7](#_Toc78901743)

[5. General Policies 7](#_Toc78901744)

[6. Review and Evaluation of Policy 8](#_Toc78901745)

[7. Confidentiality Agreement 8](#_Toc78901746)

**DOCUMENT REVISION CONTROL**

REVISION HISTORY

| **Date** | **Author** | **Version** | **From** | **To** | **Description** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

REVIEWERS

| **Name** | **Position** | **Date** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

DISTRIBUTION

| **Date** | **Distributed to** | **Version** | **Distribution Format** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

APPROVALS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Version** | **Approved by** | **Designation** | **Signature** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**LIST OF ABBREVIATIONS**

|  |  |  |
| --- | --- | --- |
| **Index** | **Abbreviation** | **Stands For** |
| I | IT | Information Technology |
| 2 | SLA | Service Level Agreement |
| 3 | IOT | Internet of things |
| 4 | IAS | International Accounting Standards |
| 5 | FDP | Finance Department |
| 6 | ITSM | Information Technology Service Management |
| 7 | NDA | Non-Disclosure Agreement |

Risk assessment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Asset** | **Risk plan** | **Approver** | **Risk summary** | **Risk value** | **Department** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Communication

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Subject** | **Date** | **Whom to communicate** | **Who shall communicate** | **Risk involved** | **Mode of communication** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. **Purpose**

This ISMS Policy document is aimed to define the security requirements for the proper and secure use of the Information Technology services in the Organization. Its goal is to protect the Organization and users to the maximum extent possible against security threats that could jeopardize their integrity, privacy, reputation, and business outcomes

1. **Scope**

This document applies to all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services. Compliance with policies in this document is mandatory.

1. **Responsibilities**

|  |  |
| --- | --- |
| **Roles** | **Responsibilities** |
| [Chief Information Security Officer] | * Accountable for all aspects of the Organization’s information security. |
| Information Security Officer | * Responsible for the security of the IT infrastructure. * Plan against security threats, vulnerabilities, and risks. * Implement and maintain Security Policy documents. * Ensure security training programs. * Ensure IT infrastructure supports Security Policies. * Respond to information security incidents. * Help in disaster recovery plans. |
| Information Owners | * Help with the security requirements for their specific area. * Determine the privileges and access rights to the resources within their areas. |
| IT Security Team | * Implements and operates IT security. * Implements the privileges and access rights to the resources. * Supports Security Policies. |
| Users | * Meet Security Policies. * Report any attempted security breaches. |

1. **ISMS Policy**

The purpose of the Policy is to protect the organization’s information assets from all threats, whether internal or external, deliberate, or accidental.

It is the Policy of the organization to ensure that:

* Information should be made available with minimal disruption to staff and the public as required by the business process,
* The integrity of this information will be maintained
* Confidentiality of information not limited to research, third parties, personal and electronic communications data will be assured
* Regulatory and legislative requirements will be met
* Information security education, awareness and training shall be made available to staffs,
* All breaches of information security, actual or suspected, shall be reported to, and investigated by the relevant authorities not limited to System Administration and Incident Response
* Appropriate access control will be maintained, and information is protected against unauthorized access.

Policies, Procedures and Guidelines for <Company Name> will be made available in both hardcopy and online format through intranet system to support the ISMS Policy.

## **4.1 Information security requirements**

A clear definition of requirements for information security will be agreed and maintained with the internal business and cloud service customers so that all ISMS activity is focused on the fulfillment of those requirements. Statutory, regulatory, and contractual agreements will also be documented and input to the planning process. Specific requirements about the security of new or changed systems or services will be captured as part of the design of each project.

It is a fundamental principle of the <Company Name> ISMS that controls implemented are driven by business needs and this will be regularly communicated to all staff through team meetings and briefing documents.

## **4.2 Approach to managing risk**

Risk management will take place at several levels within ISMS including:

* Management planning- risks to the achievement of information security objectives will be assessed and reviewed on regular basis.
* Information security and IT service continuity risk assessments
* Assessment of the risk of changes via the change management process
* As part of major projects to achieve business change e.g. new computer systems and services
* High level risk assessments will be reviewed on an annual basis or upon significant change to the business or service position.

## **4.3 Human resources**

<Company name> will ensure that all staff involved in information security are competent based on appropriate education, training, skills and experience. The skills required will be determined and reviewed on regular basis together with an assessment of existing skill levels within <Company name>. Training needs will be identified, and a plan maintained to ensure that the necessary competencies are in place. Training, education, and other relevant records will be kept by the HR department to document individual skill levels attained.

## **4.4 Improvement of ISMS**

<Company name> policy about continual improvement is to:

* Increase the level of proactivity (and stakeholder perception of proactivity) about information security.
* Make information security processes and controls more measurable to provide a sound basis for informed decisions.
* Review relevant metrics on annual basis to assess whether it is appropriate to change them based on historical data.
* Obtain ideas for regular improvement via regular meetings and other forms of communication with interested parties.

The following criteria must be used in assessment of improvement proposals:

* Cost
* Business benefit
* Risk
* Implementation timescale
* Resource requirement

# General Policies

1. Exceptions to the policies defined in any part of this document may only be authorized by the Information Security Head or his designated Officer. In those cases, specific procedures may be put in place to handle request and authorization for exceptions.
2. Every time a policy exception is invoked, an entry must be entered into a security log specifying the date and time, description, reason for the exception and how the risk was managed.
3. All the IT services should be used in compliance with the technical and security requirements defined in the design of the services.
4. Infractions of the policies may lead to disciplinary actions. In some serious cases they could even led to prosecution.

# Review and Evaluation of Policy

Audits and reviews of policy shall be conducted bi-annually, and necessary improvisations will be made. Independent review of security systems shall be performed.

# Confidentiality Agreement

This document is copyrighted, and all rights are reserved. This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent, in writing, from an authorized representative of **<Company Name>**. This document is for internal use only and may, in whole or in part be provided to anyone outside of company including customer, clients, or prospects after taking an approval from an authorized representative of **<Company Name>**.