COMPANY LOGO HERE

**{companyName}**

**Information Security Policy**

**Version {version}**

This document contains internal information of {**companyName}** No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of {**companyName}**. The information contained herein is internal to of {**companyName}** and shall not be distributed to any persons other than those involved in the development, assessment and delivery of services. {**companyName}** reserves the right to revise and update this document as and when required

**Document Management Information:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Version No.** | **Date** | **Prepared By** | **Reviewed/ Updated By** | **Reviewer Signature** | **Approved By** | **Approver Signature** | **Description of Change** |
| {version} | {issueDate} | {preparedBy} | {reviewerName} | Reviewer Sign | {approverName} | Approver Sign | Initial Release |

Contents

[1 Introduction 4](#_Toc83915709)

[2 Objective 4](#_Toc83915710)

[3 Scope 5](#_Toc83915711)

[4 Responsibility 5](#_Toc83915712)

[5 Information security principles 6](#_Toc83915713)

[6 Information Classification 7](#_Toc83915714)

[7 {companyName} Information Security Organizational Structure 8](#_Toc83915715)

[8 Incident Handling 9](#_Toc83915716)

[9 Exceptions 9](#_Toc83915717)

[10 Policy Violations 10](#_Toc83915718)

[11 Policy Review 10](#_Toc83915719)

[12 References and related documents 11](#_Toc83915720)

# Introduction

Information and supporting processes, systems and networks are important business assets. These information assets are stored on a number of computing devices, hard copies and networks and made available to business partners, clients, employees and suppliers.

Securing these assets is essential to run the business. Defining, achieving, maintaining, and improving information security are essential to maintain competitive edge, cash flow, profitability, legal compliance and commercial image.

The Information Security Policy defines the process/approach of {companyName} towards establishing and implementing information security measures, adopting the industry best practices/regulations such as the ISO 27001 security standard and other relevant privacy laws/regulations.

# Objective

We understand the dynamic nature of our business; in response we are committed to continually improving our processes to uphold information security. The overall objective of {companyName} is to ensure protection of its information systems against unauthorized disclosures, unauthorized changes, and damage or destruction. The specific information security objectives of {companyName} are:

* To identify all information assets that directly or indirectly impact {companyName} operations, to understand their vulnerabilities and the threats that may expose them to risk through appropriate risk assessment.
* To manage the identified risks to an acceptable level through the design, implementation, and maintenance of Information Security .
* To comply with applicable laws, regulations and contractual obligations pertaining to information security and data privacy, for its client data and internal data directly or indirectly impacting the client data.
* To raise awareness of information security in {companyName}.
* To implement mechanisms to ensure that all breaches and suspected weaknesses of information security are reported and investigated, to be followed by adequate remedial action.
* To maintain and continually improve the established Information Security Management.

# Scope

This policyis applicable to all the information assets and location of {companyName}. An information asset is a piece of information, stored and/or processed in any form, which is recognized as having value to the business.

Examples of information assets are software, physical assets, intangible assets, services, people, or information assets that are physically or electronically stored, processed and/or transmitted by any of these assets.

This policy is applicable to all employees and third parties’ staff of {companyName}. The term ‘third-party staff’ includes all the employees, agents, consultants, and representatives of all third parties who are, in any way, accessing, processing, storing, transmitting, modifying, or disposing any of {companyName}’s information assets.

# Responsibility

Following are the responsibilities of roles involved in the implementation of Information security policy and/or those responsible for overseeing the implementation of this process.

* **{approverDesignation}**: He is responsible for approving the Information Security Policy.
* **{reviewerDesignation}**: He is responsible for reviewing the policies and the sub policies and related procedures including any subsequent modifications to the same.
* **{designationOfSecurityHead}:** He is responsible for preparing the sub policies and related procedures including any subsequent modifications to the same
* **{SecurityComplianceCommittee}**: The Committee is responsible for ensuring that policies are implemented and are current and reflect the requirements of {companyName}.
* **All Employees**: It is the responsibility of all employees and third-party staff to read, understand and abide by this policy and its principles.

# Information security principles

The following information security principles provide overarching governance for the security and management of information at {companyName}.

* **Know your information – classify it**: Information should be classified according to an appropriate level of confidentiality, integrity, and availability.
* **Handle information appropriately**: Employees with particular responsibilities for information must ensure the classification of that information; must handle that information in accordance with its classification level; and must abide by any contractual requirements, policies, procedures or systems for meeting those responsibilities.
* **Be aware of the regulations and {companyName}’s commitments**: {companyName} should comply with relevant legislative, regulatory, and contractual requirements of security and privacy defined by its geographical footprints as well as its customer’s footprints.
* **Promise the availability of information for authorized use:** Information should be both secure and available to those with a legitimate need for access.
* **Protect the confidentiality of information:** The access to information should be provided on a need-to-know basis and periodically assessed for its relevance.
* **Preserve the integrity of information:** Information should be accurate, consistent, and complete throughout its life cycle.
* **Identify vulnerabilities and plan ahead:** Understand vulnerabilities and the threats that may expose them to risk through appropriate risk assessment and managed to an acceptable level through risk mitigation plan.
* **Be proud to disclose incidents:** All employees encouraged to report information security incidents and privacy breaches including breaches to this policy.
* **Security depends on us:** Security is everyone’s responsibility and even seemingly harmless behavior, or small mistakes can have big consequences in today’s dynamic environment. Security awareness is a continuous exercise and should include all stakeholders.
* **Review, Review, Review:** Information security provisions and the policies that guide it will be regularly reviewed using self-reviews, annual internal audits and third-party audits.
* **There is nothing better than best practices:** Best practiceslike ISO27001, NIST cybersecurity framework help us to continually improve our security and privacy posture.
* **Balance functionality and assurance**: Strive to achieve balance between security, and functionality and make security and privacy an enabler for the business.

# Information Classification

The following table provides a summary of the information classification levels that have been adopted by {companyName} and which underpin the 12 principles of information security defined in this policy.

|  |  |
| --- | --- |
| **Security Level** | **Definition** |
| 1. Confidential | Most sensitive business information intended for use only within {companyName}. Its unauthorized disclosure could cause serious impact and/or adversely affect {companyName}, its employees, Third parties, business partners and/or the brand.  Confidential Information includes but is not limited to purpose-related technical, financial, and marketing information; software, including program specifications and source code; inventions, research and development information; financial information, including business plans and Client and prospective Client lists; and, other information which is not generally known either to the public or in the industry pertaining to the respective businesses and technologies of Client and Vendor. |
| 1. Sensitive | Sensitive personally Identifiable information (SPII) or Personally Identifiable Information(PII).Its unauthorized disclosure could cause serious impact and/or adversely affect Trust on {companyName} and can also result in Legal and Compliance Issues. |
| 1. Internal | Information for which unauthorized disclosure, particularly outside the organization, would be inappropriate and inconvenient; however, if this information were to be disclosed to a third party, it could provide a commercial advantage. This is routine business information, which {companyName} simply wishes to keep private. |
| 1. Public | Information approved by {companyName} management for release to the public. This information may be circulated freely and disseminated outside {companyName} without any potential harm after being made public, and hence does not require any special protection. |

# {companyName} Information Security Organizational Structure

The Organizational structure at {companyName} for information security shall consist of following roles. For detailed roles and responsibilities, refer to {companyName}’s Security roles and responsibilities document.

* + {CEO}
  + {CTO}
  + {ITHeadName}
  + {SecurityManagerDesignation}
  + {SecurityComplianceCommittee}
* **Allocation of Information Security Responsibilities**

**{SecurityComplianceCommittee}** shall ensure that the information security responsibilities of employees in their functions are identified, documented, and communicated to them.

* **Authorization Process for Information Processing System**

Access to information processing Systems shall be allowed only after receiving the necessary approvals from authorized personnel of {companyName} and after following defined procedure. No computing/storage devices, such as Server, E-mail , Shared Documentation Tools, Collaboration Tolls etc,shall be physically or logically connected to the network or to any information system of {companyName} prior to authorization.

* **Contact with Authorities**

Contacts with law enforcement authorities, fire department, emergency services and service providers shall be maintained by the {ContactAuthorities}. The contact details of these agencies should be maintained and displayed at appropriate places that are accessible to users.

* **Confidentiality Agreements**

Requirements for confidentiality or non-disclosure agreements reflecting the Organization’s need for protection of information shall be identified and regularly reviewed and will be signed off with the Employees and the Third Parties ( Supplier, Supplier Employee ).

# Incident Handling

If any employee is aware of any information security and data privacy incident, then they must report it to {incidentHandlingMail}.

Incidents will be handled, documented and reported as per process for reporting and handling of security and privacy breach and incidents.

# Exceptions

This policy is intended to be a statement of information security and data privacy requirements that need to be met at {companyName}. However, exceptions against individual controls in specific policy domains shall be formally documented, which will include, at minimum, the following:

* Justification for the exception.
* Risk due to the exception.
* The mitigation controls to manage the risk.
* The validity period of the exception; and
* Details of assets on which the exception is applicable.

The exception request, validation and management shall be done, and exceptions must be reviewed and approved by {SecurityComplianceCommittee}.

# Policy Violations

* All employees and third parties are required to comply with the information security policies.
* Non-compliance with the information security policies is grounds for disciplinary action. Disciplinary procedures as per the Disciplinary Policy shall be invoked to deal with such non-compliances.

# Policy Review

This policy (including all sub-policies and procedures) shall be reviewed at the time of any major change(s) in the existing business environment affecting policies and procedures or at least every year, whichever is earlier. This document shall be reviewed by the {reviewerDesignation} and approved by the {approverDesignation}. The reviews shall be carried out for assessing the following:

* Impact on the risk profile due to, but not limited to, the changes in information assets, people, deployed technology/ architecture, vendors, and strategic partners, regulatory and/ or legal and/ or contractual requirements; and
* The effectiveness of the policies.

As a result of the reviews, additional policies may be issued and/ or existing policies may be updated, as required. These additions and modifications will be incorporated into the policies. Policies that are identified as redundant shall be withdrawn.

# References and related documents

* ISO 27001:2013
* ISO 27002:2013
* GDPR
* CCPA

Supporting policies have been developed to strengthen and reinforce this policy statement. These policies further mandate the implementation of information security controls and are typically structured to address the specific processes and procedures of the ISMS. Following are the supporting information security policies:

* Access Control Policy
* Physical and Environmental Security Policy
* Asset Management Policy
* Acceptable Usage Policy
* Clear Desk and Clear Screen Policy
* Mobile Devices and Teleworking Policy
* Backup and Restoration Policy
* Cryptographic Controls Policy
* Communications Security Policy
* Operational Security Policy
* Network Security Policy
* Capacity Management Policy
* Change Management Policy
* Information Systems Acquisition, Development & Maintenance Policy
* Secure Systems Engineering Policy
* Security Incident Management Policy
* Password Management Policy
* Patch Management Policy
* Employee Disciplinary Policy
* Human Resources Security Policy
* Risk Management Policy
* Data Protection Policy
* Removable Media Policy
* Ant-Virus Policy
* Business Continuity Policy
* Configuration Management Policy
* Firewall Policy
* Logging and Monitoring Policy
* Vulnerability Management Policy
* Wireless Security Policy
* Privacy Policy
* Internal Audit Policy
* Third Party Relationship Management Policy

All employees and any third parties authorized to access {companyName}’s network or computing facilities are required to familiarize themselves with these supporting documents and to adhere to them in the working environment. These policies are published together on the company's share drive or on a need-to-know basis.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*End of Document\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*