



VEDANTA INFORMATION SECURITY POLICY



TABLE OF CONTENTS


1.	VEDANTA SECURITY VISION.....	4
2.	VEDANTA SECURITY MISSION	4
3.	INFORMATION SECURITY POLICY APPLICABILITY	4
4.	OBJECTIVES OF INFORMATION SECURITY POLICY.....	4
5.	ORGANIZATION OF INFORMATION SECURITY.....	5
6.	POLICY FRAMEWORK.....	5
7.	POLICY DEVIATIONS	5
8.	POLICY REVIEW	5



DOCUMENT CONTROL

DOCUMENT NAME: Vedanta Information Security Policy

AUTHORIZATION:

Prepared By	Reviewed By	Approved By
Vriti Aggarwal, Anoushka Sharma	Sandeep Gupta, Neha Taneja, Ramadevi Sangu, Rahul Rathore, Violet Jemimah, Thanga Vijaya, Amitava Chakraborty, Nidhi Garg, Jitendra Kumar Patra, Dileep K Singh, Parveen Dhingra, Mahesh Toshniwal, Dr. Sujit Senapati, Garima Singh, Subrata Banerjee, Shobha Raikar, Roy Suvendu, Vikas Ingle, G Priyanka, Kritideep Kaur	Chetan Trivedi 
Signature: Electronically submitted	Signature: Electronically reviewed	Signature: Electronically Approved
Date: 25 th April, 2022	Date: 26-05-2022	Date: 13/06/2022

SECURITY CLASSIFICATION: Internal (C3)

VERSION HISTORY

S.No	Version	Issue Date	Effective Date	Description
1	1.0			
2	2.0	22 nd July 2016	22 nd August 2016	Change in section 1.4 policy framework was conducted. Added a section 1.7 Organization of Information Security Above changes were conducted to map the requirements as defined in ISO27001 2013 edition.
3	3.0	16 th Oct 2019	16 th Oct 2019	<ul style="list-style-type: none"> • Removed Introduction Section • Minor changes in section 1.3 • Objectives of Information Security Updated • Policy Framework section updated • Policy Review section updated • Information Security Roles & Responsibilities removed • Remove Contact with Authorities section • Remove Contact with Special Interest Groups
4	3.1	23 rd Sep 2020	13 th Oct 2020	<ul style="list-style-type: none"> • Removed first line from section 2. • Removed HR information from section 3 and added paper information digital assets. • Section 6 – minor typo error corrected.
5	3.2	3 rd Jun 2021	3 rd Jun 2021	<ul style="list-style-type: none"> • Updation of Reviewer's list
6	3.3	26 th May 2022	13 th Jun 2022	<ul style="list-style-type: none"> • Reviewer List Updated • Minor Language Changes • Added All Virtual Assets/ Machines in Section 3

1. Vedanta Security Vision

To secure Vedanta Limited and its Indian Subsidiaries and Fujairah Gold and Vedanta Zinc International (henceforth referred to as Vedanta Group) information assets to support and sustain our business vision of being a premium global conglomerate.

2. Vedanta Security Mission

Vedanta Group shall develop, implement, and comply with security procedures and controls at all levels to protect the confidentiality and integrity of information stored and processed on its systems and ensure that information is available to authorized persons when required.

3. Information Security Policy Applicability

The security policies and standards contained in this document have been established to cover information, data, software, hardware, and networks used at all the Vedanta Group locations. The policy extends to companies, entities, and business units (collectively called Entities). In particular, the information security policy applies to the following information assets of Vedanta Group:

- All proprietary information that belongs to Vedanta Group
- All client / customer information
- All supplier, contractor, and other third-party information
- All software assets such as application software, system software, development tools and utilities
- All physical assets such as computer equipment, communication equipment, paper documents, media and equipment relating to facilities maintenance
- Digital/Virtual assets in the form of soft copies such as SLA's, SOW's, License documents, SOP's, Audit reports etc.,
- All Virtual Assets/ Machines

This security policy applies to any person (such as employees, third party contractors and other personnel) who access Vedanta Group's information systems. This security policy shall be communicated throughout the organization to users in a form that is relevant, accessible, and understandable to the intended audience.

4. Objectives of Information Security Policy

The group has defined principles for all entities to create specific Information Security Objectives relevant for protection of business data. These principles are:



- To identify the value of information assets and understand the corresponding vulnerabilities and threats that may expose them to risk, which can be done through a periodic risk assessment exercise
- To manage the identified risks to an acceptable level through the design, implementation, and maintenance of a formal Information Security Management System
- To comply with applicable laws and regulations pertaining to information security, be it for its own data or customer data held by Vedanta Group
- To ensure accountability of user actions carried out from Vedanta information systems
- To raise awareness about the security risks associated with information and information systems among its employees
- To implement mechanisms to ensure that all breaches of information security and suspected weaknesses are reported, investigated, and followed by adequate action
- To implement appropriate controls to minimize loss of information, data, and other resources due to fraudulent activities

Entities shall define Information security objectives in alignment to above principles.

5. Organization of Information Security

Entities shall define Information Security roles and responsibilities to provide appropriate governance structure to their Information Security Management System.

6. Policy Framework

The policy will be supported by a comprehensive Information Security Standard that shall cover all the controls required to be adhered to, in order to fulfill the requirements stated in this policy. Respective entities shall maintain up-to-date supporting documents for adherence to this policy and the standard.

7. Policy Deviations

Any deviations from the policies and Standard mentioned herein, either due to conflicts with laws / regulations, pre-existing policies, or implementation issues, shall be documented or the risk associated must be accepted by the IT Head / Business Head. A log of deviations with a rationale to be maintained at the entity level and should be available for review at all times.

8. Policy Review

This policy shall be reviewed and approved by management annually or whenever there are major changes (if applicable) in the organization.

Records of the management review and approval(s) shall be maintained.

