Data Governance Framework

Document Information

Document Name	Data Governance Framework
Status	Approved
Version	1.4
Classification	Internal (C3)
Last Review Date	13th June 2022
Last Approved Date	13th June 2022
Changes Introduced	• Reviewer List Updated • Reference added
Prepared by	Rahul Rathore
Reviewed by	All BU CISOs
Approved by	Chetan Trivedi

REVISION HISTORY

Version No	Prepared by	Reviewed by	Approved by	Release date
1.0	Aditya Gautam	Gomeet Pant, Sarah Deori, Shobha Raikar, Parveen Dhingra, Chetan Trivedi, Neha Kini, Avijit Deb, Subrata Banerjee, Rahul Rathore, Gourav Fatehpuria, Vardhman Baishakhiya, S Pravin Kumar, Amitava Chakraborty, Mukut Banerjee, Nidhi Garg, Jitendra Kumar Patra, Arunanjan Pattanayak, Dileep K Singh, Mahesh Toshniwal	G.R. Arun Kumar	16th Sep 2019
1.1	Airika Kochhar, Amogh Paranjpe, Nidhi Chandra	Neha Taneja, Sarah Deori, Rahul Rathore, Gomeet Pant, Gourav Fatehpuria, Vardhman Baishakhiya, S Pravin Kumar, Amitava Chakraborty, Mukut Banerjee, Nidhi Garg, Jitendra Kumar Patra, Dileep K Singh, Mahesh Toshniwal, BijayaLaxmi Martha, Ramadevi Sangu Parveen Dhingra, Chetan Trivedi, Avijit Deb, Subrata Banerjee, Shobha Raikar, Subrata Banerjee, Roy Suvendu, Srinivasrao S, Dr. Sujit Senapati, Garima Singh	Anand Laxshmivarahan R	13th Oct 2020
1.2	Vriti Aggarwal, Anoushka Sharma	Indradyumna Datta, Neha Taneja, Sarah Deori, Chetan Trivedi, Ramadevi Sangu, Rahul Rathore, Gourav Fatehpuria, Violet Jemimah, Vardhman Baishakhiya, Thanga Vijaya, Amitava Chakraborty, Nidhi Garg, Jitendra Kumar Patra, Dileep K Singh, Parveen Dhingra, Mahesh Toshniwal, Avijit Deb, Dr. Sujit Senapati, Garima Singh, BijayaLaxmi Martha, Subrata Banerjee, Shobha Raikar, Roy Suvendu	Anand Laxshmivarahan R	3rd Jun 2021
1.3	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	13th Jun 2022
1.4	Rahul Rathore	All BU CISOs	Chetan Trivedi	29th Sept 2023

Table of Contents

A. Introduction – Data Governance

As per National Institute of Standards and Technology (NIST), Data Governance is a set of processes that ensures that data assets are formally managed throughout the enterprise. A Data Governance model establishes authority, management and decision-making parameters related to the data produced or managed by the enterprise. To derive benefits of data classification and design controls on data, it is imperative for Vedanta, hereinafter referred as Company, to have a defined and approved framework around all the aspects of data during its lifecycle.

Following are the key elements of a Data Governance framework:

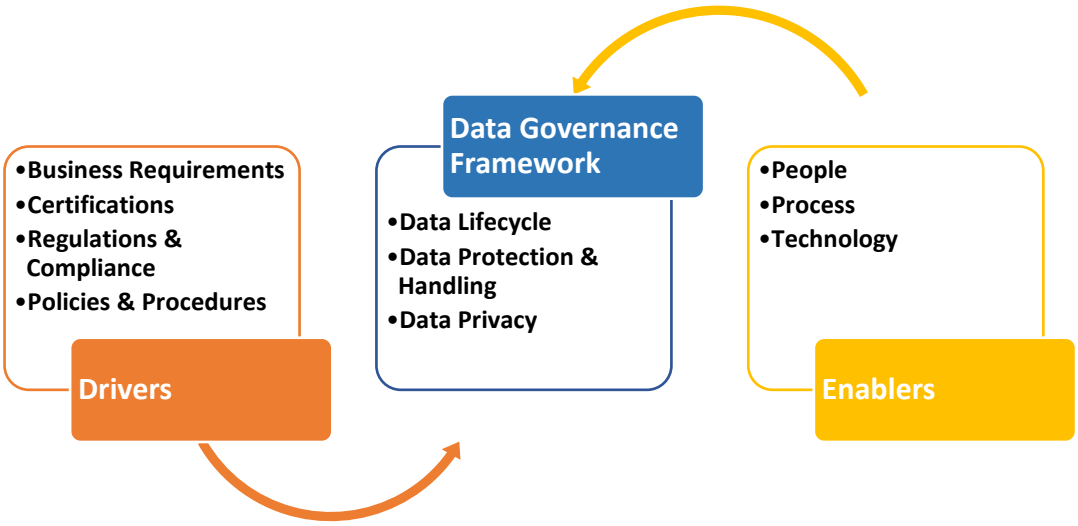

Figure 1: Data Governance Framework

B. Objective

This Data Governance framework intends to provide:

- Guiding principles based on business & regulatory requirements;
- Applicability of framework on Company data handled by people, process and technology;
- Prescribe controls based on sensitivity (classification) throughout data lifecycle;
- Labelling & handling guidelines for all of Company's information assets;
- Management structure with roles and responsibilities;

Data, for the purposes of this document, can be described as recorded information, in any physical or electronic format, whether duplicate or original, that is created, received, and maintained to support the activities and processes of the Company.

This framework is aligned to and should be read in conjunction with any Entity-wide policy / standard on Information Security & Information Management.

NOTE: In case of conflict between this framework and any entity level policy, the policy shall supersede as long as the policy is not in deviation to the Company's policies and/or standards.

C. Scope & Applicability

This framework is applicable to all data (physical as well as electronic) that is created, obtained, stored, transmitted, processed, and disposed in the course of business operations of Company, irrespective of the data location, or the type of device it resides on.

All personnel including employees, trainees, third party contractors, interns, and other personnel who use Company's data / data assets and information provided by third parties, suppliers, customers in the due course of business operations shall adhere to this framework.
For third party provided information, Company's classification procedures shall supersede third party information classification procedures unless specified otherwise in the contract. Any unclassified information will be treated as "Internal" and handled accordingly.

D. Framework

This section provides the details on actual framework and its various components.

1. Guiding principles

Data is one of the most valuable assets available to business and its accuracy depends on how effectively we define the ownership, manage the accountability and safeguard the data asset. The successful governance of data requires participation and accountability across the Company, from data owners through to top level executives. Below are the guiding principles that will enable the Company and its entities to drive a successful data governance implementation:

- Ensuring data protection related compliance including but not limited to applicable regulations (IT Act 2000, SOX, Industry specific regulations etc.), ISO27001, Company policies and standards;
- Identifying business needs for protection of information and the associated classifications;
- Identifying industry best practices and standards;
- Implementing standardized data protection and data handling practices across the Company to ensure ownership, confidentiality, integrity, availability and auditability for appropriate access to datasets throughout its lifecycle;
- Ensuring that the data ownership, management commitment and accountability is established

(Please refer latest version of Vedanta Information Security Standard for more details)

2. Data Classification

Governance and protection of Company's data can be effectively defined and implemented if the data is appropriately classified. Company's data can include personal and/or business critical information and must be adequately protected.
Regulatory requirements, Company reputation, potential impact from exposure/leakage and privacy are key considerations in data classification.

As per Company's Information Security Standard, data can be classified into four categories to indicate the needs, priorities, and expected level of protection when handling the data.
All data must be classified by its owner into one of the following categories:

Data Category	Description	Examples
Secret (C1)	Classified Information that is highly sensitive or business critical information that is available only to a very restricted set of individuals (or specific positions).	Trade secrets, Merger & Acquisition information (till it is publicly released), financial reports (before release), exploration information, etc.
Confidential (C2)	Information that is sensitive within the Company/Business and available only to a specific function, group or role.	Intellectual Property, Sensitive Personal Information (SPI), financial data, Operational and production information, drilling schedules, Salary structure, etc.
Internal (C3)	Information that is not necessarily sensitive in nature but should be accessible only to employees and contracted third parties. There is usually no need for such document to be available in public domain.	Policies, procedures, templates, frameworks, organizational announcements, etc.
Public (C4)	Information that is intended for public use. There is no negative impact or implication if disclosed or lost.	Banner, website content, annual reports, post, etc.

NOTE:

1. Secret (C1), Confidential (C2) and Internal (C3) data types must be shared with third-parties only after a Non-Disclosure agreement (NDA) is in place.
2. Secret (C1) and Confidential (C2) information should be shared strictly on a "Need-to-know" basis. In case of any additional access grant to Secret (C1) and Confidential (C2) information, business justification/rationale should be available.
3.
    a. As a group, we mandate the use of classification labels. Default classification should not be enabled for use by employees/contractors/other personnel. Each Entity should use this as a guidance for their individual classification implementation projects, using AIP as a technology. The AIP labels in use should be consistent across the group. Labels to be used are Secret (C1)
    b. Confidential (C2)
    c. Confidential (C2)/ Label Only
    d. Confidential (C2)/ Full protection
    e. Internal (C3)
    f. Internal (C3)/All employees
    g. Internal (C3)/ All employees and Partners
    h. Public (C4)

2.1 Secret (C1)

- Secret Data is Company's highly sensitive and business critical information. Access to secret information is restricted to a very limited set of people who have a legitimate purpose for accessing such information.
- Copying and forwarding is permitted with only those who need the data to perform the assigned tasks, with approval of the Data Owner.

- This data must be protected in its hard copy form as well as its soft copy form through the data handling techniques/processes mentioned in the Information Security Standard/Policy and Information.
- Secret information type can also be interchangeably called **'Restricted'**.
- Example: Acquisition and divestiture plans, top secret formulas and plans, etc.

2.2 Confidential (C2)

- Information that is sensitive within the Company/Business and available only to a specific function, group or role. Access to this information is restricted to limited audience on a 'Need-to-know' basis.
- Copying and forwarding is prohibited, unless approved by the Data Owner.
- This data should be protected in its hard copy form as well as its soft copy form through the data handling techniques/processes mentioned in the Information Security Standard/Policy and Information.
- Example: Financial data, Vendor Contracts, Performance Reports of HR, Company Employees' Personally Identifiable Information & sensitive personal information such as PAN card, License Number, etc., passwords, IP addresses, process flow diagrams of Plant Teams, Project Tracker Reports of Business Excellence, Price of procurement by Commercial Department.

2.3 Internal (C3)

- Information that is not necessarily sensitive in nature but should be accessible only to employees and contracted third-parties. There is usually no need for such document to be available in public domain.
- Copying and forwarding to external parties is permitted with approval from Data Owner.
- This data can be internally available in its hard copy form or its soft copy form inside the Company's premises and devices or with third-parties as per agreement.
- Example: Employee information (general email address, phone number) from Internal Directory, Company policies, Training material, internally published Notices and Newsletters, etc.

2.4 Public (C4)

- Information that is intended for public use. There is no negative impact or implications if disclosed or lost.
- Public information type can also be interchangeably called **'External' or 'Unrestricted'**.
- Data that is freely available and can be made public either through direct distribution or accessible through different media channels, and whose breach has no significant impact on the Company or employees; should be categorized as Public.
- Example: Brochures, press releases, awards and recognitions and certifications.

NOTE:

Entire record/data/document is classified according to the highest classification of data contained in the record.

– For example: If a document contains Public, Secret and Confidential data, entire data will be classified as Secret (C1) and handled accordingly.
– If data is entered into a spreadsheet, and it contains secret, confidential and internal data, then the spreadsheet must be classified and treated as Secret (C1). Procedures to be followed as per the classification and must be documented for every department.

3. Guidelines for Data Labelling

Data classification is a vital part of securing Company's information, as location of confidential and sensitive data and the level of accesses maintained for this data is essential. Data Classification is the process of identifying and assigning pre-determined levels (labels) of sensitivity to different types of data/information. If employees do not appropriately classify and label the data, then it will be difficult to safeguard Company's data. Below provided are the data labels to be used for the different categories of data classified.

Classification	Data Labelling
Secret	Secret (C1)
Confidential	Confidential (C2)
Internal	Internal (C3)
Public	Public (C4)

(Please refer latest version of Vedanta Information Security Standard for more details)

4. Data Protection & Handling Guidelines

Different laws are taking effect across the globe to regulate the collection, use, storage, retention, disclosure and disposal of personal information. At the same time, the rate of cyber-attacks, data breaches and unauthorized use of personal data is growing exponentially. In the current environment, it is important to define handling guidelines for all data types e.g. government data, financial data, and other Personally Identifiable Information (PII), to understand the rights and obligations of individuals and Company.

Key points

- Secret, Confidential & Internal data should not be disclosed outside the Company without approval from Data Owner.
- Access to Confidential data shall be limited to need-to-know basis for data in-use, in-transit or at-rest.
- Secret & Confidential data in-transit should be encrypted.

(Please refer latest version of Vedanta Information Security Standard for more details)

Additionally, leakage of sensitive information needs to be protected by use of technology rather than only relying on personal judgment. Entities must make use of Data leakage prevention solutions to implement the same.

5. Data Governance Management Structure

Data governance involves decision-making, management, and accountability related to data in a Company. A data governance team is built to ensure proper handling of data. Data governance is dependent on people being informed of their roles and responsibilities. One can have multiple roles for different datatype. This section defines roles and responsibilities of various parties involved in Data governance lifecycle.

5.1 IT Steering Committee

IT steering committee, functional within each entity, should govern the data governance programme at entity level and provide direction for bringing solutions and processes required to maintain compliance to this framework as well as Vedanta Information Security Standard.

5.2 Data Governance Working Group

Entity level Data Governance Working Groups are responsible to drive any initiative from data governance perspective. This group is also responsible for maintaining and updating policies based on the direction from IT Steering Committee before enforcement. This group should ensure that any initiatives taken up are in alignment to Vedanta Information Security Standard. Note that the entities may not have named individuals/groups notified for this role at all times however at any given time, they should be able to associate individual or personnel taking care of this.

5.3 Data Owner

Data owner is the most important role in the data governance framework. Data owner is an individual who is accountable for protection of data in their ownership and is responsible for ensuring data classification is applied to the specific data. Secondary responsibilities include defining business rules and protection procedures for respective data set, in alignment with overall data governance framework for data types that cannot be handled with the prevailing procedures.
The term 'owner' does not necessarily mean that the person has intellectual property rights to the data. The term simply implies that the Data Owner is responsible and accountable for data.
Typically, HODs, SBU presidents and functional leaders are considered data owners for their verticals.

Key Roles and responsibilities:

- Ensure data is classified correctly by data producers and reclassify the information based on the sensitivity as and when required
- Responsible for reviewing the classification, reclassification and relabeling of data as its sensitivity changes over time during data lifecycle
- Classify data based on the business requirements, legal / regulatory requirements and the impact associated with unauthorized disclosure, modification or loss, thereby ensuring Confidentiality, Integrity and Availability (CIA) of data
- Determine controls (handling procedure applicable, retention period and disposal techniques) to protect the data based on data classification not covered within prevailing standards and procedures
- Adhere to controls towards protection and access to data, provide guidelines for access provisioning and revocation
- As and when required, perform review of process being followed for data protection, quality and consistency on a defined periodic basis
- Delegate the responsibility for implementing the controls to the Data Custodian (accountability primarily rests with the Data Owners)

5.4 Data Producer

Data producers are the initiators / authors of data. Besides being an individual or multiple individual, data producer can be a user interface, automation service or device that collects data relevant to Company business. In some cases, multiple systems and processes may also produce data for the Company. It is then the responsibility of interface handler and the personnel generating report through the tool to act as a data producer. Data producer could be an employee or third-party person. It is the responsibility of employee, vendor, partner and/or any service provider acting as a data producer to adhere to the data governance framework.

Key roles and responsibilities:

- Perform classification of information based on the content
- Perform due diligence while creation of data to ensure correctness, completeness and validity of entered data
- Enter data into Company's system through authorized means and software
- Adhere to Company's security policy, standard, procedures and guidelines
- Provide timely feedback to Data Custodians to highlight challenges, bugs or weakness in data process wherever applicable
- Report to Data Owner/s in case of any wrong classification

5.5 Data Consumer

Data consumers use data to fulfil the assigned role in the due course of business operations. Their primary responsibility is to adhere to the requirements specified in the Vedanta Information Security Standard and handling of information based on information classification. Data consumers are also authorized to change the classification of information, however, in case of any upgrading / downgrading the sensitivity of document, Data Owners consent should be taken.

Key roles and responsibilities:

- Be held responsible for security of the data handled by them
- Exercise due care while accessing sensitive information (Secret or Confidential Data) and securing them from unauthorized use, disclosure, alteration or destruction
- Comply with the protection requirements defined in the Vedanta Information Security Standard

5.6 Data Custodian

Data Custodians are responsible for the safe custody, including transport, storage of the data and implementation of appropriate business rules. It is the responsibility of each data owner to align a data custodian for all data items in their ownership.

Key roles and responsibilities:

- Understand and comply with Vedanta Information Security Standard
- Ensure data security, integrity, accuracy and consistency across various platforms as prescribed by data owner
- Highlight significant issues to Data Owner and Data Governance Working Group

5.7 Data Custodian – IT

Data Custodian – IT are the system providers for Data Owners where data can reside in adherence to the data security requirements provided in the Vedanta Information Security Standard.

Key roles and responsibilities:

- Ensure data is created, stored and controlled in authorized systems and is in alignment with Vedanta Information Security Standard
- Maintain data security and audit trail, where required, across the applications in use by departments
- For the reported / noted incidents; perform root cause analysis, discuss the exceptions with Data Owners and drive the closure of action plans
- Ensure availability, accuracy and consistency of data
- Partner with Data Custodians and Owners for any data issues

- Maintain secure storage of data, based on classification
- Design and maintain infrastructure to create, process, store, utilize and distribute data in a secured manner

NOTE: All roles mentioned above are not mandatory for all kind of data and in all kind of scenarios.

Glossary

Term	Definition
Company	Vedanta Limited and its Indian Subsidiaries and Fujairah Gold and Vedanta Zinc International (henceforth referred to as Vedanta Group)
Data Minimization	This refers to the practice of limiting the collection of personal information to that which is directly relevant and necessary to accomplish a specified purpose
Entity	All the subsidiaries and business units of Vedanta Group.
SOX	Sarbanes-Oxley Act
NIST	National Institute of Standards and Technology, promotes and maintains measurement standards
IT Act 2000	Information Technology Act 2000 is the primary law in India dealing with cybercrime and electronic commerce
ISO	International Organization for Standardization

References

1. Information Technology Act, 2000
2. Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, 2011
3. Section 43A & IT rules of Information Technology Act of India.
4. Supreme Court of India's verdict on Right to Privacy as a Fundamental Right, 28th August 2017.
5. European General Data Protection Regulation (GDPR).
6. OECD (Organization for Economic Co-Operation and Development) Privacy Guidelines
7. US Privacy Act 1974
8. Australian Privacy Act 1988
9. Aadhaar Act, 2016
10. SEBI (LODR) Regulations, 2015
11. Securities Contract (Regulation) Rules, 1957
12. Indian Companies Act, 2013
13. Vedanta Information Security Policy
14. Cert-IN directions (No. 20(3)/2022-CERT-In)
15. Digital Personal Data Protection Act 2023