Information Classification & Handling Policy

Jan 05 2020

Document Title:	Information Classification and Handling Policy
Author(s)	Rajesh Kumar Singh, Rushi Luhar
Version Number:	V1.0
Document Status:	Approved
Date Approved:	Jan 05 2020
Approved By:	Executive Board
Effective Date:	Jan 10 2020
Date of Next Review:	Jan 05 2021

1 Policy Statement

To meet the enterprise business objectives and ensure continuity of its operations, SENTISUM shall adopt and follow well-defined and time-tested plans and procedures, to ensure that sensitive information is classified correctly and handled as per organizational policies. Information is considered as primary asset of an organization. An organization uses different types of information assets. The sensitivity of these information assets may vary and similarly, their handling mechanisms are also different.

3 Purpose

The Policy aims to ensure that information is handled according to the risk or impact to ensure the confidentiality, integrity and availability of data. The purpose of this policy is to ensure the appropriate handling of all formats of information by establishing a company-wide system of categorising information in relation to its sensitivity and confidentiality, and to define rules for the handling of each category of information in order to ensure the appropriate level of security of that information.

4 Scope

4.1 Employees

This policy applies to all managers, employees, contractors, and third party employees who have access to IT assets of SENTISUM and may be bound by contractual agreements.

4.2 IT Assets

This policy applies to all information assets of SENTISUM.

4.3 Documentation

The policy documentation shall consist of Information Classification and Handling Policy and related procedures & guidelines.

4.4 Document Control

The Information Classification and Handling Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

4.5 Records

Records being generated as part of the Information Classification and Handling Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

4.6 Distribution and Maintenance

The Information Classification and Handling Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of this document shall be with the CISO and website administrator.

5 Privacy

The Information Classification and Handling Policy document shall be considered as “confidential” and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

6 Responsibility

The CISO / designated personnel is responsible for proper implementation of the Information Classification and Handling Policy.

7 Policy

SENTISUM categorizes information into four classes: Confidential, Project / Process / Department specific, Internal, and Public.

1. **Confidential** – The information assets which have high confidentiality value belong to this category. Only a limited set of authorized users shall access these information assets. Examples include business strategy, customer data and personnel files.

2. **Project / Process / Department specific** – The information assets that contain data pertaining to the needs of a specific department, project team, or business process, belong to this category. Such information assets shall be accessible to members of the concerned department, project, or business process only.
3. **Internal** – The information assets which can be distributed within all offices of SENTISUM belong to this category. Examples are office orders and internal circulars.
4. **Public** – The information assets which do not have any confidentiality requirement and / or can be disseminated to the general public belong to this category. Examples include annual financial report of SENTISUM and information displayed on SENTISUM's website.

Following are the policies for secure handling of information assets of SENTISUM:

1. Handling and labeling of all media shall be according to its indicated classification level.
2. Depending on the classification of information, electronic transmission, copying and distribution of copies of such information, shall require prior approval of CISO / CEO, as applicable.
3. Mailing and/or shipment of confidential information shall require that information be sent through a reputed mail service / courier with proper authentication.
4. Confidential information shall be stored with proper security and / or in safe lockers.
5. Disposition of confidential and Project / Process / Department specific information shall require shredding in the presence of CISO / DGM / GM / CEO / Process In-charge, as applicable.
6. Appropriate access restrictions shall be applied to prevent access from unauthorized personnel.
7. Formal record of the authorized recipients of data shall be maintained.
8. Information processing operations shall ensure the following: that input data is complete, that processing is properly completed, and that output validation is applied.
9. Storage of media shall be in accordance with the manufacturers' specifications.
10. All copies of media shall be clearly marked for the attention of the authorized recipient.

11. Spooled data awaiting output shall be protected to a level consistent with its sensitivity.
12. Distribution of data shall be based on “need to know” and “need to use” principles.
13. Distribution lists and lists of authorized recipients shall be reviewed at regular intervals.

8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy.