Logo, company name

Description automatically generated

**Company Information Classification & Handling Policy**

**Doc A8.2**

**Version: 1.0**

**Publication Date: January 01, 2019**

**Current Status: Published**

**Author(s): A.D.Jaliya**

**Last Reviewed: A.D.Jaliya**

**Table of Contents**

1 Information Classification and Handling Policy 3

1.1 Scope 3

1.2 Responsibilities 3

1.3 Classification 3

1.4 Labelling 4

1.5 Confidentiality Agreements and Non-Disclosure Agreements (NDA’s) 4

1.6 Storage 4

1.7 Cloud Storage and sharing services 5

1.8 Storage on Personal Equipment 5

1.9 Communication & Transmission 5

1.10 Reclassification 5

1.11 Destruction 5

1.12 Exchange of Information and Transport of information 5

1.13 System Documentation 5

2 Document Control and Approval 6

2.1 Distribution 6

2.2 Version Information 6

Annex A: Classification and Handling Guidelines Summary 7

# Information Classification and Handling Policy

## Policy Statement

Tellida will establish and execute well-defined and time-tested strategies and processes to guarantee that sensitive information is categorized appropriately and managed according to organizational rules in order to fulfill the enterprise's business objectives and maintain the continuity of its operations. Information is regarded as an organization's most valuable asset. Different sorts of organizational assets are used by an organization. The sensitivity of this organization's assets varies, and their management procedures fluctuate as well.

## Purpose

The objective of these policies is to protect personal and private information against unauthorized access and disclosure. This policy aids in the identification of information in order to allow routine disclosure and active distribution. It also aids in the protection of Tellida's intellectual property.

## Scope

## 1.3.1Employees

## All Tellida management, workers, clients, and third-party personnel who have access to Tellida's IT assets and may be obligated by contractual agreements are subject to this policy.

## 1.3.2 IT Assets

This policy applies to all Tellida information assets.

### Documentation

The information categorization and handling policy, as well as associated processes and guidelines, must be included in the policy document.

### Documentation Controls

All additional linked papers, as well as the information categorization and handling policy document, must be managed. Version control will ensure that the most recent release is preserved, with the prior version of the document being kept for just two years for legal and knowledge preservation considerations.

### Records

Records being generated as part of the information classification and handling policy shall be retained for a period of two years. Record shall be in hard copy of electronic media. The records shall be owned by the respective system administrator and shall be audited once a year.

### Distribution and Maintanance

All workers covered by the scope must have access to the information categorization and handling policy document. All updates and new versions of this document must be made available to those who are affected. The CISO and website administrator will be responsible for maintaining this document.

## Privacy

The information categorization and handling policy document is to be treated as confidential and only given to those who need it with adequate access control. This document's further modifications and revisions will be monitored.

## Responsibility

The CISO or designated individual is in charge of ensuring that the information categorization and handling policy is properly implemented.

## Policy

Tellida categorize information in to four classes;

* Confidential
* Project/ Process/ Department Specific
* Internal
* Public

1. ***Confidential*** – the information assets which have high confidentiality values belong to this category. Only a limited set of authorized users shall access these information assets.
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 can be accessible to members of those concerned department, project or business process only.
3. ***Internal***  - the information assets which can distributed within all offices of Tellida belong to this category. Examples are office orders an 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 and annual financial report of Tellida and information displayed on Tellida’s website.

Following are the policies of secure handling of information assets of Tellida;

1. All media must be handled and labelled in accordance with the level of classification stated on the media.
2. Electronic communication, copying, and distribution of copies of classified material need the prior permission of the CISO / DGM / GM / CEO as appropriate, depending on the classification.
3. Confidential information must be delivered through a reputable primary service or courier with appropriate authentication when mailing or shipping it.
4. Safe lockers or appropriate security are required for the storage of confidential information.
5. This information must be shredded in front of the CISO/DGM/GM/CEO or process owner as appropriate before it may be disposed of confidentially.
6. Appropriate actions restraints will be used to prevent unauthorised individuals from gaining access.
7. It is necessary to have a documented record of the individuals who are allowed to receive data.
8. Information processing activities must verify that input data is complete or that processing is correctly finished and output validation is performed before they can proceed to the next step.
9. Media storage must follow the manufacturer's instructions.
10. All media copies must be properly labelled so that the authorised receiver may easily identify them.
11. Data that has been tampered with and is awaiting output must be safeguarded to a degree commensurate with its sensitivity.
12. Data will be distributed according to "need to know" and "need to utilise" standards.
13. Lists of approved recipients and distribution should be checked on a regular basis.

# Document Control and Approval

The Chief Information Security Officer is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to all members of staff and is the published version.

Signature: Jaliya Date: 03.10.2021

## Distribution

|  |  |
| --- | --- |
| **Name** | **Role** |
| *Intranet* | *Distribution to all staff* |

## Version Information

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author(s)** | **Details** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Annex A: Classification and Handling Guidelines Summary

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Classification** | **Public** | **Company Sensitive** | **Confidential** | **Personal Data, PII or PCI** | **Company Secret** |
| **Description** | Information that can be disclosed to the general public without concern for harming the company, employees, customers or business partners. | Information that can be disclosed within the company but may cause harm to the company if disclosed externally | Anything that provides a competitive advantage and if disclosed would create severe problems for the organization. | Personal Data, Personally Identifiable Information (PII) or payment data such as credit card details covered by Payment Card Industry Data Security Standard  (PCI DSS) | Information usually available to Board members only and if disclosed could cause irreparable harm to the company. |
| **Examples** | Company brochure or web-site.  Business contact information. | Policies and procedures, Intranet content, system and software in use, contracts, offers, other company data that isn’t commercially sensitive. | Customer Confidential Data, Passwords, Pricing, executed contracts, technical design data, customer details, safety information etc. | Individuals name and address, IP Addresses, VIN, usernames, bank account number, credit card number. | Board papers, takeover plans, confidential financial data etc. |
| **Labelling** | Optional | Optional | Mandatory  Printed records must be numbered sequentially as part of a set | Mandatory  Printed records must be numbered sequentially as part of a set | Mandatory  Printed records must be numbered sequentially as part of a set |
| **Storage Encryption** | Not required | Optional | Mandatory | Mandatory | Mandatory |
| **Logging** | No Restrictions | Logs are for internal use only and should not be shared externally without consent from asset owner | Information may be logged. Access is limited to a “need to know basis” down to record level, and access controls should be implemented on the log access (both directly and through tools) | Only IP Address, VIN, and Username may be logged. Requirements:   * Logged information can be removed upon request * Access controls - “need to know” * Obfuscate where possible to eliminate PII (0 of last 5 of VIN) | Never |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Classification** | **Public** | **Company Sensitive** | **Confidential** | **Personal Data, PII or PCI** | **Company Secret** |
| **Reproduction** | No restrictions | Due care and custody | Due care and custody based on Access Control requirements. | None permitted except for any backups necessary to meet business continuity needs | Copies must be limited and returned to the originator or designated representative. |
| **Transmit Encryption** | Not required | Optional | Mandatory for transmission across open public networks using Company approved technology | Mandatory for transmission across open public networks using Company approved technology | Mandatory for transmission across open public networks using Company approved technology |
| **Physical Transmit** | Not required | Retained within company premises or addressed to intended recipient | Retained within company premises or addressed to intended recipient | Secure courier if sent outside company or hand delivered. | Secure courier if sent outside company or hand delivered. |
| **Access Control** | Not required | Staff and trusted contractors only | Discretionary access as determined by owner.  Principle of least access should be followed. | Strictly need to know only enforced by both physical and logical controls | Strictly need to know only enforced by both physical and logical controls |
| **Access Auditing** | Not required | Not required | Optional | Track and monitor all access | Optional |
| **Secure Disposal** | Optional | Mandatory using Company approved method | Mandatory using Company approved method | Mandatory using Company approved method | Mandatory using Company approved method |
| **Transmit approval** | Not required | Not required | Data owner or Document Creator | Data owner or Document Creator | Executive data owner |
| **Retention requirements** | Disposal must be authorized by the data owner | Disposal must be authorized by the data owner | Disposal must be authorized by the data owner | Disposal must be authorized by the data owner | Disposal must be  authorized by a data owner |
| **Classification** | **Public** | **Company Sensitive** | **Confidential** | **Personal Data, PII or PCI** | **Company Secret** |
| **Classification Review** | After any major change and every three years | After any major change and every two years | After any major change and annually | Annually | After any major change and annually |
| **Sharing of information** | Internal: Free to share  External: Free to share | Internal: Free to share  External: Need to know | Internal: Need to know  External: Need to know with NDA in place | Internal: Need to know  External: Rare occasion. Legal approval. NDA and Contract in place | Internal: Strict need to know  External: Strict need to know with NDA in place |
| **Stored on Public Cloud or File Sharing Service** | Allowed | Temporary | Temporary. Must be encrypted.  Never exposed in plain text on 3rd party system | Limited to need. Must be encrypted.  Never exposed in plain text on 3rd party system | Limited to need. Must be encrypted.  Never exposed in plain text on 3rd party system |