Table of Contents

[1. Introduction to Information Classification………………………………………………………………………………… 5](#_Toc78189269)

[2. Purpose…………………………………………………………………………………………………………………………………….. 5](#_Toc78189270)

[3. Objectives of This Policy……………………………………………………………………………………………………………. 5](#_Toc78189271)

[4. Scope………………………………………………………………………………………………………………………………………… 5](#_Toc78189272)

[5. Classification of Information Assets………………………………………………………………………………………….. 5](#_Toc78189273)

[6. Roles and Responsibilities…………………………………………………………………………………………………………. 8](#_Toc78189274)

[ **Data owner**…………………………………………………………………………………………………………………………………. 8](#_Toc78189275)

[ **Data custodians……………………………………………………………………………………………………………………….** 8](#_Toc78189276)

[ **Data user-………………………………………………………………………………………………………………………………..** 8](#_Toc78189277)

[7. Classification Sensitivity Crietria – Information Asset……………………………………………………………… 9](#_Toc78189278)

[8. Electronic Protected Health Information (ePHI)………………………………………………………………………… 9](#_Toc78189279)

[9. Payment Card Information (PCI)………………………………………………………………………………………….…... 9](#_Toc78189280)

[10. Classification Guidelines…………………………………………………………………………………………………………. 9](#_Toc78189281)

**DOCUMENT REVISION CONTROL**

REVISION HISTORY

| **Date** | **Author** | **Version** | **Change Reference** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

REVIEWERS

| **Name** | **Position** | **Date** |
| --- | --- | --- |
|  |  |  |

DISTRIBUTION

| **Date** | **Distributed to** | **Version** | **Distribution Format** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

APPROVALS

| **Date** | **Version** | **Approved by** | **Designation** | **Approval remarks** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

**Information Classification**

Below is the table of guidelines that might be helpful in determining a type of data’s classification level. High Business Impact (HBI), Medium Business Impact (MBI), Low Business Impact (LBI)

| **Information** | **HBI** | **MBI** | **LBI** |
| --- | --- | --- | --- |
| Email Address |  | **\*** |  |
| Social security number | **\*** |  |  |
| Documents regarding process or procedure |  | **\*** |  |
| Private cryptographic keys | **\*** |  |  |
| Username and passwords | **\*** |  |  |
| Publicly accessible information |  |  | **\*** |
| Company trade secrets |  | **\*** |  |
| Financial information related to revenue generation | **\*** |  |  |
| List of phone numbers | **\*** |  |  |
| Employee Zip codes |  |  | **\*** |
| Numeric ID sequences/PINs | **\*** |  |  |

**LIST OF ABBREVIATIONS**

|  |  |  |
| --- | --- | --- |
| **Index** | **Abbreviation** | **Stands For** |
| I | IT | Information Technology |
| 2 | SLA | Service Level Agreement |
| 3 | IOT | Internet of things |
| 4 | IAS | International Accounting Standards |
| 5 | FDP | Finance Department |
| 6 | ITSM | Information Technology Service Management |
| 7 | NDA | Non-Disclosure Agreement |

# Introduction to Information Classification

This policy is concerned with managing information assets owned by <COMPANY NAME> and used by staff in office and at remote locations.

# Purpose

The purpose of this policy is to define the responsibilities of individuals for safeguarding information assets and provide a standard classification system which is adhered by all staff and users, and ensure that information assets are protected, and information assets in respect of sensitive information are classified, in accordance with <Company Name> requirements.

# Objectives of This Policy

* To define the responsibilities of individuals for safeguarding <Company Name> information assets.
* To provide a rigorous and consistent classification system which ensures that information assets are appropriately protected, in accordance with <Company Name> and <Company Name> policies.
* To minimize the damage to the <Company Name>, to its user, staff as a result of sensitive information assets being intercepted or exposed.
* To ensure that information assets which are lost, stolen, damaged or intercepted are sufficiently protected and unreadable.

# Scope

This procedure applies to all documents created, distributed, and retained for information and action in the Information Security Management System (ISMS) and IT service management system (ITSM).

This policy applies to all <Company Name> staff and users.

# Classification of Information Assets

The following procedure shall be followed to determine the Information Asset classification.

Information assets owned and managed by <Company Name> which are sensitive or have value must be protected at all times.

All information in <Company Name> must be classified into one of the following categories by those who own or are responsible for the information:

Impact on Confidentiality shall refer to the impact value on confidentiality if information was revealed to external parties. Impact values are

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr.No.** | **Classification** | **Accessibility/ Availability** | **Impact** |
| 1 | Low | Public | **Public Information**  No Impact. Such information comes from public sources or is provided by <Company Name> to the general public. Examples include periodicals, public bulletins, published press releases, etc. |
| 2 | Medium | Internal | **Internal Information (All departments and personnel within <Company name> )**  Such information is the property of <Company Name>. <Company Name> has the sole rights to this information. This form of information must be used within <Company Name> and not shared with third parties.  Examples include staff memos, company newsletters, staff awareness program documentation or bulletins etc. Sharing Internal documents with subcontractors and vendors shall require official approval, signature of Non-Disclosure agreement and limit information sharing with external parties to what is only necessary to business |
| 3 | High | Private | **Private Information (Individual departments)**  Such information is the property of <Company Name>. <Company Name> has the sole right over this information (exception: subjects of the information in most cases will also have rights to the information, such as a plan member having access rights to their contract). This form of information must be used within <Company Name> and not shared with third parties.  Such information must be restricted to departmental personnel only.  Examples include Strategy Document, Information Security Policy etc. Sharing information across departments shall be governed by official approval and proper scope definition |
| 4 | Very High | Confidential | **Confidential Information (Need to Know)**  Confidential information is a sensitive form of information. This information is distributed on a “Need to Know” basis only. Information that is classified as sensitive and disclosure or usage would have a definite impact on <Company Name>’s business and future shall be classified as confidential with the implementation of extremely restrictive controls (e.g., very limited audience).  Examples include employee personal information, plans, unpublished financial statements, etc. |

# Roles and Responsibilities

* **Data owner**- The person who is ultimately responsible for the data and information being collected and maintained by his or her department or division usually a member of senior management. The data owner shall address the following:

1. Review and categorize the data collected by his or her department or division.
2. Assign data classification labels based on data’s potential impact level
3. Ensure the data shared between departments is consistently classified and protected.
4. Develop data access guidelines for each classification label.

* **Data custodians**- They are technicians responsible for maintaining and backing up systems, databases servers that stores the organization’s data. In addition, this role is responsible for technical deployments of all rules set forth by data owners and for ensuring that the rules applied within systems working. Some responsibilities include:

1. Ensure proper access controls are implemented, monitored, and audited in accordance with data classification labels assigned by data owner.
2. Submit an annual report to the data owners that address availability, integrity, and confidentiality of classified data.
3. Perform regular backups, periodically validate data integrity, and restore data from backup media.
4. Develop data access guidelines for each data classification label

* **Data user-** Person, organization or entity that interacts with, access, uses or updates data for the purpose of performing a task authorized by data owner. Data users must use data in a manner consistent with purpose intended and comply with this policy and all policies applicable to data use.

# Classification Sensitivity Crietria – Information Asset

Sensitivity Criteria will be based on

* Impact on Confidentiality shall refer to the impact value on confidentiality if information was revealed to external parties.
* Impact on Integrity shall refer to the impact on the <Company Name>’s operations and data integrity if information was tampered or illegally changed or amended.
* Impact on Availability shall refer to the impact on the <Company Name>’s operations and security posture if the asset was not available when needed.

# ****Electronic Protected Health Information (ePHI)****

ePHI is defined as any protected health information (PHI) that is stored in or transmitted by electronic media. Electronic media includes computer hard drives as well as removable or transportable media, such as a magnetic tape or disk, optical disk, or digital memory card. Transmission is the movement or exchange of information in electronic form. Transmission media includes the internet, an extranet, leased lines, dial-up lines, private networks, and the physical movement of removable or transportable electronic storage media.

# ****Payment Card Information (PCI)****

Payment card information is defined as a credit card number in combination with one or more of the following data elements:

* Cardholder name
* Service code
* Expiration date
* CVC2, CVV2 or CID value
* PIN or PIN block
* Contents of a credit card’s magnetic stripe

# Classification Guidelines

Classification guideline will be issued by Information Security Team. In the event of uncertainty, or in case of no-knowledge as to the classification of the information asset, it will be considered as Strictly Confidential.

In case of disagreement, knowledge, user shall refer it to their supervisor, or in case it not known to supervisor, it will be sent to <Company Name>, to define and address the sensitivity criteria of the information asset.

In all cases, where there is conflict on sensitivity criteria or disagreement, <Company Name> classification manual will be used as final reference.