

Guideline for Information Asset Valuation

Document ID	ISMS/GL	001	Classification	Internal Use Only
Version No.	Initial		Owner	
Issue Date	28/03/2020		Approved By	

Guideline For Information Asset Valuation

Title	Guideline for Information Asset Valuation
Document ID	ISMS/GL/001
Date	28/03/2020
Status	Initial

Prepared By	Rahul Chugh	28/03/2020
Reviewed By		
Reviewed By		
Approved By		
Approved By		

Distribution List	
Apex Committee	To approve and authorize
ISMS Forum	To review and update
All Departments / Function Heads	To understand and comply

[illegible]

1. OVERVIEW

Information wherever it is handled or stored (e.g., in computers, file cabinets, desktops, fax machines, Xerox, printer, verbal communication etc.) needs to be suitably and appropriately protected from unauthorized access, modification, disclosure, and destruction. All information will not be accorded with the same importance. Consequently, classification of information into categories is necessary to help identify a framework for evaluating the information's relative value and the appropriate controls required to preserve its value to the organization.

To achieve this purpose, upon creation of the information (whether in a computer system, memo in a file cabinet etc.), the creator/owner of that information (generally the information asset owner) is responsible for classification. Further, the owner of information asset is responsible to review the classification of information at least annually.

The analysis is to be done by Business Process Owner i.e. process / function head.

2. Responsibility

	Responsible	Accountable	Consulted	Informed
Identification & Valuation Of Assets	Departments / Function Heads	Departments / Function Heads	ISMS Forum	Apex Committee

3. Terms

A. Information Asset:

Information in Non-digital and Digital form is created, processed, stored, archived, deleted while executing business activities. Examples are database records, mails, source code, paper documents, designs, emails, databases, Process Data, images etc.

An Information Asset is a definable piece of information, stored in any manner which is recognized as 'valuable' to the organization.

Irrespective of the nature of the information assets themselves, they all have one or more of the following characteristics:

- Information Asset is recognized to be of value to the organization.
- They are not easily replaceable without cost, skill, time, resources or a combination.
- They form a part of the organization's corporate identity, without which, the organization may be threatened.

Security classification of an Information Asset will be 'CONFIDENTIAL', 'INTERNAL USE' or 'PUBLIC'

1. CONFIDENTIAL:

If this information is leaked outside Organisation, it will result in major financial and/or image loss. Compromise of this information will result in statutory, legal non-compliance.

2. INTERNAL USE ONLY:

If this information is leaked outside Organisation, it will result in negligible financial loss and/or embarrassment.

Disclosure of this information shall not cause serious harm to Organisation, and access is provided freely to all internal users. Examples include circulars, policies, training materials etc.

3. PUBLIC:

Non availability will have no effect. If this information is leaked outside Organisation, it will result in no loss.

This information must be explicitly approved by the Corporate Communications Department or Marketing Department in case of marketing related information, as suitable for public dissemination. Examples include marketing brochures, press releases.

B. The Information owner:

1. Has approved management responsibility for controlling production, development, maintenance, use and place security controls over the asset.
2. Is a functional owner responsible for ensuring that proper controls are in place to address confidentiality, integrity and availability of information
3. Has authority and responsibility for making cost-benefit decisions essential to ensure accomplishment of organizational mission objectives.
4. Maintain an appropriate level of protection, physical and / or logical, for the information.
5. Review the information classification periodically.
6. Ensure availability of information at all times and circumstances.
7. Periodic review of security controls.
8. Defines and periodically reviews access restrictions and classifications, taking into account applicable access control policies.
9. Defines and periodically reviews backup schedules, restoration schedules, test results of backup and restorations and integrity of the data after restoration.

C. The Information custodian:

1. Is a person designated by the owner to be responsible for protecting information by maintaining safeguards and controls established by the owner
2. Take prior approval of the Business Process Head before sharing information.
3. Perform regular backup and data validity testing activities.
4. Perform data restoration from backups periodically.
5. Implement access control as defined by information owner.
6. Perform regular administrative tasks.

4. Information Asset Valuation**a) Confidentiality of Information Asset**

Confidentiality of information refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from jeopardizing organization security to the disclosure of private data of employees. Following table provides guideline to determine Confidentiality requirements:

This table provides a guideline to identify the confidentiality requirements.

Confidentiality Requirement	Explanation
Low	Non-sensitive information available for public disclosure. The impact of unauthorized disclosure of such information shall not harm Organisation anyway. E.g. Press releases, Company's Newsletters E.g. Information published on company's website
Medium	Information belonging to the company and not for disclosure to public or external parties. The unauthorized disclosure of information here can cause a limited harm to the organization. e.g. Organization Charts, Internal Telephone Directory.
High	Information which is very sensitive or private, of highest value to the organization and intended to use by named individuals only. The unauthorized disclosure of such information can cause severe harm (e.g. Legal or financial liability, adverse competitive impact, loss of brand name). E.g. Client's pricing information, Merger and Acquisition related information, Marketing strategy.

b) Integrity of Information Assets

Integrity refers to the completeness and accuracy of Information. Integrity is lost if unauthorized changes are made to data or IT system by either intentional or accidental acts. If integrity of data is not restored back, continued use of the contaminated data could result in inaccuracy, fraud, or erroneous decisions. Integrity criteria of information can be determined with guideline established in the following Table.

Integrity Requirement	Explanation
Low	There is minimal impact on business if the accuracy and completeness of data is degraded.
Medium	There is significant impact on business if the asset if the accuracy and completeness of data is degraded.
High	The Integrity degradation is unacceptable .

c) Availability of Information Assets

Availability indicates how soon the information is required, in case the same is lost. If critical information is unavailable to its end users, the organization's mission may be affected. Following Table provides guideline to determine availability criteria of information assets

Availability Requirement	Explanation
Low	There is minimal impact on business if the asset / information is not Available for up to 7 days
Medium	There is significant impact on business if the asset / information is not Available for up to 48 hours
High	The Asset / information is required on 24x7 basis