INFORMATION SECURITY CLASSIFICATION GUIDELINES

Document History

#	Version	Date	Created/ Modified by	Change Doc. No & Brief description of the change incorporated	Approved by / Approved Date
1	Initial	24th July 2024	Zamir Shaikh	Initial version released	Azim Shaikh

INFORMATION SECURITY CLASSIFICATION GUIDELINES (TIER 2)

1.
2.

Scope

All the Organization's information assets and services are classified, taking into account their legality, value, sensitivity and criticality to the Organization.

3. Responsibilities

3.1 The Owner of each asset is responsible for its classification, for ensuring it is correctly labeled and for its correct handling in line with its classification.
3.2 The intended recipient of any information assets sent from outside the Organization becomes the Owner of that asset.
3.3 The Information Security Officer is responsible for maintaining the inventory of assets and services together with their classification levels.
3.4 The Information Security Officer is responsible for the technical labeling mechanisms.
3.5 The Manager - Operations is responsible for the creation, maintenance and review of electronic distribution lists and for ensuring that they conform to this security classification system.
3.6 All users of Organizational information assets have specific responsibilities identified in their user agreements.
3.7 Admin is responsible for ensuring that mail/postal services, couriers and sensitive documents (including cheques, invoices, and headed notepaper) are handled in line with specific work instructions.

4. Classification

The Organization classifies information into four levels of classification (High confidential, medium confidential and internally available material and publicly available information.) Classification schedule ISMS-C DOC 8.2A

4.1 The classification level of all assets is identified, both on the asset and in the asset inventory.
4.2 The classification information must be included in the document footer, which must be manually set to appear on all pages of the document, or on the media on which it is recorded, in line with clause 8, below.
4.3 Information received from outside the Organization is dealt in similar manner, however.
4.4 Information that is not marked with a classification level is returned to its sender for classification; if it cannot be returned, it is destroyed.
4.5 The classifications of information assets are reviewed every six months by their Owners and if the classification level can be reduced, it will be. The asset Owner is responsible for de-classifying information.

INFORMATION SECURITY CLASSIFICATION GUIDELINES (TIER 2)

5. High Confidential:

5.1 All the information related to Sr. Management will be treated as confidential information.
5.2 Due care has to be taken to ensure that this information is stored and accessible only to the team who needs it.
5.3 All the client proposals, financial data, sales data are some of the examples of confidential information.

6. Confidential

6.1 This data is specific to client; however, it is provided to a team working on respective client's project.
6.2 Examples of Medium Confidential data include: Customer test data, General Correspondence containing customer information, Proprietary/custom software, specified as Medium Confidential by client/senior management, sales specific data available to sales team.
6.3 Due care has to be taken to ensure that this information is stored and accessible only to the team who needs it.

7. Internal and Private.

7.1 This data is specific to the Organization and shared with all the MBP Pvt Ltd resources.
7.2 The information may include company updates and are strictly internal to MBP Pvt Ltd team.
7.3 Examples of Internal data include: Not coming under High/Medium Confidential data, Specified as Low Confidential by client / senior management, internal publications etc.

8. Publicly available information

8.1 All the information which is published on the internet site or is printed and circulated as a Marketing material is treated as publicly available information.
8.2 Such information is not liable for the confidentiality however integrity of such information is to be ensured all the time.

9. Labeling

9.1 Documents are labeled as set out above. Physical assets are marked by addition of a physical, stick-on label.
9.2 Removable and storage media (CD ROMs, USB sticks, tapes, etc) are labeled to indicate classification levels].
9.3 Information processing facilities are labeled as per sensitivity.

10. Handling

Information assets can only be handled by individuals that have appropriate authorizations or on facilities.

The requirements for receipt, storage and declassification of classified and restricted information are described above. Destruction of information media can only be carried out by someone who has an appropriate level of authorization and in line with the requirements of ISMS-C DOC 11.2.5

10.1 Portable and storage media (including spooled media) must be moved, received and stored based on the highest classification item recorded on them, and are subject to the physical security controls specified in DOC 9.10, and are protected appropriately while being recorded.

The 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 specified members of staff on the corporate intranet and published.

This procedure was approved by the BOD and is issued on a version-controlled basis under his/her signature