CHOICE EQUITY BROKING PVT. LTD

Information Classification Policy

Version Control

Action	Date	Revision Details	Prepared / Amended By	Approved By
Created On	17-Oct-16	1.0	Mahesh Tamhankar	Amit Jaokar
Reviewed On	21-Feb-17	1.1	Mahesh Tamhankar	Amit Jaokar
Reviewed On	13-Feb-18	1.2	Mahesh Tamhankar	Amit Jaokar
Reviewed On	20-Feb-18	1.3	Mahesh Tamhankar	Utpal Parekh
Reviewed On	10-Aug-19	1.4	Mahesh Tamhankar	Yogesh Jadhav
Reviewed On	11-Jan-20	1.5	Mahesh Tamhankar	Yogesh Jadhav
Reviewed On	15-July-21	1.6	Sunil Utekar	Yogesh Jadhav
Reviewed On	08-Jan-22	1.7	Sunil Utekar	Yogesh Jadhav
Reviewed On	09-Apr-23	2.0	Ashutosh Bhardwaj	Yogesh Jadhav
Reviewed On	31-Jan-24	2.1	Anil Ashok & Associates	Ashutosh Bhardwaj
Approved On	08-Jan-2025	2.2	Abhishek Vinayak	Yogesh Jadhav

INFORMATION CLASSIFICATION POLICY

1.0 Purpose

To ensure that integrity and confidentiality of information is maintained, an information classification scheme has been designed for Choice Equity Broking Pvt. Ltd. (Choice). The level of security to be afforded to the information / data of Choice Equity Broking Pvt. Ltd. (Choice)is dependent directly on the classification of the information. All employees are expected to familiarize themselves with this information classification scheme, to consistently use it in their business activities.

2.0 Scope

This information classification scheme is applicable to all information including intellectual property (IP), whether stored or transmitted, which is in the possession or under the control of Choice Equity Broking Pvt. Ltd. (Choice). For example, confidential information entrusted to Choice Equity Broking Pvt. Ltd. (Choice)by its customers, suppliers, business partners, and others shall be protected with this information classification scheme. Similarly, the employees, contractors & service providers of Choice Equity Broking Pvt. Ltd. (Choice)are expected to protect third party information with the same care that they protect information belonging to Choice Equity Broking Pvt. Ltd. (Choice).

3.0 Policy

3.1 Information

Information is an asset which, like other business assets, has value to the organization and consecutively, needs to be protected. Information can be of any form as mentioned below:

- Printed or written on paper
- Stored electronically
- Transmitted by emails or any other electronic means
- Shown on corporate videos
- Spoken in conversation

3.2 Personal Information:

Personally Identifiable Information (PII) is data that can be traced back to an individual and that, if disclosed, could result in harm to that person. Such information includes biometric data, medical information, personally identifiable financial information (PIFI) and unique identifiers such as passport or Social Security numbers.

Information containing PII data shall be considered as confidential information and shall be protected using minimum baseline controls mention in Information classification policy.

Personal information received / stored / sent by employees without any business reason will not be treated as confidential information. Safeguarding personal information stored on corporate systems shall be user responsibility. Any such personal information stored on corporate infra shall be accessed by Choice Equity Broking Pvt. Ltd. (Choice)only post management approval. e.g. Employees share personal data with HR to complete the HR formalities and forget to delete these records like PAN card, Salary slip from the corporate systems. Choice Equity Broking Pvt. Ltd. (Choice)shall not be liable to safeguard this data.

3.3 Business information:

Sensitive business information includes anything that poses a risk to the company in question of discovered by a competitor or the general public. Such information includes trade secrets, acquisition plans, financial data and supplier and customer information, among other possibilities.

- Information pertains to business is further classified to restrict the use or access the information based on its level of sensitivity (for example, confidential, internal and public). Information is generally classified to protect such information from unauthorized use.

Any information classified as confidential and internal shall be protected with minimum baseline controls as mentioned in information classification policy. Access / sharing of such information shall not be conducted without any business reason and appropriate approval. Information classified as public will have no control and restriction on disclosure and storage.

3.4 Intellectual Property (IP):

Choice Equity Broking Pvt. Ltd. (Choice)Intellectual Property includes anything that poses a risk to organization if discovered by a competitor or the general public. Such information includes trade secrets, algorithmic trading source codes / products, acquisition plans, financial data and supplier and customer information, among other possibilities. Such IP may be created by Choice Equity Broking Pvt. Ltd. (Choice)employees or contractors or consultants.

To protect intellectual property, maintain appropriate asset registers giving details of asset ownership and controls implemented for each asset. Ownership of each Intellectual property need to be assigned and reviewed on quarterly basis.

Detailed authority matrix needs to be developed by respective Business Heads to grant appropriate access to Business specific IP. Respective Business Head is overall owner for all the IPs developed and managed by business unit. Different Controls need to be implemented to protect the IP.

Intellectual Property need to be classified as “Confidential” by default.

3.5 Classification Responsibilities

The respective Information owners / business owner are responsible for execution of the policy on Information Classification. Unclassified information shall always be deemed as sensitive information.

3.6 Need to Know

One of the fundamental principles of information security is "need to know." This principle holds that information shall be disclosed only to those people who have a legitimate business need for the information. The following information classification scheme has been designed for Choice Equity Broking Pvt. Ltd. (Choice)to support the need-to-know principle so that information will be protected from unauthorized disclosure, use, modification, and deletion.

3.7 Inventory of assets

The information of Choice Equity Broking Pvt. Ltd. (Choice)shall be consistently protected throughout its life cycle, from its origination to its destruction. Information shall be protected in a manner commensurate with its sensitivity; no matter where it resides, what form it takes, what technology is used to handle it, and what purpose it serves. Although this Information Classification scheme provides overall guidance to achieve consistent information protection, employees of Choice Equity Broking Pvt. Ltd. (Choice)need to apply and extend these concepts to fit the needs of day-to-day operations.

Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.

The lifecycle of information shall include creation, processing, storage, transmission, deletion and destruction. Documentation shall be maintained in dedicated or existing inventories as appropriate. The asset inventory shall be accurate, up to date, and consistent and aligned with other inventories.

3.7.1 Information Asset Owner

The information asset owner is the individual who oversees the implementation and is responsible for the availability of the information. The information asset owner is responsible to define the access matrix for policy implementation. Information Owner shall coordinate with the information asset custodian to ensure the access privileges as defined on “need to know” basis is implemented.

Any individual creating any official document related to the company, he/she becomes an information owner for those set of documents created by him. There shall be an information owner for every information asset. The information owners shall be responsible for assigning / maintaining appropriate information classifications for the critical information under their custody as defined below.

- Ensure that assets are inventoried.
- All files / e-mails created by individuals shall be owned and classified by them.

- The information classification process shall be completed for existing critical information and shall be undertaken for any new avenues that can create new form /instance of the information like new software application
- Same information stored in several media formats (either hard copy or electronic) shall have the same level of classification.
- Define and periodically review access restrictions and classifications to important assets, considering applicable access control policies.
- Ensure proper handling when the asset is deleted or destroyed.

3.7.2 Acceptable use of information assets

- The Choice Equity Broking Pvt. Ltd. (Choice)information assets shall be used only for business purpose
- The responsibility of ensuring the security of the asset shall lie with the asset owner (information owner)
- However, the user shall exercise Due Diligence and Due Care towards the information asset assigned to him
- Any misuse, abuse of Information asset shall be considered as a policy violation
- Information assets shall not be shared with unauthorized individual

3.7.3 Return of assets

- All employees and external party users shall return all the Choice Equity Broking Pvt. Ltd. (Choice)assets in their possession upon termination of their employment, contract or agreement.
- The termination process shall be formalized to include the return of all previously issued physical and electronic assets owned by or entrusted to the Choice Equity Broking Pvt. Ltd. (Choice).
- In cases where an employee or external party user purchases the Choice Equity Broking Pvt. Ltd. (Choice)'s equipment or uses their own personal equipment, procedures shall be followed to ensure that all relevant information is transferred to the organization and securely erased from the equipment.
- In cases where an employee or external party user has knowledge that is important to ongoing operations, that information shall be documented and transferred to the Choice Equity Broking Pvt. Ltd. (Choice).
- During the notice period of termination, the Choice Equity Broking Pvt. Ltd. (Choice)shall control unauthorized copying of relevant information (e.g. intellectual property) by terminated employees and contractors.

3.8 Information Classification Matrix

Information owners of Choice Equity Broking Pvt. Ltd. (Choice)shall use the following matrix to classify information assets in a manner that balances the risk of compromise with the needs of normal business operations.

Table No. 1

Classification Level	**Definition**	**Examples** (includes but not limited to)
Confidential (Level III)	This classification applies to the most sensitive business information, which is intended strictly for use within Choice Equity Broking Pvt. Ltd. (Choice). Its unauthorized disclosure could seriously and adversely impact Choice Equity Broking Pvt. Ltd. (Choice), its stockholders, its business partners, and/or its customers leading to legal and financial repercussions and adverse public opinion. Information that some people would consider to be private is included in this classification.	Investment plans, trading positions, trading strategies (long / short), Algorithm Trading (source codes / developed products), merger and acquisition plans, customer Information, information security risk, Strategy Documents. Employee performance evaluations, internal audit reports, short-term marketing plans, analysis of competitive products / services and intellectual capital of Choice Equity Broking Pvt. Ltd. (Choice)which comprises the collective experience, knowledge, skill, and information of Choice Equity Broking Pvt. Ltd. (Choice)and its people. Sensitive personal information and information that can come under data protection act / legislation.
Internal (Level II)	This classification applies to all other information, which does not clearly fit into any of the other two classifications. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impacts Choice Equity Broking Pvt. Ltd. (Choice), its employees, its stockholders, its business partners, and/or its customers.	Choice Equity Broking Pvt. Ltd. (Choice)internal telephone directory, training materials, and policy documents

Classification Level	**Definition**	**Examples** (includes but not limited to)

Public (Level I)	This classification applies to information, which has been explicitly approved by Choice Equity Broking Pvt. Ltd. (Choice)management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm.	Published research reports, Published annual/quarterly published reports Web site content, Service brochures, advertisements, job opening announcements, and press releases

3.8.1 Cumulative Classification

The information classification levels represent cumulative information sensitivity. As the levels of sensitivity increase, the access and modification controls become more rigorous and comprehensive. For example, confidential information is a restricted subset of internal information and requires additional security controls.

3.8.2 Minimum Baseline Security Control Matrix

The requirements in the following table outline the minimum baseline security control (MBSC) mechanisms that shall be used for each information classification.

Security Objective	**Public**	**Internal**	**Confidential**
Identification and Authentication	None	User IDs and Passwords	User IDs and Passwords, Strong Authentication (2 Factor)
Authorization and Access Control	Access Control for Modification	Authorization for granting access by LOB Head, access control as per functions, or directory level access control	Fine-grained access control
Confidentiality	None	Encryption over public communications facilities (Internet, dial- up)	Encrypted communications and encrypted files on storage media
Integrity	Access / change control	Minimal audit trail (e.g., document history), data integrity checks	Detailed audit trail (e.g., system-level file history), “maker-checker”, Field-level change history

Non-repudiation	Access / change control	Minimal audit trail (e.g., document history)	Detailed audit trail (e.g., system-level file history), Field-level change history, digital signatures
Auditing	Modification, events, alarms	User activities, access denials, alarms	All events, alarms

Security			
Objective	**Public**	**Internal**	**Confidential**
Availability	Virus scanning, backup / restore	Virus scanning, backup/restore	Virus scanning, strong change control over system configuration, backup/restore

3.8.3 Consistent Classification Labeling

All confidential information in physical format shall be labeled accordingly, from the time it is created until the time it is destroyed or re-labeled. Such markings shall appear on all manifestations of the information (hard copies, floppy disks, CD-ROMs, etc.).

3.8.4 Handling of assets

The handling of sensitive material shall be guided by:

- Access restrictions supporting the protection requirements for each level of classification
- Storage of IT assets in accordance with manufacturers' specifications.
- Labeling material to reflect its sensitivity and security classification
- Minimizing distribution of sensitive material
- Recording authorized recipients, marking information with the recipient's identity, confirming

receipt of transmitted data and periodically reviewing records of authorized recipients

- Checking completeness of sensitive material (e.g. by ensuring all information is Input / processed and there is proper accounting for all computer media)
- Sensitive documents and data storage media shall be stored in physically secure locations (e.g. locked, fireproof cabinets etc.)

3.9 Media handling

3.9.1 Management of removal media

Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the Choice Equity Broking Pvt. Ltd. (Choice). The following guidelines for the management of removable media shall be considered:

- If no longer required, the contents of any re-usable media that are to be removed from the Choice Equity Broking Pvt. Ltd. (Choice)shall be made unrecoverable by destroying the media
- Where necessary and practical, authorization shall be required for media removed from the Choice Equity Broking Pvt. Ltd. (Choice)and a record of such removals shall be kept in order to maintain an audit trail.
- All media shall be stored in a safe, secure environment, in accordance with manufacturers' specifications.
- If data confidentiality or integrity is important considerations, cryptographic techniques shall be used to protect data on removable media.
- To mitigate the risk of media degrading while stored data are still needed, the data shall be transferred to fresh media before the media is rendered unreadable.
- Multiple copies of valuable data shall be stored on separate media to further reduce the risk of coincidental data damage or loss.
- Removable media drives shall only be enabled if there is a business reason for doing so.
- Where there is a need to use removable media the transfer of information to such media shall be monitored.

3.9.2 Disposal of media

The disposal of sensitive documents and data storage media shall be guided by:

- Using secure means of disposal
- Recording its disposal
- Checking that embedded data storage media has been erased prior to disposal

3.9.3 Media transfer

Media containing information shall be protected against unauthorized access, misuse or corruption during transportation. The following guidelines shall be considered to protect media containing information being transported:

- Reliable transport or couriers shall be used.
- A list of authorized couriers shall be agreed with management.
- Procedures to verify the identification of couriers shall be developed.
- Packaging shall be enough to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications, for example protecting against

any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields.

- Logs shall be kept, identifying the content of the media, the protection applied as well as recording the times of transfer to the transit custodians and receipt at the destination.
- All confidential information must be encrypted during transfer, both in transit and at rest, to protect it from unauthorized access, interception, or tampering.
- Sensitive data, such as personally identifiable information (PII), financial information, or intellectual property, must only be transferred when absolutely necessary and in accordance with organizational policies.
- Ensure that transferred data is not retained longer than necessary and is securely disposed of or deleted once it is no longer required.

When information is exchanged between two parties with the use of information exchange equipment's like mobile, answering machine, fax machine, electronic mail, Internet etc., following controls shall be considered:

- While using a mobile phone in a public place, ensure that the information is not overheard by others
- Inform the receiver before sending a fax.
- Follow the controls on exchange of information or software using electronic mail and Internet as described in the "Electronic Mail Security Policy" and "Internet Security Policy" respectively
- Users shall ensure that any internal or confidential information is not left as a message on answering machines

3.10 Responsibility of Information Custodian and Information Users

3.10.1 Information Custodian

The information custodian is the individual or team managing the infrastructure needs of the system. The information custodian is responsible for providing a secure infrastructure in support of the data, including, but not limited to, providing physical security, backup and recovery processes, granting access privileges to system users as authorized by information owners or their designees, and implementing and administering controls over the information.

3.10.2 Information User

Information users are individuals who need and use Choice Equity Broking Pvt. Ltd. (Choice)data as part of their assigned duties or in fulfillment of assigned roles or functions within Choice Equity Broking Pvt. Ltd. (Choice). Individuals who are given access to sensitive information have a position of special trust and as such are responsible for protecting the security and integrity of that information.

3.11 Declassification / Downgrading

- The designated information owner may, at any time, upgrade or downgrade (declassify) the classification level of information. To achieve this, the owner shall change the classification label

appearing on the original document and notify all known recipients / users. Any change in the Information classification level shall be authorized by the LOB Head / COO. Proper justification should be provided during label downgrade.

- If known, the date that the confidential information shall no longer be sensitive shall be recorded.
- The designated information owner's LOB head may, at any time prior to scheduled declassification or downgrading, extend the period that information is to remain at a certain classification level.
- To determine whether sensitive information may be declassified or downgraded, it is recommended, at least once a year, information owners shall review the sensitivity classifications assigned to information for which they are responsible.