Choice
The Joy of Earning

CHOICE EQUITY BROKING PVT. LTD

Data 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

Data Classification Policy

OVERVIEW

To implement the security policy and prevent PII data leakage. It also improves compliance and helps organizations adhere to data protection regulations.

Data classification is important because it allows organizations to understand the types of information they are processing and storing. The knowledge gained through data classification allows a company to take the necessary measures to protect the data based on its importance or sensitivity.

What is Personally Identifiable Information (PII)?

Personally Identifiable Information (PII) includes:

1. Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records.
2. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Examples of PII include, but are not limited to:
    a. Name: full name, father's name, mother's name, nominee name.
    b. Date of birth.
    c. Personal identification numbers: passport number, driver's license number, PAN number, Bank account number, or credit card number
    d. Personal address information: street address, or email address
    e. Personal Mobile numbers

f. Personal characteristics: photographic images (particularly of face or other identifying characteristics), fingerprints, or handwriting

will define the security standards and Set of sensitive data for organization on different levels.

Data Types

Highly Sensitive Data: A data point which represents or can be used to identify an unique customer / entity in the system and associated permanently with the customer / entity.

Example of Highly Sensitive Data Points: PII Data (refer above definition).

Medium sensitive data: A data point assigned to customer / entity to be used by internal team members to address customer / entity.

Example of Medium Sensitive Data Points:It should however be noted that, a system generated data property that is assigned to the customer / entity may not qualify as PII data, for example Client Id or a unique customer identifier or lead id, as these are specific to the local scope of the system and does not possess any significant data exposure (identity exposure / identity theft) when seen in isolation

Non-sensitive Data:A data point which is system generated and does not hold any significant value individually.

Example of Non-Sensitive Data Points:System generated dates (createdOn,modifiedOn),System Generated Flags.

Data Leakage Protection

Data Classification:

- Implement a data classification scheme to categorize data based on sensitivity (e.g., public, internal, confidential).
- Ensure that employees understand which types of data are considered sensitive and require extra protection.

Data Loss Prevention Software:

- Implement DLP software to monitor and block unauthorized data transfers (e.g., to USB devices, cloud storage, or external email).
- Configure the DLP system to detect attempts to send, print, or copy sensitive information outside the organization.

GOALS

1. To protect All types of data that are associated with the organization and can potentially expose the customer / entity.
2. To protect User and organization data from unauthorized access.
3. To follow the compliance rules and regulations.
4. Proper Authentication/Authorization to access data on server and databases.

Classification Levels

Developer

1. While logging data avoid logging PII data (PAN,Mobile,email,etc)in log files.
2. While logging PII data is unavoidable then keep it masked.
3. PII files should be privately accessible (PAN, AADHAR, SELFIE)
4. Do not use PII data as file name use.
5. While Storing data use encryption mechanisms to store PII data in database,elastic,redis etc.
6. Follow relevant compliance rules and regulations like SEBI CyberSecurity Framework.

Example of data classification at developer level for **a specific domain**

Project	Whom are we	What are we	Sensitivity Level

	protecting	protecting	
KYC	Customer	PAN Number	HIGH
KYC	Customer	Mobile Number	HIGH
KYC	Customer	EMAIL ADDRESS	HIGH
KYC	Customer	Name	HIGH
KYC	Customer	FATHERS NAME	HIGH
KYC	Customer	MOTHER’S NAME	HIGH
KYC	Customer	DOB	HIGH
KYC	Customer	ADDRESS	HIGH
KYC	Customer	BANK DETAILS	HIGH
KYC	Customer	EDUCATION	NONE
KYC	Customer	INCOME	NONE
KYC	Customer	DOCUMENT POI	HIGH
KYC	Customer	DOCUMENT POA	HIGH
KYC	Customer	DOCUMENT BANK	HIGH

KYC	Customer	DOCUMENT SELFIE	HIGH
KYC	Customer	DOCUMENT VIDEO IPV	HIGH
KYC	Customer	DOCUMENT INCOME PROOF	HIGH
KYC	Customer	DOCUMENT SIGNATURE	HIGH
KYC	Customer	SYSTEM GENERATED DATES (createdOn, Modified)	NONE
KYC	Customer	System Generated Flags	NONE
KYC	Customer	CLIENT ID	MEDIUM
KYC	Customer	INVESTOR ID	NONE
KYC	Customer	LEAD ID	NONE
KYC	Customer	SUBJECT ID	NONE
KYC	RM (Employee / Partner)	REFER CODE	NONE
KYC	RM (Employee / Partner)	REFERRAL PII	HIGH

DevOps

1. At the time of server to server communication, use a private network for data transferring.
2. Authorize/Authenticate users properly.
3. While logging data, avoid logging PII data in log files.
4. Limit database and server and maintain proper user permission.
5. Conduct security audits on a regular basis.

Example of data classification at DevOps level for a specific domain

Project	What are we protecting	Sensitivity Level
KYC	Application Server	HIGH
KYC	Databases	HIGH
KYC	API Endpoints	HIGH
KYC	File Storage	HIGH
KYC	Media storage	HIGH
KYC	Redis / Elastic	HIGH
KYC	S3	HIGH
KYC	Network Access	HIGH

Organization

1. Conduct regular risk assessments to identify potential security vulnerabilities and prioritize actions to mitigate risks.
2. Limit access to sensitive data to only those who need it.
3. Educate employees on data security best practices and provide regular training on how to identify and respond to security incidents
4. Use internal tools for data analytics and visualization.

Business Entity	Assets / Software Under Protection	Sensitivity Level
CEBPL	Data Center Hardware	HIGH
CEBPL	Trading System	HIGH
CEBPL	LMS Software	HIGH
CEBPL	KYC Software	HIGH
CEBPL	Back Office Software	HIGH
CEBPL	RMS	HIGH
CWMPL	MF BACK OFFICE SOFTWARE	HIGH
CHOICE CONNECT	Partner System	HIGH
CHOICE INSURANCE	Insurance Back Office System	HIGH
CEBPL	KYC Department - Physical Documents	HIGH

Authority / Regularity

1. We can educate employees on data security best practices and provide regular training on how to identify and respond to security incidents.
2. Can implement access controls, as they are critical for ensuring that only authorized users have access to the organization's data assets. Access controls can include user authentication, role-based access controls, and data encryption.
3. Can conduct security audits on a regular basis.
4. The authority can check whether the system complies with relevant regulations, standards, and guidelines