Choice
The Joy of Earning

Choice Equity Broking PVT. LTD

Asset Classification POLICY

Version Control

Action	Created Date	Revision Details	Prepared / Amended By	Approved Date	Approved By
Initial Creation	17-Oct-16	1.0	Mahesh Tamhankar	17-Oct-16	Amit Jaokar
Revision	17-Feb-17	1.1	Mahesh Tamhankar	21-Feb-17	Amit Jaokar
Revision	09-Feb-18	1.2	Mahesh Tamhankar	13-Feb-18	Amit Jaokar
Revision	16-Feb-18	1.3	Mahesh Tamhankar	20-Feb-18	Utpal Parekh
Revision	07-Aug-19	1.4	Mahesh Tamhankar	10-Aug-19	Yogesh Jadhav
Revision	09-Jan-20	1.5	Mahesh Tamhankar	11-Jan-20	Yogesh Jadhav
Revision	13-July-21	1.6	Sunil Utekar	15-July-21	Yogesh Jadhav
Revision	05-Jan-22	1.7	Sunil Utekar	08-Jan-22	Yogesh Jadhav
Revision	06-Apr-23	2.0	Ashutosh Bhardwaj	09-Apr-23	Yogesh Jadhav
Revision	29-Jan-24	2.1	Anil Ashok & Associates	31-Jan-24	Ashutosh Bhardwaj
Approved	08-Jan-2025	2.2	Abhishek Vinayak	08-Jan-2025	Yogesh Jadhav

Version Control Revised Format

Version	Activity	Date	Description	Person Responsible
2.3	Amendments	05th April, 2025	Amendments done and submitted for review regarding the monitoring and logging in the protection mechanisms.	Abhishek Vinayak, Associate Information Security
2.3	Reviewed	07th April, 2025	Reviewed the changes.	Shripad Mayekar, Manager Information Security
2.3	Approved	07th April, 2025	Approved the changes	Ashutosh Bhardwaj, CISO

Table of Contents

1. Objective

The primary objective of this policy is to establish a structured framework for classifying IT assets, in accordance with their criticality and sensitivity. This will ensure appropriate protection measures are in place, facilitate regulatory compliance with regulatory guidelines, and safeguard the confidentiality, integrity, and availability of Choice Equity Broking Pvt. Ltd. 's (CEBPL) data and systems.

2. Scope

This policy defines asset criticality and data sensitivity levels and establishes appropriate security controls and procedures.

This policy applies to all CEBPL employees, contractors, and third-party service providers who handle or manage organizational assets. It covers all assets across physical & digital domains, including:

- **Data Assets:** Customer databases, KYC documents, trade transactions, financial records, internal communications (email, messaging)
- **End-User Devices:** Laptops, desktops, and mobile devices used by staff and dealers
- **Compute Infrastructure:** On-premise servers (e.g., MSSQL, MySQL, Redis, Elastic), virtual machines, cloud compute (e.g., AWS EC2)
- **Network Infrastructure:** Firewalls, routers, switches
- **Software Assets:** Core business and trading systems (RMS, OMS, back office), SaaS tools (Zoho Analytics, JIRA, Freshdesk, Slack), monitoring platforms (Grafana, Zabbix)
- **Physical Infrastructure:** CCTV systems, UPS, access control mechanisms

This policy defines the classification levels and protection controls applicable to each asset type. A detailed and up-to-date inventory, including asset criticality and sensitivity labels, to be maintained in the internal Critical Asset Register.

3. Key Definitions

- **Asset**: Any system, software, hardware, or data that holds value to the organization or is required to perform business operations.
- **Data Classification**: The process of categorizing data based on its level of sensitivity, regulatory requirements, and impact on business if exposed or compromised.
- **Critical Asset**: Any asset whose unavailability, compromise, or unauthorized access would directly impact the continuity, integrity, or security of CEBPL's trading operations, client obligations, or regulatory compliance.

4. Asset and Data Classification Framework

The framework classifies all assets at CEBPL along two independent type of classification levels:

- **Asset Criticality Level** - Based on impact to trading, operations, or compliance if the asset is unavailable or compromised.
- **Data Sensitivity Level** - Based on risk from unauthorized access, disclosure, or misuse of the data content.

4.1 Asset Criticality Levels

Assets are classified into two levels based on their impact on CEBPL's trading operations, regulatory obligations, and business continuity: **Critical** and **Non-Critical**.

4.1.1 Critical Assets

Assets essential for maintaining trading operations, regulatory obligations, and core business continuity. Disruption or compromise of these assets can lead to significant financial, operational, or reputational damage.

Asset Type	Asset Name / Examples	Scope & Usage
Compute Infrastructure	AWS EC2, On-prem SQL, MySQL, Redis, Elastic	Servers hosting trading related web servers, application servers, databases and storage / file servers
Network Infrastructure	Firewalls & Network Equipments such as switches at Head Office, Primary Data Center & Disaster Recovery Site	Maintains secure communication with exchanges and trading systems
Trading Applications	RMS, OMS	Core applications for real-time order routing and execution

4.1.2 Non-Critical Assets

Assets that support internal operations, reporting, or analysis. Their unavailability has limited or no immediate impact on critical business functions.

Asset Type	Asset Name / Examples	Scope & Usage
Business Support Apps	Zoho Analytics, Freshdesk	BI, analytics, and customer service - supports decision making
Monitoring Tools	Grafana, Zabbix, Superset	Used for monitoring system performance and visualizations
General IT Devices	Laptops, Desktops, Printers	Used for documentation, internal communication
Physical Infrastructure	CCTV, Biometric & Door Access Systems	Shadow IT used for physical surveillance and attendance tracking

4.2 Data Sensitivity Levels

Data is classified based on the potential impact of unauthorized access, disclosure, or misuse. Classification helps determine the appropriate level of protection and controls required.

4.2.1 Confidential

Highly sensitive information that, if compromised, could result in significant legal, regulatory, financial, or reputational damage.

Data Type	**Examples**	**Scope & Usage**
Personally Identifiable Information (PII)	KYC documents, PAN, Aadhaar, customer account data, login information	Used for login, onboarding, trading session, regulatory compliance, and client servicing
Financial & Transactional Data	Customer trades, ledgers, margin statements	Used in trading, reporting, and compliance submissions

4.2.2 Internal

Data intended for internal use only, where unauthorized access could result in internal disruptions but no regulatory impact.

Data Type	**Examples**	**Scope & Usage**
System Logs	Non-sensitive operational logs	Used for operational management
MIS	Non-sensitive, internal only business MIS Reports	Used for business reporting

4.2.3 Public

Data that can be freely shared without significant risk to the organization or clients.

Data Type	**Examples**	**Scope & Usage**
Public Notices	Ads, Circulars	Used for marketing campaigns.
Market data	Stock price historical data, Stock price live data	Used for providing information to clients.

5. Protection Mechanisms

Each asset and data classification level requires specific security controls and procedures to ensure its protection.

5.1 Critical Assets

Protection Mechanisms:

- **Physical Security**: Restricted access to physical infrastructure (e.g., servers, data centers) using biometric or keycard systems.
- **Network Security**: Implement firewalls at both primary and DR sites to block unauthorized network access.
- **Encryption**: Use encryption at rest and in transit for all critical databases (SQL, MySQL, Redis, Elastic), ensuring that sensitive data is encrypted with organization-managed keys.
- **Backup & Disaster Recovery**:
  - Daily encrypted backups of critical data (KYC, PII) to AWS S3 with a minimum retention period of 10 years.
  - Test DR plans annually, ensuring business continuity from the DR site.
- **Access Control**:
  - Active Directory with Role-Based Access Control (RBAC) to enforce least privilege.
  - Mandatory Multi-Factor Authentication (MFA) for all critical systems, including AWS access, GitLab, and customer databases.
- **Monitoring & Logging**:
  - Continuous monitoring of servers using **Grafana** and **Zabbix** for real-time alerts on anomalies.
  - Retain logs for firewalls, databases, and applications for a minimum of 6 months in active mode and 2 years in archival as per SEBI guidelines.

5.2 Non-Critical Assets

Protection Mechanisms:

- **Basic Security Controls**: Access control using Active Directory, regular software updates.
- **Regular Backups**: Weekly backups of non-critical data to AWS S3.
- **Basic Monitoring**: Systems monitored for operational efficiency without extensive security controls.

6. Data Handling Procedures

6.1 Data Collection and Storage

- **Confidential Data**: PII and trade secrets should only be collected where necessary and stored in encrypted databases. Access to this data must be logged and monitored continuously.

- **Anonymization & Masking**: For non-production environments, any use of sensitive data must be anonymized or masked to prevent unauthorized access to real customer information.

6.2 Data Sharing & Transfer

- **Internal Sharing**: Sensitive data should only be shared internally on a need-to-know basis, utilizing secure channels such as encrypted email.
- **External Sharing**: When sharing with third parties (e.g., auditors), ensure that data is transferred securely using encryption mechanisms.

6.3 Data Retention & Deletion

- **Data Retention**: Critical customer data must be retained for 10 years to comply with SEBI requirements.
- **Data Deletion**: Once the retention period is complete, data must be irreversibly deleted or destroyed following secure data wiping practices.

7. Asset Lifecycle Management

7.1 Asset Onboarding

- **Risk Assessment**: Prior to deployment, every new asset must undergo a comprehensive risk assessment to determine its criticality and required protection measures.

7.2 Asset Decommissioning

- **Secure Deletion**: Before decommissioning any hardware or cloud instances, ensure that all sensitive data is securely wiped and cannot be recovered.
- **Compliance Verification**: Conduct an audit to confirm that no critical data remains on decommissioned systems.

8. Compliance with Regulations

- **Periodic Reports**: The CISO must submit detailed reports to cyber security committee covering:
  - Compliance with cybersecurity frameworks.
  - Incident reports related to critical data breaches or compromises.
  - Updates on audits and assessments of critical and sensitive assets.
- **Regulatory Audits**: Regular audits must be conducted internally and by third-party auditors to ensure ongoing compliance with SEBI’s data security requirements.

9. Roles & Responsibilities

9.1 Chief Information Security Officer (CISO)

- Ensure regular reviews of asset criticality and data sensitivity levels.
- Coordinate regulatory reporting and compliance efforts.

9.2 Operations & IT Teams

- Implement technical controls for asset protection, such as firewalls, encryption, and backups.
- Conduct periodic reviews of access control mechanisms and backup processes.

9.3 Data Owners

- Ensure accurate classification of data based on data classification.
- Manage access rights to ensure the principle of least privilege.

10. Review and Maintenance

This policy must be reviewed and updated annually or upon significant changes to regulatory requirements, business operations, or the IT environment.

Annexure

A. **Classification Matrix**

Link: Annexure-Asset Classification Matrix