

Vardhaman Capital Pvt.Ltd.

POLICY ON IDENTIFICATION OF CRITICAL ASSETS BASED ON SENSITIVITY

Policy created by	Designated Officer
Policy reviewed by	Technology Committee
Policy reviewed on	31-12-2024
Policy Approved by	Board of Directors
Policy approved on	04-01-2025

Version – 1.0

Purpose

The purpose of this Critical Asset Identification Policy is to establish guidelines and procedures for the identification and classification of critical assets based on sensitivity at [Vardhaman Capital Pvt.Ltd.], a stock brokerage firm. This policy aims to ensure the prioritized protection and security of assets crucial to the firm's operations, compliance, and client trust.

Scope

This policy applies to all employees, contractors, third-party vendors, and any other individuals involved in the identification and classification of critical assets within the stock brokerage firm.

Policy Guidelines

Asset Identification Criteria

- Assets will be identified based on their significance to the firm's operations, regulatory compliance, and client services.
- Criteria for identification include financial impact, legal requirements, operational dependence, and potential harm in case of compromise.

Data Sensitivity Classification

- Data will be classified based on its sensitivity and importance to the business.
- Each classification level will determine the security controls and access restrictions for the identified critical assets.

Identification Process

- A systematic process will be established to identify critical assets, involving collaboration between business units, IT, security, and compliance teams.
- The identification process will be periodic and reactive to changes in the business environment.

Asset Inventory

- A comprehensive inventory of critical assets will be maintained, including but not limited to financial data, client information, trading platforms, and communication systems.
- The inventory will include details such as asset type, classification, owner, and associated risks.

Access Control

- Access to critical assets will be restricted based on their sensitivity classification.
- Access permissions will be regularly reviewed and adjusted as necessary.

Data Encryption

- Encryption will be applied to critical data assets, both in transit and at rest.
- Encryption protocols will align with industry standards and regulatory requirements.

Physical Security Measures

- Critical physical assets, such as servers and communication infrastructure, will be housed in secure locations with access controls and monitoring.
- Adequate measures will be taken to protect against physical threats.

Incident Response Plan for Critical Assets

- An incident response plan specifically addressing critical assets will be established to ensure a swift and effective response in case of security incidents.
- Regular testing and updates of the incident response plan will be conducted.

Compliance and Legal Considerations

Regulatory Compliance

- The asset identification and protection processes will comply with relevant financial regulations and industry standards.
- Regular audits will be conducted to verify compliance.

Review and Update

This policy will be reviewed regularly and updated as necessary to address changes in the business environment, regulatory requirements, and emerging security threats.

Employee Responsibilities

Employees involved in the identification and management of critical assets are responsible for adhering to this policy and promptly reporting any concerns or incidents.

Training and Awareness

- Employees will undergo training on critical asset identification, classification, and protection.
- Awareness campaigns will be conducted to foster a culture of responsibility and security.

Change in the Policy will be adopted as and when required by the company and is binding on all the Staff / Employees /and Directors of the Company.

Vardhaman Capital Pvt.Ltd.

CISO :- Anup Kumar Khandelwal

Dated: - 04-01-2025