VARDHAMAN CAPITAL PVT.LTD.

TECHNICAL GLITCHES POLICY

Circular: - Ref. SEBI/HO/MIRSD/TPD-1/P/CIR/2022/160 dated November 25, 2022

Policy created by	Designated Officer
Policy reviewed by	Technology Committee
Policy reviewed on	31st Dec 2023
Policy Approved by	Board of Directors
Policy approved on	4th Jan 2024

Version – 1.0

Objective

To establish a comprehensive framework for addressing and mitigating technical glitches in electronic trading systems, ensuring investor protection and market integrity.

Definition of Technical Glitch

A technical glitch refers to any malfunction in the stock broker's systems, including hardware, software, networks, processes, or services provided electronically. This malfunction may lead to stoppage, slowing down, or variance in normal system functions for a contiguous period of five minutes or more.

Reporting Requirements

- We will inform the respective stock exchanges about any technical glitch, not later than one hour from the time of occurrence.
- Submission of a Preliminary Incident Report to the Exchange within T+1 day of the incident, including details of the incident, its impact, and immediate actions taken.
- Submission of a Root Cause Analysis (RCA) Report to the stock exchange within 14 days, covering the incident's cause, duration, impact analysis, and corrective/preventive measures. The RCA report, for all technical glitch incidents greater than 45 minutes, an independent auditor's report on the RCA shall be submitted within 45 days of the incident.

Capacity Planning

- We will conduct regular capacity planning for their trading infrastructure, including servers, network availability, and trading applications.
- Monitoring peak load with installed capacity at least 1.5 times the observed peak load.
- Deploying mechanisms to receive alerts on capacity utilization beyond 70% of installed capacity.

Software Testing and Change Management

- Rigorous testing of all software changes before deployment.
- Creation of test-driven environments, automated testing, and a traceability matrix between functionalities ar unit tests.
- Implementation of a change management process to prevent unplanned and unauthorized changes.

Monitoring Mechanism

- Establishment of an API-based Logging and Monitoring Mechanism (LAMA) between stock exchanges and st brokers' trading systems.
- Real-time or near-real-time monitoring of key parameters by both stock brokers and stock exchanges.

- We ensure to preserve the logs of the key parameters for a period of 30 days in normal course. However, if a technical glitch takes place, the data related to the glitch, shall be maintained for a period of 2 years.

Business Continuity Planning (BCP) and Disaster Recovery Site (DRS)

- Mandatory establishment of BCP-DR set up for stock brokers with a specified client base i.e. 'Specified Members'.
- Periodic review of BCP-DR policy outlining standard operating procedures.
- Conducting DR drills/live trading from DR site, ensuring full redundancy and ISO certification.

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.

For Vardhaman Capital Pvt. Ltd.

Khandelwal

Director.

Designated Officer

(Anup Kumar Khandelwal)

Dated: - 31/12/2024

Vardhaman Capital Private Limited

Members : NSE & BSE • DEPOSITORY PARTICIPANT : NSDL • SEBI Regd. No.: INZ000204533

EMPOWERING INVESTORS
A SEBI Initiative

CERTIFIED TRUE COPY OF THE RESOLUTION PASSED AT THE BOARD MEETING OF "VARDHAMAN CAPITAL PRIVATE LIMITED" AT THE REGISTERED ADDRESS -25, SWALLOW LANE 2ND FLOOR, KOLKATA-700001 HELD ON 04th DAY OF JANUARY, 2024.

Resolved that the Board of Directors recognizes the increasing importance of cybersecurity in safeguarding the organization's assets and sensitive information from potential threats and breaches. The Board acknowledges the need to identify and prioritize critical systems that play a vital role in the organization's operations and house sensitive or confidential data.

Resolved further, that the Board of Directors hereby approves the following list of critical systems that require cybersecurity measures:

- [Firewall- Sophos]: [HAS BEEN SETUP TO PROTECT THE WHOLE SYSTEM FROM ANY OUTSIDE VIRUS/HACKERS/MALWARES/UNAUTHORISED PENITRATION THROUGH INTERNET]
- [Server]: [SERVER IS INSTALLED TO HANDLE CTCL AND OTHER IMPORTANT FRONT END AND BACK END ACTIVITIES INCLUDING OUTSOURCES CLOUD BASED SERVERS . TO RUNNING THE WHOLE PROCESS THE SERVER ARE MUST.]
- [Networking]: [THE NETWROKING HAS BEEN DONE UNDER GUIDENCE FROM VENDOR AND RUNNING OF ALL SYSTEM SMOOTHLY]

Resolved further, that Shri/ Smt./ Kum Anup Kumar Khandelwal (Designated Officer) of **Vardhaman Capita Private Limited** be hereby authorize to implement and oversee enhanced cybersecurity measures for the identified critical systems.

Resolved further, that the Board commits to regular reviews and updates of the list of critical systems to adapt to evolving cybersecurity risks and changes in the organization's technology landscape.

For M/s. VARDHAMAN CAPITAL PVT.LTD.

For Vardhaman Capital Pvt. Ltd.

Director.

(Anup Kumar Khandelwal)
Director

Date: 04/01/2024
Place: Kolkata

VARDHAMAN CAPITAL PVT.LTD.

BCP AND RESPONSE MANAGEMENT POLICY

Policy created by	Designated Officer
Policy reviewed by	Technology Committee
Policy reviewed on	31st Dec 2023
Policy Approved by	Board of Directors
Policy approved on	4th Jan 2024

Version – 1.0

Purpose

The purpose of this Business Continuity Planning (BCP) and Response Management Policy is to establish guidelines and procedures to ensure the continuity of critical business operations, mitigate the impact of disruptions, and provide a structured response to emergencies or unforeseen events at our Company.

Scope

This policy applies to all employees, contractors, and third-party vendors who have responsibilities related to the business continuity and response management efforts of the stock brokerage firm.

Policy Guidelines

Risk Assessment and Business Impact Analysis (BIA)

- Regular risk assessments and BIAs will be conducted to identify potential threats and assess their impact on critical business functions.
- Findings from risk assessments and BIAs will inform the development and updating of the BCP.

Business Continuity Planning (BCP) Framework

- A comprehensive BCP framework will be established to guide the development, implementation, and maintenance of business continuity plans.
- BCPs will address various scenarios, including but not limited to technology failures, natural disasters, and pandemics.

Emergency Response Plan

- An Emergency Response Plan will be developed to provide clear guidelines for immediate response to emergencies.
- Roles and responsibilities during emergencies will be clearly defined.

Communication Protocols

- Effective communication protocols will be established to ensure timely and accurate dissemination of information during emergencies.
- Communication channels will be diverse to accommodate various scenarios.

Employee Training and Awareness

- Employees will receive regular training on their roles and responsibilities during emergencies.
- Awareness campaigns will be conducted to ensure all employees are familiar with the BCP and Emergency Response Plan.

Alternative Work Arrangements

- Plans for alternative work arrangements, such as remote work, will be in place to ensure continuity in the event of office unavailability.
- Technology infrastructure will be equipped to support remote work.

Data and System Backup

- Data backup and system recovery procedures will be established to ensure the availability of critical systems and data during disruptions.

- Regular testing of backup and recovery processes will be conducted.

Testing and Exercises

- Regular testing and simulation exercises will be conducted to assess the effectiveness of the BCP and response plans.
- Findings from exercises will inform updates and improvements to the plans.

Coordination with External Partners

- Coordination with external partners, such as regulators and key vendors, will be established to ensure a collaborative and effective response during emergencies.

Compliance and Legal Considerations

Regulatory Compliance

- The BCP and response management efforts will comply with relevant financial regulations and industry standards.
- Periodic audits will be conducted to verify compliance.

Review and Update

- This policy will be reviewed regularly and updated as necessary to address emerging risks, technological advancements, and regulatory changes.

Employee Responsibilities

- Employees are responsible for familiarizing themselves with the BCP and Emergency Response Plan and following guidelines during emergencies.
- Reporting incidents promptly is crucial to effective response and recovery efforts.

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.

For Vardhaman Capital Pvt. Ltd.

Director.

Designated Officer

(Anup Kumar Khandelwal)

Dated: - 31/12/2024

VARDHAMAN CAPITAL PVT.LTD.

BRING YOUR OWN DEVICE POLICY

Policy created by	Designated Officer
Policy reviewed by	Technology Committee
Policy reviewed on	31st Dec 2023
Policy Approved by	Board of Directors
Policy approved on	4th Jan 2024

Version – 1.0

Purpose

The purpose of this Bring Your Own Device (BYOD) policy is to establish guidelines for the secure and productive use of personal devices by employees at our Company. This policy outlines the responsibilities of both employees and the organization to ensure the confidentiality, integrity, and availability of sensitive financial information.

Scope

This policy applies to all employees, contractors, and third-party vendors who use personal devices to access company resources, data, or systems.

Policy Guidelines

Eligibility

- Employees eligible for BYOD must meet certain security and compliance criteria determined by the IT department.

Device Security Requirements

- Devices must have up-to-date antivirus software and security patches.
- Employees must use strong, unique passwords or passcodes to access devices.
- Devices must be configured to automatically lock after a specified period of inactivity.

Data Protection

- Employees must adhere to data classification policies and take necessary precautions to protect sensitive financial data.
- Company data should not be stored on personal devices unless authorized by the IT department.

Network Security

- Employees must connect to secure and password-protected Wi-Fi networks.
- Public Wi-Fi networks should be avoided when accessing company resources.

Software and Application Management

- Only authorized software and applications should be installed on personal devices.
- Employees are responsible for keeping software and applications up to date.

Compliance and Legal Considerations

Regulatory Compliance

- All activities conducted on personal devices must comply with relevant financial regulations and industry standards.

Monitoring and Auditing

- The organization reserves the right to monitor and audit personal devices for security and compliance purposes.

Employee Responsibilities

Purpose

The purpose of this Bring Your Own Device (BYOD) policy is to establish guidelines for the secure and productive use of personal devices by employees at our Company. This policy outlines the responsibilities of both employees and the organization to ensure the confidentiality, integrity, and availability of sensitive financial information.

Scope

This policy applies to all employees, contractors, and third-party vendors who use personal devices to access company resources, data, or systems.

Policy Guidelines

Eligibility

- Employees eligible for BYOD must meet certain security and compliance criteria determined by the IT department.

Device Security Requirements

- Devices must have up-to-date antivirus software and security patches.
- Employees must use strong, unique passwords or passcodes to access devices.
- Devices must be configured to automatically lock after a specified period of inactivity.

Data Protection

- Employees must adhere to data classification policies and take necessary precautions to protect sensitive financial data.
- Company data should not be stored on personal devices unless authorized by the IT department.

Network Security

- Employees must connect to secure and password-protected Wi-Fi networks.
- Public Wi-Fi networks should be avoided when accessing company resources.

Software and Application Management

- Only authorized software and applications should be installed on personal devices.
- Employees are responsible for keeping software and applications up to date.

Compliance and Legal Considerations

Regulatory Compliance

- All activities conducted on personal devices must comply with relevant financial regulations and industry standards.

Monitoring and Auditing

- The organization reserves the right to monitor and audit personal devices for security and compliance purposes.

Employee Responsibilities

- Employees are responsible for the security of their personal devices used for work purposes.
- Promptly report lost or stolen devices to the IT department.
- Report any suspicious activity or security incidents to the IT department.

Termination of Access

Access to company resources via personal devices may be revoked at any time, especially in the event of a security breach or termination of employment.

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.

For Vardhaman Capital Pvt. Ltd.

Director.

Designated Officer

(Anup Kumar Khandelwal)

Dated: - 31/12/2024

VARDHAMAN CAPITAL PVT.LTD

DATA DISPOSAL AND RETENTION POLICY:

Policy created by	Designated Officer
Policy reviewed by	Technology Committee
Policy reviewed on	31st Dec 2023
Policy Approved by	Board of Directors
Policy approved on	4th Jan 2024

Version – 1.2

Purpose:

The purpose of this policy is to detail the procedures for the retention and disposal of information to ensure that we carry this out consistently and that we fully document any actions taken. Unless otherwise specified the retention and disposal policy refers to both hard and soft copy documents. This Policy is also for the purpose of aiding employees in understanding their obligations of retaining electronic documents - including email, text files, digital images, sound and movie files, PDF documents, and all Microsoft Office or other formatted files or paper documents.

Review:

This policy defines the Data retention and destruction schedule for paper and electronic records. The Data Retention Schedule is approved as the initial maintenance, retention and disposal schedule for the physical (paper) and electronic records. The Technology committee of Company is responsible for the administration of this policy and the implementation of processes and procedures. In continuation with SEBI guidelines, the Designated Officer is also authorized to; make modifications to the Record Retention Schedule as needed to ensure that it is in compliance with SEBI regulations; ensure the appropriate categorization of documents and records on behalf of the company annually review the policy; and monitor compliance with this policy. Review is the examination of closed records to determine whether they should be destroyed, retained for a further period or transferred to an archive for permanent preservation.

How long we should keep our paper records -

✓ Records should be kept for as long as they are needed to meet the operational needs of the Authority, together with legal and regulatory requirements. We have assessed our records to:

- Determine their value as a source of information about the Authority, its operations, relationships and environment
- Assess their importance as evidence of business activities and decisions
- Establish whether there are any legal or regulatory retention requirements

✓ Where records are likely to have a historical value, or are worthy of permanent preservation, we will transfer them to the National Archives after 25 years.

Responsibilities of Employees -

All employees are responsible for:

✓ checking that any information that they provide in regards to their employment is accurate and up to date

✓ informing the regulatory authority of any changes to information, which they have provided i.e. changes of address

✓ Checking the information that the Organization will send out from time to time, giving details of information kept and processed about employees.

✓ Informing Designated Officer of any errors or changes. The Company cannot be held responsible for any errors unless the employees has informed the management of them.

Disposal schedule:

✓ A disposal schedule is a key document in the management of records and information.

✓ Records on disposal schedules will fall into three main categories:

- Destroy after an agreed period – where the useful life of a series or collection of records can be easily predetermined (for example, destroy after 3 years; destroy 2 years after the end of the financial year).
- Automatically select for permanent preservation – where certain groups of records can be readily defined as worthy of permanent preservation and transferred to an archive.
- Review is the examination of closed records to determine whether they should be destroyed, retained for a further period or transferred to an archive for permanent preservation.

✓ Records can be destroyed in the following ways:

- **Destruction**

▪Non-sensitive information – can be placed in a normal rubbish bin

▪Confidential information – cross cut shredded and pulped or burnt

▪Highly Confidential information – cross cut shredded and pulped or burnt

✓ Electronic equipment containing information - destroyed using kill disc and for individual folders, they will be permanently deleted from the system.

✓ Destruction of electronic records should render them non-recoverable even using forensic data recovery techniques.

✓ Archival transfer

- This is the physical transfer of physical records to a permanent custody at the National Archives Office.

Sharing of information:

✓ Duplicate records should be destroyed. Where information has been regularly shared between business areas, only the original records should be retained in accordance with the guidelines mentioned above. Care should be taken that seemingly duplicate records have not been annotated.

✓ Where we share information with other bodies, we will ensure that they have adequate procedures for records to ensure that the information is managed in accordance with the Authority's policies, relevant legislation and regulatory guidance.

✓ Where relevant to do so we will carry out a data privacy impact assessment and update our privacy notices to reflect data sharing.

Data Security:

✓ All employees are responsible for ensuring that: Any personal data which they hold is kept securely. Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorized third party.

✓ Employees should note that unauthorized disclosure and/or failure to adhere to the requirements set out above will usually be a disciplinary matter, and may be considered gross misconduct in some Data cases.

✓ Personal information should be; kept in a locked filing cabinet; or in a locked drawer; or if it is computerized, be password protected; or when kept or in transit on portable media the files themselves must be password protected.

✓ Personal data should never be stored at employees' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites.

✓ Ordinarily, personal data should not be processed at employees' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites. In cases where such off-site processing is felt to be necessary or appropriate, the agreement of the relevant Data Controller must be obtained, and all the security guidelines given in this document must still be followed.

- ✓ Data stored on portable electronic devices or removable media is the responsibility of the individual employee who operates the equipment.

An Audit Trail:

- ✓ You do not need to document the disposal of records which have been listed on the records retention schedule. Documents disposed out of the schedule either by being disposed of earlier or kept for longer than listed will need to be recorded for audit purposes.
- ✓ This will provide an audit trail for any inspections conducted by the regulatory and will aid in addressing Freedom of Information requests, where we no longer hold the material.

Monitoring:

- ✓ Responsibility for monitoring the disposal policy rests with the designated officer. The policy will be reviewed annually or more often as required.

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

For M/s. VARDHAMAN CAPITAL PVT.LTD.

For Vardhaman Capital Pvt.,Ltd.

Director

(Anup Kumar Khandelwal)

Designated Officer