

# 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	31 <sup>st</sup> Dec 2023
Policy Approved by	Board of Directors
Policy approved on	4 <sup>th</sup> 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 at 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 stock 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.

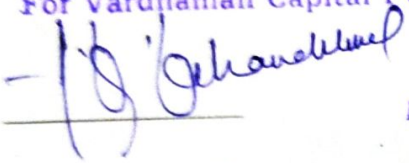
### Business Continuity Planning (BCP) and Disaster Recovery Site (DRS)

- 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.



Director.

Designated Officer

(Anup Kumar Khandelwal)

Dated: - 31/12/2024



# Vardhaman Capital Private Limited

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



CERTIFIED TRUE COPY OF THE RESOLUTION PASSED AT THE BOARD MEETING OF "VARDHAMAN CAPITAL PRIVATE LIMITED" AT THE REGISTERED ADDRESS -25, SWALLOW LANE 2<sup>ND</sup> FLOOR, KOLKATA-700001 HELD ON 04<sup>TH</sup> 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:

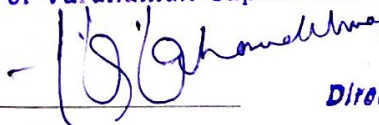
- [Firewall- Sophos]: [HAS BEEN SETUP TO PROTECT THE WHOLE SYSTEM FROM ANY OUTSIDE VIRUS/HACKERS/MALWARES/UNAUTHORISED PENITRATION THROUGH INTERNET ]
- [Server ]: [SERVER IS INSTALLED TO HANDLE CTCL AND OTHER IMPORTANT FRONT END AND BACK END ACTIVITIES INCLUDING OUTSOURCES CLOUD BASED SERVERS . TO RUNNING THE WHOLE PROCESS THE SERVER ARE MUST.]
- [Networking]: [THE NETWORKING 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	31 <sup>st</sup> Dec 2023
Policy Approved by	Board of Directors
Policy approved on	4 <sup>th</sup> 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.

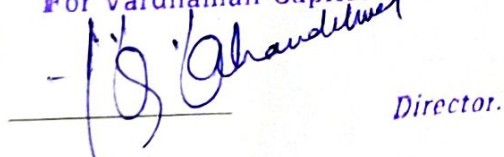
### **Employee Responsibilities**

- 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	31 <sup>st</sup> Dec 2023
Policy Approved by	Board of Directors
Policy approved on	4 <sup>th</sup> 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.



- 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	31 <sup>st</sup> Dec 2023
Policy Approved by	Board of Directors
Policy approved on	4 <sup>th</sup> 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.

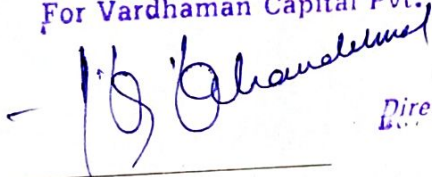
#### **Monitoring:**

- ✓ 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

# **VARDHAMAN CAPITAL PVT.LTD**

## **DATA LEAKAGE POLICY**

**Circular: - Ref. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018**

<b>Policy created by</b>	<b>Designated Officer</b>
<b>Policy reviewed by</b>	<b>Technology Commitee</b>
<b>Policy reviewed on</b>	<b>31<sup>st</sup> Dec 2023</b>
<b>Policy Approved by</b>	<b>Board of Directors</b>
<b>Policy approved on</b>	<b>4<sup>th</sup> Jan 2024</b>

**Version - 1.0**



## Purpose

This policy is a guide in identifying and gaining an understanding of the components that make up the information security system to manage risk to systems, assets, data, and capabilities.

## Scope

Data Leakage Policy (DLP) is a set of technologies and business policies to make sure end-users do not send sensitive or confidential data outside the organization without proper authorization. DLP enforces remediation with alerts, encryption, and other protective actions to prevent end users from accidentally or maliciously sharing data that could put the organization at risk. Sensitive information might include financial records, client data, credit card / debit card data, or other protected information. The most common method that this data is leaked is via email.

## Policy

Data Leakage Policy (DLP) features and products enable your organization to locate, monitor and protect your sensitive content from loss or misuse. Through policy enforcement, the organization will be complying by minimizing risk and preventing unauthorized use of confidential information.

Data Leakage Policy (DLP) encompasses the processes and rules used to detect and prevent the unauthorized transmission or disclosure of confidential information. The purpose of this procedure is to establish a framework of controls for classifying and handling the organization's data based on the data's level of sensitivity, storage location, value, etc. Confidential data can reside on or in a variety of mediums (pictures, paper documents, shred bins, physical servers, virtual servers, databases, file servers, personal computers, point-of-sale devices, USB drives and mobile devices) and can move through a variety of methods (human, network, wireless, etc.). The organization relies on a variety of DLP strategies and solutions to prevent data loss. The organization's DLP strategies and solutions are reevaluated regularly to ensure their relevancy and effectiveness. This security procedure applies to all the employees and users of the organization. Individuals working for the organization internally or externally are subject to the same rules when they are using the organization's information technology resources or have any means of access to data that has been classified as confidential or private.

### • Best Practices

- The sender will receive an Outlook message when an email is sent that contains sensitive information. Faculty and staff can still manually encrypt any email.
- Do not forward email you receive that contains sensitive information. If it is required to do so, redact the sensitive information before replying.
- Seek alternate means of transmitting the sensitive data. (secure web applications, etc.)

### • Data classification

In the context of information security, is the classification of data based on its level of sensitivity and the impact to the organization should that data be disclosed, altered or destroyed without authorization. Classification of data will aid in determining baseline security controls for the protection of the data. All organizational data is classified into one of three sensitivity levels (tiers), or classifications:



### Tier 1-

**Confidential Data** i.e., when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the organization. Unauthorized access to or disclosure of confidential information could constitute an unwarranted invasion of privacy and cause financial loss and damage to the organization's reputation and the loss of community confidence. The highest level of security controls should be applied. Access to Confidential data must be controlled from creation to destruction, and will be granted only to those persons affiliated with the organization who require such access in order to perform their job ("need-to-know"). Access to Confidential data must be requested for an individual and approved by the Technology Committee. Data access granted to individuals must be reviewed and authorized by the Data Owner who is responsible for the data.

Restricted Data is a particularly sensitive category of Tier 1-Confidential data. Restricted data is defined as 'any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transmission'.

### Tier 2-

**Internal/Private Data** i.e., when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the organization. By default, all information assets that are not explicitly classified as Confidential or Public data should be treated as Internal/Private data. A reasonable level of security controls should be applied to internal data. Access to Internal/Private data must be requested for an individual and approved by the Technology Committee. Data access granted to individuals must be reviewed and authorized by the Data Owner who is responsible for the data. Access to Internal/Private data may also be authorized to groups of persons by their job classification or responsibilities ("role-based" access), and may also be limited by one's department. Internal/Private Data is moderately sensitive in nature. Often, Tier 2 Internal/Private data is used for making decisions, and therefore it's important this information remain timely and accurate. The risk for negative impact on the organization should this information not be available when needed is typically moderate. Examples of Internal/Private data include such as financial reports, some research data.

### Tier 3-

**Public Data** i.e., when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the organization. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data. Public data is not considered sensitive; therefore, it may be granted to any requester or published with no restrictions. The integrity of Public data should be protected.

### Violations -

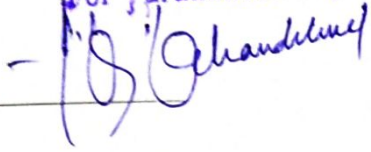
Anyone who knows or has reason to believe that another person has violated this procedure shall report the matter promptly to his/her supervisor, department head or the Technology Committee. After a violation of this procedure has been reported or discovered, the issue will be handled as soon as possible to reduce harm to the organization. Violators of this procedure may be subject to disciplinary action, up to and including the termination of employment depending on the severity of the violation or data breach.



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

Date: -31/12/2024

O F D N I

# VARDHAMAN CAPITAL PVT.LTD.

## ELECTRONIC STORAGE MEDIA DISPOSAL POLICY

Circular: - Ref. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018

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

Version - 1.2



## Purpose

The purpose of this policy is to define standards for proper data sanitization and/or disposal of electronic storage media that has (or may have) contained personal information at the Company's end and to emphasize the importance of protecting sensitive information and complying with legal and regulatory requirements during the disposal of electronic storage media.

## General/Definitions

- **Electronic Storage Media** - Any electronic device that can be used to store data. This includes but is not limited to internal and external hard drives, CDs, DVDs, Floppy Disks, USB drives, ZIP disks, magnetic tapes and SD cards.
- **Personal information** - An individual's first name and last name or first initial and last name in combination with one or more of the following data elements: social security number, driver's license number or state-identification card number, or financial account number, or credit or debit card number, with or without any required security code, access code, personally identifiable identification number or password, that would permit access to a resident's financial account.
- **Sensitive Information** - Data whose disclosure would not result in any business, financial or legal loss but involves issues of personally identifiable credibility, privacy or reputation. The security and protection of this data is dictated by a desire to maintain staff and student privacy.
- **Sanitizing Storage Media** -
  - Disposal is defined as the act of discarding media with no other sanitization considerations. Examples of Disposal include discarding paper in a recycling container, deleting electronic documents using standard file deletion methods and discarding electronic storage media in a standard trash receptacle.
  - Clearing is defined as a level of sanitization that renders media unreadable through normal means. Clearing is typically accomplished through an overwriting process that replaces actual data with 0's or random characters. Clearing prevents data from being recovered using standard disk and file recovery utilities.
  - Purging is defined as a more advanced level of sanitization that renders media unreadable even through an advanced laboratory process. In traditional thinking, Purging consists of using specialized utilities that repeatedly overwrite data; however, with advancements in electronic storage media, the definitions of Clearing and Purging are converging. For example, purging a hard drive manufactured after 2001 only requires a single overwrite. For the purpose of this Policy, Clearing and Purging will be considered the same. Degaussing is also an acceptable method of Purging electronic storage media
  - Destroying is defined as rendering media unusable. Destruction techniques include but are not limited to disintegration, incineration, pulverizing, shredding and melting. This is a common sanitization method for



single-write storage media such as a CD or DVD for which other sanitization methods would be ineffective. This is also a common practice when permanently discarding hard drives.

- **Data Wiping -**

- **Identify the Media:** Clearly identify the electronic storage media that needs to be wiped. Ensure that you are working with the correct device.
- **Backup Important Data:** Before initiating the data wiping process, backup any important data if necessary. Ensure that critical information is securely stored elsewhere.
- **Disconnect from Network:** Disconnect the electronic storage media from any network connections to prevent remote access during the wiping process.
- **Choose Wiping Method:** Select an appropriate wiping method based on the type of storage media. Common methods include overwriting, cryptographic erasure, or using specialized software tools. Choose a method that complies with your organization's security policies.
- **Use Certified Software:** If using software for data wiping, ensure that it is certified and recognized for secure data erasure.
- **Follow Software Instructions:** If using a software tool, follow the step-by-step instructions provided by the software vendor. This may involve creating a bootable disk or USB drive, selecting the target storage media, and initiating the wiping process.
- **Verify Completion:** After the wiping process is complete, use the software's verification features to ensure that all data has been successfully erased. Some tools provide a certificate or report confirming the completion of the process.
- **Physically Label or Tag:** Physically label or tag the wiped media to indicate that it has undergone the data wiping process. This helps in tracking and inventory management.
- **Record Details:** Maintain a record of the data wiping process, including the date, time, method used, and any relevant details. This documentation may be required for compliance purposes.
- **Secure Storage or Disposal:** If the storage media will be reused, store it securely. If it will be disposed of, follow the organization's disposal procedures, ensuring that it is done securely and in compliance with environmental regulations.
- **Consider Cryptographic Erasure for SSDs:** For SSDs, consider using cryptographic erasure methods that leverage the built-in encryption features of the device. This can be more effective than traditional overwriting methods.

### Organizational Scope

This policy applies to all personnel who have responsibility for the handling and proper disposal of electronic storage media at Company.



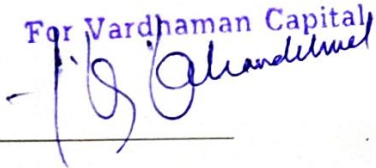
## Policy Content and Guidelines

- All electronic storage media should be sanitized (Cleared/Purged) prior to sale, donation, being moved to unsecured storage (for spare parts), or transfer of ownership. A transfer of ownership may include transitioning media to another individual or department at the Company or replacing media as part of a lease agreement.
- All electronic storage media must be destroyed when it has reached the end of its useful life and/or when other sanitizing methods are not effective (e.g. single-write media or media that is permanently write protected), provided that the destruction does not conflict with Company data retention policies or any regulatory requirements (e.g. electronic discovery).

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.**

## **INTERNET ACCESS POLICY**

Circular: - Ref. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018

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

**Version - 1.2**



## Objective

Our organisation recognizes that use of the Internet and e-mail is necessary in the workplace, and employees are encouraged to use the Internet and e-mail systems responsibly, as unacceptable use can place Company and others at risk. This policy outlines the guidelines for acceptable use of Company's technology systems. This policy helps ensure network security, protect sensitive information, and promote responsible and productive use of internet resources.

## Scope

This policy must be followed in conjunction with other policies governing appropriate workplace conduct and behaviour. Any employee who abuses the company-provided access to e-mail, the Internet, or other electronic communications or networks, including social media, may be denied future access and, if appropriate, be subject to disciplinary action up to and including termination. Company complies with all applicable central, state and local laws as they concern the employer/employee relationship, and nothing contained herein should be misconstrued to violate any of the rights or responsibilities contained in such laws.

Questions regarding the appropriate use of Company's electronic communications equipment or systems, including e-mail and the Internet, should be directed to your supervisor or the information technology (IT) department.

## Policy

Company has established the following guidelines for employee use of the company's technology and communications networks, including the Internet and e-mail, in an appropriate, ethical and professional manner.

### **Confidentiality and Monitoring**

- All technology provided by Company, including computer systems, communication networks, company-related work records and other information stored electronically, is the property of the Company and not the employee. In general, use of the company's technology systems and electronic communications should be job-related and not for personal convenience. Company reserves the right to examine, monitor and regulate e-mail and other electronic communications, directories, files and all other content, including Internet use, transmitted by or stored in its technology systems, whether onsite or offsite.
- Internal and external e-mail, voice mail, text messages and other electronic communications are considered business records and may be subject to discovery in the event of litigation. Employees must be aware of this possibility when communicating electronically within and outside the company.

### **Appropriate Use**

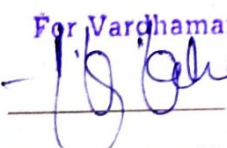
- Company employees are expected to use technology responsibly and productively as necessary for their jobs. Internet access and e-mail use is for job-related activities; however, minimal personal use is acceptable.
- Employees may not use Company's Internet, e-mail or other electronic communications to transmit, retrieve or store any communications or other content of a defamatory, discriminatory, harassing or pornographic nature. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference may be transmitted. Harassment of any kind is prohibited.

- Disparaging, abusive, profane or offensive language and any illegal activities—including piracy, cracking, extortion, blackmail, copyright infringement and unauthorized access to any computers on the Internet or e-mail—are forbidden.
- Copyrighted materials belonging to entities other than Company may not be transmitted by employees on the company's network without permission of the copyright holder.
- Employees may not use Company's computer systems in a way that disrupts its use by others. This includes sending or receiving excessive numbers of large files and spamming (sending unsolicited e-mail to thousands of users).
- Employees are prohibited from downloading software or other program files or online services from the Internet without prior approval from the IT department. All files or software should be passed through virus-protection programs prior to use. Failure to detect viruses could result in corruption or damage to files or unauthorized entry into company systems and networks.
- Every employee of Company is responsible for the content of all text, audio, video or image files that he or she places or sends over the company's Internet and e-mail systems. No e-mail or other electronic communications may be sent that hide the identity of the sender or represent the sender as someone else. Company's corporate identity is attached to all outgoing e-mail communications, which should reflect corporate values and appropriate workplace language and conduct.
- Every employee should emphasize the importance of maintaining strong and secure passwords for internet access and encourage regular password updates and provide guidelines for creating strong passwords.

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.

## NETWORK SECURITY POLICY

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

Version - 1.0

## Purpose

The purpose of this Network Security Policy is to establish guidelines and procedures to secure the network infrastructure, data, and communication systems of our Company. This policy aims to mitigate risks, protect sensitive information, and ensure the availability and reliability of network resources.

## Scope

This policy applies to all employees, contractors, vendors, and any other individuals who have access to the stock brokerage firm's network infrastructure and systems.

## Policy Guidelines

### **Access Control**

- Access to the network and systems shall be granted based on job responsibilities.
- User accounts must be unique to individuals and tied to specific job roles.
- Access permissions will be reviewed regularly and adjusted as needed.

### **Authentication and Passwords**

- Strong, unique passwords are required for all user accounts.
- Multi-factor authentication (MFA) is mandatory for accessing sensitive systems.
- Passwords must be changed at regular intervals.

### **Network Monitoring**

- Network traffic will be monitored for abnormal patterns and potential security threats.
- Regular audits of network logs will be conducted to identify and respond to suspicious activities.

### **Firewall Configuration**

- Firewalls must be configured to restrict unauthorized access and protect against external threats.
- Regular reviews of firewall rules and configurations will be conducted.

### **Data Encryption**

- All sensitive data transmitted over the network must be encrypted using secure protocols.
- Virtual Private Network (VPN) connections are required for remote access.

### **Wireless Network Security**

- Wireless networks must be secured with strong encryption and authentication mechanisms.
- Guest Wi-Fi networks should be isolated from the main network.

### **Incident Response Plan**

- An incident response plan will be established to promptly address and mitigate security incidents.
- Employees shall be trained on reporting security incidents and breaches.

### **Remote Access Security**

- Remote access to company networks must adhere to the same security standards as on-site access.
- Secure connections, such as VPNs, must be used for remote access.



## **Vendor Security**

Third-party vendors with network access must comply with security standards and undergo periodic security assessments.

## **Compliance and Legal Considerations**

### **Regulatory Compliance**

The network security policy will adhere to relevant financial regulations and industry standards.

### **Audit and Assessment**

Periodic audits and security assessments will be conducted to ensure compliance with this policy.

### **Employee Responsibilities**

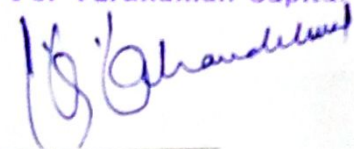
Employees are responsible for using the network resources in a secure and responsible manner.

Any suspicious activity or potential security vulnerabilities must be reported promptly.

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.

## STANDARD OPERATING PROCEDURE

Policy created by	Compliance Team
Policy reviewed by	Designated Officer
Policy reviewed on	31 <sup>st</sup> Dec 2023
Policy Approved by	Board of Directors
Policy approved on	4 <sup>th</sup> Jan 2024

Version - 1.2



## Cyber Security incident handling process document:

Cyber security incident management is not a linear process; it's a cycle that consists of a preparation phase, an incident detection phase and a phase of incident containment, mitigation and recovery. The final phase consists of drawing lessons from the incident in order to improve the process and prepare for future incidents.

Drawing up a cyber security incident response plan is an important first step of cyber security incident management. It is also crucial that management validates this plan and is involved in every step of the cyber security incident management cycle.

### The following elements should be included in the cyber security incident response plan:

#### **Identification of the assets that need to be protected:**

- ✓ Identification and assignment of responsibilities in the context of a cyber-security incident;
- ✓ In house capabilities or contracts with external experts for incident response and/or forensic investigation in case of an actual cyber security incident;
- ✓ The equipment and technology to detect and address a cyber-security incident;
- ✓ A basic containment strategy:
  - Disconnect the systems immediately in order to recover as quickly as possible?
  - Or take the time to collect evidence against the cybercriminal who perpetrated the system?
- ✓ A communication strategy for management and for authorities such as Depository and SEBI.

A good cyber security incident response plan can make the difference between a cyber-security incident and a cyber-security crisis. The pace at which we are able to recognize, analyse and respond to an incident will influence the damage done and the cost of recovery. Such a cyber-security incident response plan should not be limited to technology. Processes, people and other aspects of organization are also important elements to take into consideration.

### Important terms to be known for Cyber Security incident handling:

- ✓ **Cyber Security Event** - A cyber security change that may have an impact on our operations (including mission, capabilities, or reputation).
- ✓ **Cyber Security Incident** - A single or a series of unwanted or unexpected cyber security events that are likely to compromise our operations.
- ✓ **Cyber Security Incident Management** - Processes for preparing, for detecting, reporting, assessing, responding to, dealing with and learning from cyber security incidents.

### Basic Principles for examine the cyber security incidents:

- ✓ **There is no simple one-size-fits-all solution** -When it comes to Cyber Security there is no one-size-fits-all solution. What will work for us will depend on its mission and goals, the kind of infrastructure and information we are protecting, available resources, etc. Finally, recognise that some techniques will only be learned with time and experience.
- ✓ **Top management's commitment** - Cyber security incidents are a risk that should be incorporated in the overall risk management policy of company. Furthermore, managing cyber security incidents does not just mean applying technology. It also requires the development of a plan that is integrated into the existing processes and structures, so that it enables rather than hinders critical business functions. Therefore, top management should be



actively involved in defining a cyber security prevention and incident response plan, because top management's explicit support through appropriate internal communication and the allocation of personnel and financial resources is key to the success of the plan. The Designated Officer will be aware both of the risks of cybercrime and of his own exemplary role in encouraging all employees of company to assume their responsibility.

- ✓ **Involve every employee of the Company** - It is often said that humans are the weakest link when it comes to cyber security. Having said that, it is also important to realise that the employee of company have great potential to help detect and identify cyber security incidents. Make sure that every employee of our company is aware of the cyber security incident response plan and of their own role within it; even if this just means informing the right person.
- ✓ **Keep an offline copy of the documents need during an incident** - We have to keep in mind that when a cyber-security incident occurs, we may not always have access to the files on our computer. It is always a good idea to keep a hard copy/offline copy of any document we are likely to need during a cyber-security incident or crisis.
- ✓ **Don't link backups to the rest of the system** - When it comes to backups, it is not only crucial to have them. It is also very important to have a backup that is not linked in any way to the rest of the system. If the backup is linked to the system, chances are that the infection of the system also spreads to the backup, which makes the backup useless.
- ✓ **The importance of logging and keeping those logs during a certain time (up to 6 months)** - Logs can help to trace back the origin of the cyber security incident. This is not only important to be able to identify the cybercriminal; it will also help the company to get back to business as soon as possible.
- ✓ **Ensure to take all legal aspects into account when managing a cyber-security incident** - Evidence will only be admissible in Police or cyber security cell if it has been collected in respect of all applicable laws and regulations.
- ✓ **Document every step of a cyber-security incident** - Ensure to note down any action that is taken, such as the reporting of the incident, the collecting of evidence, conversations with users, system owners and others, etc. When something goes wrong it may allow looking back and evaluating where and why the problem started. Furthermore, documenting the cyber security incident response will ensure that the knowledge regarding what is going on is not just in a few people's heads.

### Cyber Security Action / Response Mechanism

#### ✓ **IDENTIFY THE ASSETS AND POTENTIAL THREATS -**

- When hit by an incident the first questions that will arise are: which assets are at risk?
- And which of those assets are vital for the business's activity?

We will have to decide which assets need attention first in order to remain in business and keep the damage to business as low as possible. That's why it is crucial to identify, document and categorise 'vitals': the assets of company depend on to conduct its core activities. This will help to identify where to apply which protective measures and to take quick and justified decisions during the incident management process. The following will give an idea of what those 'vitals' could be: management, company, processes, knowledge (e.g. intellectual property has been stolen), people, information (e.g. data sets have been stolen or altered), and applications (e.g. website is down or defaced, infrastructure (e.g. system and/ or network connections are down), financial capital (e.g. bank accounts). It's also a good idea to identify vulnerabilities and potential threats.



## ✓ HOW TO IDENTIFY, DOCUMENT AND CATEGORISE VITALS, VULNERABILITIES AND POTENTIAL THREATS? -

- **Identify the business and the resources that need to be protected**
  - Determine which are core business activities that enable our company to exist, to achieve its corporate objectives and generate income.
  - For each of those activities, identify which IT systems (databases, applications, control systems) and network connections are supporting them.
  - Determine also where these IT systems are located: on own servers or in the cloud
  - When identifying these assets, don't forget flows of information to third parties (suppliers, clients, etc.).
- **Determine what the crown jewels are**
  - Determine now which assets, data, processes or network connections are so important for our company that we lose (control of) them, we will be in big trouble or even out of business?
- **Assign business priorities for recovery**
  - This priority will determine the order in which the systems will be re-established. In most cases the underlying network will need the highest priority, as this is not only the path for system administrators to reach the assets but also the path that cyber criminals use to attack the systems. As long as criminals can use the network connections, any other recovery activity might be undone by them. When assets have equal priorities, parallel recovery activities might be considered.
- **Document how the systems work and keep this documentation up to date**

Ensure that the way systems work is documented and that this information is kept up to date and available on the incident response team's documentation systems.

### Especially needed documents are:

- **Network Scheme** displaying the network architecture with internal network segmentation and the different gateways to external networks, DMZ, VPN, IP-address ranges used. This scheme should also include the different security devices in place that might contain logging information of network activity (firewalls, (reverse) proxy servers, intrusion detection systems, security incident event management systems). For larger companies with complex networks, it is also necessary to have a high-level version of the network architecture so that one can quickly get an idea of the network in case of emergency.
- **Equipment and services inventory.** This inventory will include, for the vital assets in the environment, all the different servers and the network components used for delivering the different corporate services. As some of these (physical) servers might be servicing multiple business functions it is important to know per server which services are running on them.
- **Account and access lists.** At all times it is important to know who has the right to access, use and or manage the network and the different systems in it. This will allow to detect any strange or abused accounts during an incident

## ✓ ASSIGNING RESPONSIBILITIES AND CREATING A CYBER SECURITY INCIDENT RESPONSE TEAM -

It is important that the roles and responsibilities in case of a cyber-security incident are documented in the cyber security incident response plan.

When drafting the description of these roles and responsibilities, we should ask the following questions:



- Who is the internal contact point for cyber security incidents? And how can he be contacted?
- What are the different incident response tasks? And who is responsible for doing what?
- Who is managing the incident from business/technical side? This should be someone within the company with decision-making authority, who will follow the incident from the beginning until the end.
- Who will communicate with senior management?
- Who can engage the external incident response partner?
- Who can file a complaint with law enforcement/inform the regulatory bodies?

In order to adequately address a cyber-security incident, different skills are needed to take up the different responsibilities and necessary roles of an efficient incident response.

<u>SKILLS</u>	<u>RESPONSIBILITIES</u>	<u>ROLES</u>
Incident management	Manage the cyber security incident from the moment of its detection until its closure.	Cyber security Incident response manager - Designated Officer
Business decision capability	Assessing the business impact and act upon it. Engage the right resources. Take decisions on how to proceed e.g. decide if the internet connection of a compromised system can be shut down and when is the most appropriate time. Decide when to start clean-up activities. Decide whether to file a complaint or not.	Management
Network management capabilities	Technical know-how on network (firewall, proxies, IPS, routers, switches). Analyse, block or restrict the data flow in and out of the network. IT operations Information security and business continuity	IT technical support staff
Workstation and server administrator capabilities (admin rights)	Analyse and manage compromised workstations and servers.	IT technical support staff
Legal advice	Assess the contractual and judicial impact of an incident. Guarantee that incident response activities stay within legal, regulatory and our boundaries. Filing a complaint.	Designated Officer
Communication skills	Communicate in an appropriate way to all concerned stakeholder groups and answer clients immediately	Designated Officer
Physical security	Handle the aspects of the incident that are linked to <ul style="list-style-type: none"> <li>• the physical access to the premises</li> <li>• The physical protection of the cyber infrastructure.</li> </ul>	IT technical support staff

✓ **CYBER INCIDENT RESPONSE TEAM** - In an ideal world, every company should have an incident response team that is convened whenever there is an incident. Of course, the size of the company determines the size and the structure of the incident response team. Smaller companies that do not have the resources for an actual team could designate a first responder – ideally someone with business decision capability – amongst their personnel. In case of a cyber-security incident, he or she should contact external help, but remains the person ultimately responsible for the incident response within the company. The composition of this incident response team will be



determined by the different skills that are needed to handle an incident. For smaller companies, some of these skills may have to be found outside the company and contacted by the first responder.

- ✓ **HARDWARE AND SOFTWARE FOR CYBER SECURITY INCIDENT MANAGEMENT** - To improve the maturity and efficiency of the incident response team, the appropriate tools need to be in place. It is important that the incident response team disposes of autonomous systems and tools that permit them to take care of an incident even if the corporate network has been compromised. This means that when the systems or networks are no longer available, the system of the incident response team still is. Incident procedures and contact lists have to be available on these systems.

### **CLASSIFICATION OF INCIDENTS ON THE PARAMETERS OF RISK CATEGORIES:**

- ✓ Cyber security incident response has become an important component of information technology (IT) programs. Cyber security-related attacks have become not only more numerous and diverse but also more damaging and disruptive. New types of security-related incidents emerge frequently. Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services.
- ✓ The incident response process has several phases. The initial phase involves establishing and training an incident response team, and acquiring the necessary tools and resources. During preparation, we also attempt to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of risk assessments. However, residual risk will inevitably persist after controls are implemented. Detection of security breaches is thus necessary to alert us whenever incidents occur. In keeping with the severity of the incident, we can mitigate the impact of the incident by containing it and ultimately recovering from it. During this phase, activity often cycles back to detection and analysis—for example, to see if additional hosts are infected by malware while eradicating a malware incident. After the incident is adequately handled, we issue a report that details the cause and cost of the incident and the steps should take to prevent future incidents
- ✓ Periodic risk assessments of systems and applications should determine what risks are posed by combinations of threats and vulnerabilities. This should include understanding the applicable threats, including organization-specific threats. Each risk should be prioritized, and the risks can be mitigated, transferred, or accepted until a reasonable overall level of risk is reached. Another benefit of conducting risk assessments regularly is that critical resources are identified, allowing staff to emphasize monitoring and response activities for those resources.
- ✓ We shall carry out risk assessment to examine the incident and classify them into High / Medium / Low risk as per the cyber security handling document and should take necessary action to minimize the loss and destruction and to prevent the company from such threats and vulnerabilities.

### **REPORTING OF INCIDENT TO CERT - IN**

We should always seriously consider reporting cyber-security incidents to the Indian Computer Emergency Response Team, CERT-IN. Reporting to the CERT-IN is vital in determining whether the incident is isolated or not and allows to keep track of threat trends in India. The CERT-IN will be able to provide some information and advice related to the incident that can help the victim to take effective countermeasures. Furthermore, the information provides may help to prevent attacks on other computer systems.



The following information should be reported:

- ✓ Contact details
- ✓ The type of the incident
- ✓ The date of the incident
- ✓ Is the incident ongoing?
- ✓ How did company notice this incident?
- ✓ What's the impact of the incident?
- ✓ Have company already taken actions or measures? If so, which ones?
- ✓ Does company have logs or other useful data?
- ✓ Who have company already informed?
- ✓ What company expecting from the report?

We shall submit the overall details of the incident to Depository and SEBI whether the same has been reported or not reported to CERT-IN. Furthermore, if the incident is not reported to CERT-IN, members shall submit the reasons for the same to the Depository and SEBI.

### FILING A COMPLAINT WITH LAW ENFORCEMENT AGENCIES

Communication to law enforcement authorities must be made as soon as possible after discovery of the cyber security incident, given the volatility of traces and actions that need to be taken (Internet identification, etc.). For prosecution to be successful, the chain of custody needs to be preserved in a legally accepted manner, which requires the evidence to be preserved immediately after the detection of the incident.

Judicial authorities need to possess the available information regarding the incident in order to make a qualification of the offence and proceed with the identification of the suspect. The information that should be communicated to the police in case of Internet fraud (a 'traditional' crime committed by electronic means) may not be entirely the same as the information the police needs in case of IT crime (hacking, sabotage, espionage). In the course of the investigation, additional information will be requested, collected and searched for by the investigators. It is of the outmost importance that the services provide the assistance and input requested by law enforcement, to help advance the investigation.

- ✓ **POLICE:** If our company is impacted by an incident and as such has been the victim of an offence; we can decide to lodge a complaint. By default, we should go to the local police station or the police station of choice. For more complex cases, the local police will get support from the CERT-IN / MHA / Cybercrime police, specialised in dealing with IT crime (hacking, sabotage, espionage). If the case concerns a critical infrastructure or a sector with specific rules, a special procedure may apply.
- ✓ **CYBER SECURITY CELL:** It is also possible to file a complaint directly with a Cyber security cell. This should be an exceptional measure. Furthermore, we will probably have to advance the costs of the investigation, because the Cyber security cell is conducting it at specific demand.
- ✓ **INFORMATION TO DEPOSITORY AND SEBI:** We shall submit details on whether the incident has been registered as a complaint with law enforcement agencies such as Police or cyber security cell. If yes, details need to be provided to Depository and SEBI. If not, reason for not registering complaint should also be provided to Depository and SEBI.



- ✓ **INFORMATION TO DOS-MIRSD and CISO OF SEBI:** The details of reported incidents and submission to various agencies by we shall also be submitted to Division Chiefs (in charge of divisions at the time of submission) of DOS-MIRSD and CISO of SEBI.

### Quarterly Reporting of Cyber Incidents:

The Designated Officer of our company (appointed in terms of para 6 of the SEBI Circular dated December 03, 2018) shall continue to report any unusual activities and events within 24 hours of receipt of such Information as well as submit the quarterly report on the cyber-attacks & threats within 15 days after the end of the respective quarter to the respective depositories and exchanges.

**Most Common Incident types and how to neutralise them:**

INCIDENT TYPE	DEFINITION	POSSIBLE TARGET	VULNERABILITIES THAT MIGHT BE EXPLOITED	POSSIBLE REACTIONS
Social Engineering: (Spear) phishing, vishing (phone phishing)	Manipulating and tricking someone into revealing information that (e.g., password for financial information) that can be used to attack systems or networks	Management	As deems fit.	As deems fit.
(spear) phishing, vishing (phone phishing)	Attempt to acquire sensitive information (e.g. customer logins & passwords) from customers by impersonating a legitimate and trusted person or. Vardhaman Capital Pvt Ltd	Management	As deems fit.	As deems fit.
Unauthorised access	When a person gains logical or physical access without permission to a network, system, application, data, or other IT resource.	Customer information Credit card information Applications creating or processing payments Websites and services	Password cracked or sniffed Unpatched system vulnerabilities Social engineering Careless users or weak procedures	Patch vulnerabilities or block exploitation Check for malware (rootkits, backdoors, Trojans) Change passwords or inactivate accounts Forensic evidence gathering Block (network) access to the targeted resources
Denial of service	Any attack that prevents or impairs the authorised use of networks, systems or	Mail system Network appliances	Spam filter weaknesses Unpatched system	Block traffic Contact ISP Disconnect



	applications by exhausting resources.	Application servers Web sites and services	vulnerabilities Weak configuration of systems or appliances	infected system(s)
Malicious code attack	A malicious code attack is any (large- scale) infection or threat of infection by a virus, worm, Trojan horse, or other code-based malicious entity	Any server or even appliance in the network could be the target of a malicious code attack, but some systems have a higher risk profile (e.g. systems directly or indirectly connected to the outside world). Any end user workstations could be targeted via e-mail, USB storage devices, visits to web sites and web applications, etc.	Unpatched system vulnerabilities (e.g. Flash or JavaScript) Anti-virus not installed, not active or signature file not up to date Inappropriate or imprudent user behaviour (e.g. using infected USB memory device)	Block malicious web traffic Apply patches Update anti-virus signature files. Run virus clean-up tool if available. Run vulnerability assessment tool to list vulnerable resources Completely reinstall infected system Shut down vulnerable services Shut down or disconnect infect system(s)
Inappropriate usage	An inappropriate usage incident is any incident involving an internal employee or contractor violating a code of conduct or a computer policy. Inappropriate behaviour is not always malicious and targeted. Sometimes a user will simply act carelessly or even be completely unaware of the standard operating procedure or code of conduct he / she has infringed. The	Payment transactions Credit card information Customer commercial and personal information Confidential information in general	Weak management or control of confidential data Bad user password management Lack of segregation of duties, accumulation of access rights Lack of application security or monitoring Lack of procedures or control to	Inform and get advice from Compliance and/or the legal department Inactivate users or withdraw access rights Make forensic copies of logs and other crucial information to trace and prove what happened

	inappropriate behaviour will sometimes constitute a serious security incident in itself, but it can also be the cause or trigger of a serious incident (like malware infection, loss of critical data)		enforce policies and codes of conduct	Check logs and other information for traces of the infringement
Fraud	Fraud is a kind of inappropriate behaviour that is inherently malicious in nature, and aimed at personal enrichment by abusing company systems, applications or information.	Management	As deems fit.	As deems fit.
Data loss or theft	This is an incident that involves the loss or theft of confidential information. Information can be confidential because of the value it has for the company, or because it is protected by internal or external regulations. Data loss incidents can have a big financial impact, due to possible financial liability or damage done to the company image, should the information itself or the fact that it has been lost become public or known to the wrong people.	Personal information about employees or customers (protected by privacy laws or concerns) Credit card information Customer commercial information Confidential balance sheet information Confidential information about company strategy, on-going projects and decisions, etc	Personal information about employees or customers (protected by privacy laws or concerns) Credit card information Customer commercial information Confidential balance sheet information Confidential information about company strategy, on-going projects and decisions, etc.	Assess the level of protection of the data, if any (encryption, password protection, specific device required to read the data) Inform and get advice from Compliance and/or the legal department or from the external legal adviser Inform Communications department and management, define a communication strategy Inform the owner of the lost or

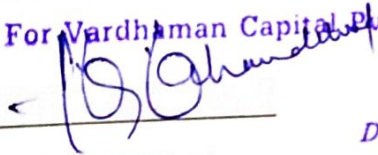


				stolen data
Brand abuse	This is an incident where someone is abusing the brand and registered trademarks.	Registration of DNS names containing the brand Spoofing of website designs Spoofing of e-mail addresses and e-mail templates	Not applicable	Inform police (in case of theft) Request a takedown of the website Inform customers about the existence of this

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

For M/s. VARDHAMAN CAPITAL PVT.LTD.

For Vardhaman Capital Pvt. Ltd,



Director.

Designated Officer

(Anup Kumar Khandelwal)

Dated:- 31/12/2024