Murari Securities Limited

BACKUP POLICY

Policy created by	**Designated Officer**
Policy reviewed by	**Technology Committee**
Policy reviewed on	**31/12/2023**
Policy Approved by	**Board of Directors**
Policy approved on	**17/01/2024**

Version – 1.0

Purpose

The purpose of this Backup Policy is to establish guidelines and procedures for the regular and secure backup of critical data at our Company. This policy aims to ensure the availability, integrity, and recoverability of data in the event of data loss, system failures, or unforeseen disasters.

Scope

This policy applies to all employees, contractors, and third-party vendors who have access to and are responsible for managing critical data within the stock brokerage firm.

Policy Guidelines

Data Classification

- Data will be classified based on its sensitivity and importance to the business.
- Backup strategies will be aligned with the classification of data.

Backup Frequency

- Critical data will be backed up regularly, with the frequency determined by the data's criticality and change rate.
- Full system backups will be performed periodically.

Backup Storage

- Backup data will be stored in secure, offsite locations to protect against on-site disasters.
- Multiple copies of backup data will be maintained to ensure redundancy.

Retention Period

- Backup retention periods will be established based on regulatory requirements, business needs, and data classification.
- Old backups will be periodically reviewed and purged in compliance with retention policies.

Encryption

- Backup data, both in transit and at rest, will be encrypted using industry-standard encryption algorithms.
- Encryption keys will be securely managed.

Testing and Verification

- Regular tests and verifications of backup and restore procedures will be conducted to ensure data recoverability.
- Testing will include both full and incremental backups.

Documentation

- Comprehensive documentation of backup procedures, schedules, and restoration processes will be maintained.
- Employees responsible for backup procedures will be adequately trained.

Monitoring and Alerts

- Backup systems will be monitored for any failures or anomalies.
- Alerts will be generated and promptly addressed to maintain the integrity of the backup process.

Compliance and Legal Considerations

Regulatory Compliance

- The backup policy will adhere to relevant financial regulations and industry standards.
- Regular audits will be conducted to ensure compliance.

Audit and Assessment

Periodic audits and assessments will be conducted to evaluate the effectiveness of the backup policy and procedures.

Employee Responsibilities

Employees are responsible for adhering to backup procedures and promptly reporting any issues or concerns related to data protection.

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.

Murari Securities Limited

_____

Designated Officer

Dated: - 17/01/2024

Murari Securities Limited

BCP AND RESPONSE MANAGEMENT POLICY

Policy created by	**Designated Officer**
Policy reviewed by	**Technology Committee**
Policy reviewed on	**31/12/2023**
Policy Approved by	**Board of Directors**
Policy approved on	**17/01/2024**

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.

Murari Securities Limited

_____

Designated Officer

Dated: - 17/01/2024

Murari Securities Limited

BRING YOUR OWN DEVICE POLICY

Policy created by	**Designated Officer**
Policy reviewed by	**Technology Committee**
Policy reviewed on	**31/12/2023**
Policy Approved by	**Board of Directors**
Policy approved on	**17/01/2024**

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

- 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.

Murari Securities Limited

_____

Designated Officer

Dated: - 17/01/2024

Murari Securities Limited

POLICY ON CYBER SECURITY AND CYBER RESILIENCE

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	**31/12/2023**
Policy Approved by	**Board of Directors**
Policy approved on	**17/01/2024**

Version – 1.3

Introduction

Our organization is a leading financial institution specializing in stock broking and depository participant services. Established [1999], we have emerged as a trusted partner in the financial market, providing comprehensive solutions to our clients.

- **Vision and Mission:**
  - **Vision:** To be a preferred choice for investors seeking reliable and innovative financial services.
  - **Mission:** To deliver exceptional value through cutting-edge technology, ethical practices, and customer-centric services.
- **Services:**
  - Stock Broking:
    - Equities Trading
    - Derivatives Trading
    - Currency Trading
    - Commodities Trading
  - Depository Participant Services:
    - Dematerialization (Demat) of Securities
    - Account Maintenance
    - Electronic Settlement of Trades
- **Technology Infrastructure** We leverage state-of-the-art technology to ensure seamless and secure trading experiences for our clients. Our robust trading platforms and advanced risk management systems contribute to the efficiency of our operations.
- **Regulatory Compliance:** As a registered stock broker and depository participant, we adheres to all regulatory requirements mandated by SEBI/Exchange(s)/Depository(s). We prioritize transparency and compliance in all our dealings.
- **Clientele:** Our diverse clientele includes retail investors, institutional clients, corporate, and HNIs. We are committed to understanding and addressing the unique financial needs of each client.
- **Awards and Recognition:** Our organization has received accolades for its excellence in the financial services industry. These recognitions underscore our commitment to delivering top-notch services.
- **Contact Information:** For inquiries or to learn more about our services, please contact us at: [Address] [Phone] [Email] [Website]
- **Social Responsibility:**Our organization is dedicated to social responsibility and community development. We actively participate in initiatives that contribute to the welfare of society.

Background

SEBI has issued circular No. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018and SEBI/HO/MIRSD/DOP/CIR/P/2019/109 dated October 15, 2019, SEBI/HO/MRD1/MRD1_DTCS/P/CIR/2022/68 dated May 20, 2022, SEBI/HO/MIRSD/TPD/P/CIR/2022/93 dated June 30, 2022 and

SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/032 dated February 22, 2023 providing guidelines on Cyber Security and Cyber Resilience. The objective of the said circular is to adapt to the rapid technological developments in Securities Market which have highlighted the need for robust Cyber and Cyber Resilience at the level of Stock brokers/Depository participants who are performing significant functions in providing services to the holder of Securities.

In order to protect the integrity of data and guard against breaches of Privacy and to comply with the applicable regulations our organization has framed a policy for implementation to meet the objectives.

Date of Implementation of the Circular

Circular shall be effective from April 1, 2019.

It is observed that the level of Cyber-attacks and threats attempt to compromise the Confidentiality, Integrity and Availability (CIA) of the computer systems, networks and databases (Confidentiality refers to limiting access of systems and information to authorized users, Integrity is the assurance that the information is reliable and accurate, and Availability refers to guarantee of reliable access to the systems and information by authorized users). Cyber Resilience is an organization's ability to prepare and respond to a cyber-attack and to continue operation during, and recover from, a cyber-attack

Accordingly, the following Policies & Procedures have been put in place

Governance

Risk management framework to manage risk to systems, networks and databases from cyber-attacks and threats.

- Identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems:
  - 'Identify' critical IT assets and risks associated with such assets.
  - 'Protect' assets by deploying suitable controls, tools and measures.
  - 'Detect' incidents, anomalies and attacks through appropriate monitoring tools/processes.
  - 'Respond' by taking immediate steps after identification of the incident, anomaly or attack.
  - 'Recover' from incident through incident management and other appropriate recovery mechanisms.

- As a Stock broker trading through APIs based terminal or acting as a depository Participants should refer best practices from international standards like ISO 27001, COBIT 5, etc., or their subsequent revisions, if any, from time to time.

  - ISO 27001 is an international standard for the establishment, implementation, maintenance, and continual improvement of an Information Security Management System. The standard is a joint effort by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC).
  - COBIT 5 is a framework from the Information Systems Audit and Control Association (ISACA) for the management and governance of information technology (IT). ... Achieve strategic goals by using IT assistance. Maintain operational excellence by using technology effectively. Keep IT-related risk at an acceptable level.

- The main benefit of implementing ISO 27001 is a systemic Information Security Management System that helps with the identification of critical information, the information security risk assessment of the system, and the implementation of security controls, all of which help to create a secure culture in the organization.
- ISO 27001 is beneficial for the organization in terms of its security.
- The five COBIT 5 principles are:
  - Meeting stakeholder needs
  - Covering the enterprise end to end
  - Applying a single integrated framework
  - Enabling a holistic approach
  - Separating governance from management

- We have designated Mr Ankush Dhyawala .to assess, identify, and reduce security and Cyber Security risks, respond to incidents establish appropriate standards and controls and direct the establishment and implementation of processes and procedures as per the Cyber Security Policy.
- A reporting procedure has been designed to facilitate communication of unusual activities and events to the Designated Officer in a timely manner.
- The Designated officer and the technology committee will periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen Cyber Security and cyber resilience framework.

- The technology committee are consisting of following members:

Sl. No.	Designation of the Members	Name of the Committee Members
1	CISO (Chief Information Security Officer)	
2	Designated Officer	
3	IT Head	
4	Compliance Head	
5	Any other employee(s) indulges in IT	

Identification

- We have identifiedand classified / designated critical assets based on their Sensitivity and criticality for business operations, services and data management. The critical assets include business critical systems, internet facing applications / systems, systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information (PII) data, etc. All the ancillary systems used for accessing/communicating with critical systems either for operations or maintenance are classified as critical system. Maintenance of up-to-date inventory of the hardware and systems and the personnel to whom these have been issued, software and information assets (internal and external), details of its network resources, connections to its network and data flows. Accordingly identify cyber risks, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.

- To this end, our organization is maintaining up-to-date inventory of its hardware and systems, software and information assets (internal and external), details of its network resources, connections to its network and data flows.

Protection

Access controls:

- Any access to systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. To identify the access we have granted access to IT systems, applications, databases and networks on a need-to-use basis and based on the principle of least privilege. Implement an access policy which addresses strong password controls for users' access to systems, applications, networks and databases.
- Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to thecritical systems, networks and other computer resources, should be subject to stringent Supervision, monitoring and access restrictions.

Physical Security:

- Physical access to the critical systems should be restricted to minimum and only to authorized officials. Physical access of outsourced staff/visitors should be properly supervised by ensuring at the minimum that outsourced staff/visitors are accompanied at all times by authorized employees. Access should be revoked immediately if the same is no longer required.
- Office premises should be physically secured and monitored by security guards.

Network Security Management:

- As a Stock Brokers / Depository Participants we have established baseline standards to facilitate Consistent application of security configurations to operating systems, databases, Network devices and enterprise mobile devices within their IT environment. The LAN and wireless networks should be secured within the premises.
- Adequate controls must be deployed to address virus / malware / ransom ware attacks.

Data security:

- Strong encryption methods to be used for identifying and encrypting the critical data. The confidentiality of information is not compromised during the process of exchanging and transferring information with external parties. The information security policy should also cover use of devices such as mobile phones, faxes, photocopiers, scanners, etc.

Hardening of Hardware and Software:

- Should deploy hardened hardware / software, including replacing default passwords with strong passwords and disabling or removing services identified as unnecessary for the functioning of the system. Open ports on networks and systems which are not in use should be blocked.
- Application Security in Customer Facing Applications: Application security for Customer facing applications offered over the Internet such as IBTs, portals containing sensitive or private information and Back office applications are paramount as they carry significant attack surfaces by virtue of being available publicly over the Internet for mass use. Measures to be taken for applications.

Patch management:

- Patch management procedures should include the identification, categorization and prioritization of patches and updates. An implementation timeframe for each category of patches should be established to apply them in a timely manner. Testing to be performed on security patches and updates, where possible, before deployment into the production environment so as to ensure that the application of patches do not impact other systems.

Disposal of data, systems and storage devices:

- Identify a Policy for disposal of storage media and systems. The critical data / Information on such devices and systems should be removed by using methods such as crypto shredding / degauss / Physical destruction as applicable.

Vulnerability Assessment and Penetration Testing (VAPT):

- We will carry out periodic vulnerability assessment and penetration testing (VAPT) which inter- aliaincludes all critical assets and infrastructure e components like Servers, Networking systems, Security devices, load balancers, other IT systems in order to detect security vulnerabilities in the IT environment and in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks.
- We will conduct VAPT at least once in a financial year. However, whose systems have been identified as "protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC),VAPT shall be conducted at least wice in a financial year. Further, only CERT-In empanelled organizations are required to engage for conducting VAPT.
- The final report on said VAPT should be submitted to SEBI after approval from Standing Committee on Technology (SCOT), within 1 month of completion of VAPT activity.
- Any gaps/vulnerabilities detected have to be remedied on immediate basis and compliance of closure off indings identified during VAPT shall be submitted to SEBI within 3 months post the submission of final VAPT report to SEBI .In addition, we should also perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which is acritical system or part of an existing critical system. Systems which are publicly available over the internet should also carry out penetration tests, at-least once a year, in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks that are exposed to the internet.

Monitoring and Detection:

- Establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events/ alerts and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices exposed to the internet should also be monitored for anomalies.

- Ensure high resilience, high availability and timely detection of attacks on systems and networks exposed to the internet, implement suitable mechanisms to monitor capacity utilization of its critical systems and networks that are exposed to the internet, for example, controls such as firewalls to monitor bandwidth usage.

Response and Recovery:

- Alerts generated from monitoring and detection systems should be suitably investigated in order to determine activities that are to be performed to prevent expansion of such incident of Cyber-attack or breach, mitigate its effect and eradicate the incident.

- The response and should have plans for the timely restoration of systems affected by incidents of cyber-attacks or breaches, for instance, offering alternate services or systems to Customers. Stock Brokers / Depository Participants should have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as specified by SEBI for Market Infrastructure Institutions vide SEBI circular CIR/MRD/DMS/17/20 dated June 22, 2012 as amended from time to time.

Sharing of Information:

- All Cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers / Depositories Participants shall be reported to Stock Exchanges / Depositories & SEBI within 6 hours of noticing / detecting such incidents or being brought to notice about such incidents. This information shall be shared to SEBI through the dedicated e-mail id: sbdp-cyberincidents@sebi.gov.in.
- The incident shall also be reported to Indian Computer Emergency Response team (CERT-In) in accordance with the guidelines / directions issued by CERT-In from time to time. Additionally, the Stock Brokers / Depository Participants, whose systems have been identified as "Protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.
- The quarterly reports containing information on cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers / Depository Participants and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities, threats that may be useful for other Stock Brokers / Depository Participants / Exchanges /Depositories and SEBI, shall be submitted to Stock Exchanges / Depositories within 15 days from the quarter ended June, September, December and March of every year.

Training and Education

Entities should conduct periodic training programs to enhance knowledge of IT / Cyber Security Policy and standards among the employees incorporating up-to-date Cyber Security threat alerts. Where possible, this should be extended to outsourced staff, vendors etc.

- The training programs should be reviewed and updated to ensure that the contents of the program remain current and relevant.

Systems managed by vendors, MIIs

- As a Stock Brokers / Depository Participants we have instructed the vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications from them to ensure compliance with the policy guidelines.

Periodic Audit

- The periodicity of audit for the purpose of compliance with Cyber Security and Cyber Resilience provisions for depository participants shall be annual.
- The periodicity of audit for the compliance with the provisions of Cyber Security and Cyber Resilience provisions for stock brokers, irrespective of number of terminals and location presence, shall be as under: (Type of stock broker as specified in SEBI circular CIR/MRD/DMS/34/2013 dated November 06, 2013)

    - For Type I - Annual
    - For Type II - Annual
    - For Type III - Half-year.

Advisory regarding Cyber security best practices

- **Roles and Responsibilities of Chief Information Security Officer (CISO)/ Designated Officer**:

  To define roles and responsibilities of Chief Information Security Officer (CISO) and other senior personnel. Reporting and compliance requirements shall be clearly specified in the security policy.

- **Measures against Phishing attacks/ websites:**
  - We need to proactively monitor the cyberspace to identify phishing websites w.r.tto domain and report the same to CSIRT-Fin/CERT-In for taking appropriate action.
  - Majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in email, can establish an essential pillar of defence. Additionally, the advisories issued by CERT-In/ CSIRT-Fin may be referred for assistance in conducting exercises for public awareness.
- **Patch Management and Vulnerability Assessment and Penetration Testing (VAPT):**
  - All operating systems and applications should be updated with the latest patches on a regular basis. As an interim measure for zero-day vulnerabilities and where patches are not available, virtual patching can be considered for protecting systems and networks. This measure hinders cybercriminals from gaining access to any system through vulnerabilities in end-of-support and end-of-life applications and software. Patches should be sourced only from the authorized sites of the OEM.
  - Security audit / Vulnerability Assessment and Penetration Testing (VAPT) of the application should be conducted at regular basis and in accordance with the Cyber Security and Cyber Resilience circulars of SEBI issued from time to time. The observation/ gaps of VAPT/Security Audit should be resolved as per the timelines prescribed by SEBI.
- **Measures for Data Protection and Data breach:**
  - To prepare detailed incident response plan.
  - Enforce effective data protection, backup, and recovery measures.
  - Encryption of the data at rest should be implemented to prevent the attacker from accessing the unencrypted data.
  - Identify and classify sensitive and Personally Identifiable Information (PII) data and apply measures for encrypting such data in transit and at rest.
  - Deploy data leakage prevention (DLP) solutions / processes.
- **Log retention:**

  Strong log retention policy should be implemented as per extant SEBI regulations and required by CERT-In and IT Act 2000. Advisable to audit that all logs are being collected. Monitoring of all logs of events and incidents to identify unusual patterns and behaviours should be done.

- **Password Policy/ Authentication Mechanisms:**
  - Strong password policy should be implemented. The policy should include a clause of periodic review of accounts of ex-employees Passwords should not be reused across multiple accounts or list of passwords should not be stored on the system.

- Enable multi factor authentication (MFA) for all users that connect using online/internet facility and also particularly for virtual private networks, webmail and accounts that access critical systems.
- Maker and Checker framework should be implemented in strict manner and MFA should be enabled for all user accounts, especially for user accounts accessing critical applications.

- **Privilege Management:**
  - Maker-Checker framework should be implemented for modifying the user's right in internal applications.
  - For mitigating the insider threat problem, 'least privilege' approach to provide security for both on-and off-premises resources (i.e., zero-trust models) should be implemented. Zero Trust is rooted in the principle of "trust nothing, verify everything." This security model requires strict identity verification for each and every resource and device attempting to get access to any information on a private network, regardless of where they are situated, within or outside of a network perimeter.
- **Cybersecurity Controls:**
  - Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses, block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.
  - Block the malicious domains/IPs after diligently verifying them without impacting the operations. CSIRT-Fin/CERT-In advisories which are published periodically should be referred for latest malicious domains/IPs, C&C DNS and links.
  - Restrict execution of "Power Shell" and "wscript" in enterprise environment, if not required. Ensure installation and use of the latest version of Power Shell, with enhanced logging enabled, script block logging and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.
  - Utilize host-based firewall to prevent Remote Procedure Call (RPC) and Server Message Block (SMB) communication among endpoints whenever possible. This limits lateral movement as well as other attack activities.
  - Practice of white listing of ports based on business usage at Firewall level should be implemented rather than blacklisting of certain ports. Traffic on all other ports which have not been white listed should be blocked by default.
- **Security of Cloud Services:**
  - Check public accessibility of all cloud instances in use. Make sure that no server/bucket is inadvertently leaking data due to inappropriate configurations.
  - Ensure proper security of cloud access tokens. The tokens should not be exposed publicly in website source code, any configuration files etc.
  - Implement appropriate security measures for testing, staging and backup environments hosted on cloud. Ensure that production environment is kept properly segregated from these. Disable/remove older or testing environments if their usage is no longer required.
  - Consider employing hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments.
- **Implementation of CERT-In/ CSIRT-Fin Advisories**:

The advisories issued by CERT-In should be implemented in letter and spirit by the regulated entities. Additionally, the advisories should be implemented promptly as and when received.

- **Concentration Risk on Outsourced Agencies:**
  - It has been observed that single third-party vendors are providing services to multiple REs, which creates concentration risk. Here, such third parties though being small non-financial organizations, if any cyber-attack, happens at such organizations, the same could have systemic implication due to high concentration risk.
  - Thus, there is a need for identification of such organizations and prescribing specific cyber security controls, including audit of their systems and protocols from independent auditors, to mitigate such concentration risk.
  - Further, to consider this concentration risk while outsourcing multiple critical services to the same vendor.
- **Audit and ISO Certification:**
  - SEBI's instructions on external audit by independent auditors empanelled by CERT-In should be complied with in letter and spirit.
  - To go for ISO certification as the same provides a reasonable assurance on the preparedness of the RE with respect to cyber security.
  - Due diligence with respect to audit process and tools used for such audit needs to be undertaken to ensure competence and effectiveness of audits.

Principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organization (NTRO), Government of India:

- Protection of Critical Information Infrastructure (CII) is of paramount concern to governments worldwide. To address this threat, the Government of India has notified the 'National Critical Information Infrastructure Protection Centre' (NCIIPC) as the nodal agencies vide Gazette of India notification on 16th January 2014.
- NCIIPC is driven by its mission to take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction, through coherent coordination, synergy and raising information security awareness among all stakeholders with a vision to facilitate safe, secure and resilient Information Infrastructure for Critical Sectors in the country. To achieve this, it is essential to ensure that relevant security mechanisms are built into Critical Information Infrastructure as key design features.
- The National Security Advisor had in July 2013 released a document listing forty controls and corresponding guiding principles for the protection of CIIs. In view of the dynamic nature of cyberspace and to ensure the continued relevance of these controls, NCIIPC is continuously reassessing these based on ongoing experience as well as feedback from NCII constituents, these controls have been grouped into five sets (or families). While all Controls in a family may not be relevant to a particular organization / infrastructure, it is important that conscious sign off (on both, controls implemented, as well as dropped) is taken from senior management based on residual risk acceptable to the Organization.

- **The five families of controls are:**

  - Planning Controls for ensuring that the security is taken as a key design parameter for all new CIIs at conceptualization and design level itself.
  - Implementation Controls for translating the design/conceptualization planning into mechanisms for protecting the CII. These controls also come into play in case of retrofitting existing, unprotected/poorly protected CII.
  - Operational Controls for ensuring that the desired security posture is maintained in the operational environment. These controls also come into play in case of retrofitting existing, unprotected / poorly protected CII.
  - Disaster Recovery/ Business Continuity Planning (BCP) Controls for ensuring minimum downtime and the restoration process.
  - Reporting and Accountability Controls for ensuring adequate accountability and oversight exercised by Senior management, as well as reporting to concerned Government agencies where required enforced through compliance controls.
  - In circumstances where a particular control may not provide the best fit, we as an organization needs to consider compensatory controls which could also be procedural, so as to ensure that the attack surface presented by the organization's Information Infrastructure is minimized.

Advisory for Stockbroker – Member on boarding for CERT-In Cyber Swachhta Kendra (CSK):

In recent times, there has been a surge in cyber-attacks in organizations across the globe impacting the continuity of their business operations and causing sensitive data leakage through malware infections at end point computing devices. To mitigate such malware and botnet infections, CERT-In has launched an initiative named '**Cyber Swachhta Kendra**' (CSK), which provides information and enables organizations to disinfect the computing devices using free-of-cost malware and botnet cleaning tools.

- **Compliance Requirement:**
  - Organization having more than 50,000 active traded clients and also providing Internet Based Trading platform are required to onboard themselves on 'Cyber Swachhta Kendra'
  - Other members (not part of the above criteria) can also voluntarily subscribe to the services and avail actionable information intelligence from CSK.
  - For receiving the reports/alerts from Cyber Swachhta Kendra on daily basis, Organizationis required to follow the guidelines for onboarding on Cyber Swachhta Kendra Portal.
  - Organization can communicate with CERT-In Cyber Swachhta Kendra through email address "**csk@cert-in.org.in**" and contact number **1800-11-4949** can also be used as an alternative.

Illustrative Measures for Data Security on Customer Facing Applications

- Analyse the different kinds of sensitive data shown to the Customer on the frontend application to ensure that only what is deemed absolutely necessary is transmitted and displayed.
- Wherever possible, mask portions of sensitive data. For instance, rather than displaying the full phone number or a bank account number, display only a portion of it, enough for the Customer to identify, but useless to an unscrupulous party who may obtain covertly obtain it from the customer's screen. For instance, if a bank accou nt number is "123 456 789", consider displaying something akin to "XXX XXX 789" instead of the whole numb er. This also has the added benefit of not having to transmit the full piece of data over various networks
- Analyse data and databases holistically and draw out meaningful and "silos" (physical or virtual) into which different kinds of data can be isolated and cordoned off. Forinstance, adatabasewith personal financial information need not be a part of the system or network that houses the public facing websites of the Stock Broker. They should ideally be in discrete silos or DMZs.
- Implement strict data access controls amongst personnel, irrespective of their responsibilities, technical or otherwise. It is infeasible for certain personnel such as System Administrators and developers to not have privileged access to databases. For such cases, take strict measures to limit the number of personnel with direct access, and monitor, log, and audit their activities. Take measures to ensure that the confidentiality of data is not compromised under any of these scenarios.
- Use industry standard, strong encryption algorithms(e.g.: RSA, AES etc.) wherever encryption is implemented. It is important to identify datathat warrants encryption as encrypting all data is infeasible and may open up additional attack vectors. In addition, it is critical to identify the right personnel to be in charge of, and the right methodologies for storing the encryption keys, as any compromise to either will render the encryption useless.

- Ensure that all critical and sensitive data is adequately backed up, and that the backup locationsare adequately secured. For instance, on servers on isolated networks that have no public accessendpoints, or on-premiseserversordiskdrives that are off-limitstounauthorizedpersonnel.Withoutup-to-datebackups,ameaningfulrecoveryfromadisasterorcyber-attackscenariobecomes increasingly difficult.

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.

Murari Securities Limited

_____

Designated Officer

Date: -17/01/2024

Murari Securities Limited

DATA DISPOSAL AND RETENTIONPOLICY:

Policy created by	**Designated Officer**
Policy reviewed by	**Technology Committee**
Policy reviewed on	**31/12/2023**
Policy Approved by	**Board of Directors**
Policy approved on	**17/01/2024**

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 copydocuments.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 paperrecords -

- ✓ Records should be kept for as long as they are needed to meet theoperational needs of the Authority, together with legal and regulatory requirements. We have assessed our recordsto:
  - Determine their value as a source of information about the Authority,its operations, relationships andenvironment
  - Assess their importance as evidence of business activities anddecisions
  - 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 25years.

Responsibilities of Employees –

All employeesare 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 employeeshas 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 maincategories:
  - 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 financialyear).
  - Automatically select for permanent preservation – where certain groups of records can be readily defined as worthy of permanent preservation and transferred to anarchive.
  - 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 permanentpreservation.
- ✓ Records can be destroyed in the followingways:
  - **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 recoverytechniques.
- ✓ Archival transfer
  - This is the physical transfer of physical records to a permanent custody at the National ArchivesOffice.

Sharing of information:

- ✓ Duplicate records should be destroyed. Where information has been regularly shared between business areas, only the original records should be retainedin accordance with the guidelines mentioned above. Care should be taken that seemingly duplicate records have not beenannotated.
- ✓ 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 assessmentand update our privacy notices to reflect datasharing.

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 filesthemselves 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 auditpurposes.
- ✓ 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 thematerial.

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 MURARI SECURITIES LIMITED,

_____

Ishwar Dass Dhyawala

Designated Officer

Murari Securities Limited

DATA LEAKAGE POLICY

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

Policy created by	**Designated Officer**
Policy reviewed by	**Technology Commitee**
Policy reviewed on	**31/12/2023**
Policy Approved by	**Board of Directors**
Policy approved on	**17/01/2024**

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 organizationwill 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 organizationrelies 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 organizationinternally 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 Datai.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 Datai.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 includesuch as financial reports, some research data.

Tier 3-

Public Datai.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.

Murari Securities Limited

_____

Designated Officer

Date: -17/01/2024

Murari Securities Limited

ELECTRONIC STORAGE MEDIA DISPOSALPOLICY

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	**31/12/2023**
Policy Approved by	**Board of Directors**
Policy approved on	**17/01/2024**

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.

Murari Securities Limited

_____

Designated Officer

Dated: - 17/01/2024

Murari Securities Limited

INFORMATION SECURITY 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	**31/12/2023**
Policy Approved by	**Board of Directors**
Policy approved on	**17/01/2024**

Version – 1.2

Purpose

The purpose of this Policy is to safeguard information belonging to the Company and its stakeholder (third parties, clients or customers and the general public), within a secure environment.

ThisPolicy informs the Company'sstaff, and other external Vendors entitled to use Company facilities, of the principles governing the holding, use and disposal of information.

It is the goal of the Company that:

- Information will be protected against unauthorised access or misuse.
- Confidentiality of information will be secured.
- Integrity of information will be maintained.
- Availability of information / information systems is maintained for service delivery.
- Business continuity planning processes will be maintained.
- Regulatory, contractual and legal requirements will be complied with.
- Physical, logical, environmental and communications security will be maintained.
- Infringement of this Policy may result in disciplinary action or criminal prosecution.
- When information is no longer of use, it is disposed of in a suitable manner.
- All information security incidents will be reported to the Director of ICT Systems, and investigated through the appropriate management channel.

Information relates to:

- Electronic information systems (software, computers, and peripherals) owned by the Company whether deployed or accessed on or off campus.
- TheCompany's computer networkused either directly or indirectly.
- Hardware, software and data owned by the Company.
- Paper-based materials.
- Electronic recording devices (video, audio, CCTV systems).

The Policy

The Company requires all users to exercise a duty of care in relation to the operation and use of its information systems.

Authorised users of information systems

- With the exception of information published for public consumption, all users of Company information systems must be formally authorised by appointment as a member of staff, or by other process specifically authorised by the designated officer. Authorised users will be in possession of a unique user identity. Any password associated with a user identity must not be disclosed to any other person. The "Network password policy" describes these principles in greater detail.
- Authorised users will pay due care and attention to protect Company information in their personal possession. Confidential, personal or private information must not be copied or transported without consideration of:

- permission of the information owner
- the risks associated with loss or falling into the wrong hands
- Howthe information will be secured during transport and at its destination.

Acceptable use of information systems

- Use of the Company's information systems by authorised users will be lawful, honest and decent and shall have regard to the rights and sensitivities of other people. The detail of acceptable use in specific areas may be found in the list of subsidiary policies.

Information System Owners

- Designated Officer/Chief Technology Officer/Directors who are responsible for information systemsare required to ensure that:
  - Systems are adequately protected from unauthorised access.
  - Systems are secured against theft and damage to a level that is cost-effective.
  - Adequate steps are taken to ensure the availability of the information system, commensurate with its importance (Business Continuity).
  - Electronic data can be recovered in the event of loss of the primary source. I.e. failure or loss of a computer system. It is incumbent on all system owners to backup data and to be able to restore data to a level commensurate with its importance (Disaster Recovery).
  - Data is maintained with a high degree of accuracy.
  - Systems are used for their intended purpose and that procedures are in place to rectify discovered or notified misuse.
  - Any electronic access logs are only retained for a justifiable period to ensure compliance with the data protection, investigatory powers and freedom of information acts.
  - Any third parties entrusted with Companydata understand their responsibilities with respect to maintaining its security.

Personal Information

- Authorised users of information systems are not given rights of privacy in relation to their use of Company information systems. Duly authorised officers of the Company may access or monitor personal data contained in any Companyinformation system (mailboxes, web access logs, file-storeetc.).
- Individuals in breach of this policy are subject to disciplinary procedures at the instigationof theDesignated Officer with responsibility for the relevant information system, including referral to the Police where appropriate.
- The Company will take legal action to ensure that its information systems are not used by unauthorised persons.

Ownership

- The Designated Officer of ICT Systems has direct responsibility for maintaining this policy and providing guidance and advice on its implementation.
- Information system owners are responsible for the implementation of this Policy within their area, and to ensure adherence.

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.

Murari Securities Limited

_____

Designated Officer

Dated: -17/01/2024

Murari Securities Limited

INTERNET ACCESS 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	**31/12/2023**
Policy Approved by	**Board of Directors**
Policy approved on	**17/01/2024**

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.

MURARI SECURITIES LIMITED

_____

Designated Officer

Dated: - 17/01/2024

Murari Securities Limited

IT ACCESS CONTROL AND USER ACCESS MANAGEMENT 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	**31/12/2023**
Policy Approved by	**Board of Directors**
Policy approved on	**17/01/2024**

Version – 1.2

PolicyStatement

- Protecting access to IT systems and applications is critical to maintain the integrity of the Company's technology and data and prevent unauthorized access to suchresources.
- AccesstoCompany'ssystemsmustberestrictedtoonlyauthorizedusersorprocesses,basedon the principle of strict need to know and leastprivilege.

Background

- Access controls are necessary to ensure only authorized users can obtain access to theCompany's information andsystems.
- Accesscontrolsmanagetheadmittanceofuserstosystemandnetworkresourcesbygranting users access only to the specific resources they require to complete their job-relatedduties.

Policy Objective

- TheobjectiveofthispolicyistoensuretheInstitutionhasadequatecontrolstorestrictaccess to systems anddata.

Scope

- This policy appliesto all branch and head office including employees, Consultants and Outside Vendors accessing Company's IT systems andapplications.

Definitions

- "Access Control" is the process that limits and controls access to resources of a computer system.
- "Users" are employees, consultants, contractors, agents and authorized users accessing Company IT systems andapplications.
- "System or Application Accounts" are user ID's created on IT systems or applications, which are associated with specific access privileges on such systems andapplications.
- "PrivilegedAccounts"aresystemorapplicationaccountsthathaveadvancedpermissions (as comparedtoregularuseraccountpermissions)onsuchsystemsorapplications.Examplesof user accounts with privileges include: administrative and super useraccounts.
- "Access Privileges" are systems permissions associated with an account, including permissionstoaccessorchangedata,toprocesstransactions,createorchangesettings,etc.
- "Administrator Account" is a user account with privileges that have advanced permissions on an IT system that are necessary for the administration of this system. For example, an administrator account can create new users, change account permissions, modify security settings such as password settings, modify system logs,etc.
- "Application and Service Accounts" are user accounts that are not associated with a person but an IT system, an application (or a specific part of an application) or a networkservice.
- "Nominative User Accounts" are user accounts that are named after aperson.
- "Non-disclosureAgreement"isacontractbetweenapersonandtheCompanystatingthatthe person will protect confidential information (as defined in the Record Classification and Handling Policy) covered by the contract, when this person has been exposed to such information.

Guiding Principles – General Requirements

- The Company will provide access privileges to Company technology (includingnetworks, systems, applications,

computers and mobile devices) based on the followingprinciples:

- **Need to know** – users or resources will be granted access to systems thatare necessary to fulfill their roles andresponsibilities.
- **Least privilege** – users or resources will be provided with the minimumprivileges necessary to fulfill their roles andresponsibilities.

- Requests for users' accounts and access privileges must be formally documentedand appropriatelyapproved.
- Requests for special accounts and privileges (such as vendor accounts, application and service accounts, system administration accounts, shared / generic accounts, test accounts and remote access) must be formally documented and approved by the systemowner.
- Application and service accounts must only be used by application components requiring authentication; access to the passwords must be restricted to authorized IT administratorsor application developers only.
- Where possible, the Company will set user accounts to automatically expire at a pre-setdate. Morespecifically,
  - Whentemporaryaccessisrequired,suchaccesswillberemovedimmediatelyafterthe user has completed the task for which the access wasgranted.
  - User accounts assigned to contractors will be set to expire according to the contract's expirydate.
  - User accounts will be disabled after 3 months of inactivity. This does not apply to accounts assigned toemployees.
  - User accounts with signed contracts for a recurring, continuing, or tenure track appointment for an upcoming term can be active for up to four months between appointments.
- Access rights will be immediately disabled or removed when the user is terminated orceases to have a legitimate reason to access Company'ssystems.
- A verification of the user's identity must be performed by the IT Director, Help Desk, or designate before granting a new password.
- Existing user accounts and access rights will be reviewed at least annually to detect dormant accounts and accounts with excessive privileges. Examples of accounts with excessive privilegesinclude:
  - An active account assigned to external contractors, vendors or employees that no longer work for theCompany.
  - Anactiveaccountwithaccessrightsforwhichtheuser'sroleandresponsibilitiesdonot require access. For example, users that do not have authority or responsibility to approve expenses should not have access with approval permissions within afinancial system.
  - System administrative rights or permissions (including permissions to change the security settings or performance settings of a system) granted to a user who is not an administrator.
  - Unknown activeaccounts.
- All access requests for system and application accounts and permissions will bedocumented using the ticketing system inplace.

Guiding Principles – Privileged Accounts

- A nominative and individual privileged user account must be created for administrator accounts (such as "first name. last name.admin"), instead of generic administrator account names.

- Privileged user accounts can only be requested by managers or supervisors and must be appropriatelyapproved.

Guiding Principles – Shared User Accounts

- Wherepossible,theuseofspecificnetworkdomain"securitygroups"shouldbeusedtoshare common access permissions across many users, instead of sharedaccounts.
- Shareduseraccountsareonlytobeusedonanexceptionbasiswiththeappropriateapproval. This includes general user accounts such as "guest" and "functional"accounts.
- When shared accounts arerequired:
  - Passwords will be stored and handled in accordance with the PasswordPolicy.
  - The use of shared accounts will be monitored where possible, including the recording of the time of access, the reason for accessing the shared user account, and the individual accessing his account. When the shared user account has administrative privileges, such a procedure is mandatory and access to the monitoring logs must be protected andrestricted.

Vendor or Default User Accounts

- Wherepossible,alldefaultuseraccountswillbedisabledorchanged.Theseaccountsinclude "guest", "temp", "admin", "Administrator", and any other commonly known or used default accounts, as well as related default passwords used by vendors on "commercial off-theshelf" systems andapplications.

Test Accounts

- Testaccountscanonlybecreatediftheyarejustifiedbytherelevantbusinessareaorproject teamandapprovedbytheapplicationowner,throughaformalrequesttotheITDirectororthe IT Help Desk.
- Test accounts must have an expiry date (maximum of 6 months). Maintaining test accounts beyond this date must be re-evaluated every 90 days and approvedappropriately.
- Test accounts will be disabled / deleted when they are no longernecessary.

Contractors and Vendors

- In accordance with the Contract Management Policy, contracts with contractors / vendors will includespecificrequirementsfortheprotectionofdata.Inaddition,contractor/vendorrepresentatives will be required to sign a Non-disclosure Agreement ("NDA") prior to obtaining approval to access Institution systems and applications.
  - Priortograntingaccessrightstoacontractor/vendor,theITDirectororHelpDeskmustverify the requirements of Section 11.1 have been compliedwith.
  - ThenameofthecontractorvendorrepresentativemustbecommunicatedtotheITHelpDesk at least 2 business days before the person needsaccess.
- The Company will maintain a current list of external contractors or vendors having access to Company'ssystems.
- Theneedtoterminatetheaccessprivilegesofthecontractor/vendormustbecommunicated to the IT Help Desk at least 1 business day before the contractor / vendor representative's need for such access ends.

Access Control Requirements

- All users must use a unique ID to access Company's systems and applications. Passwords must be set in accordance with the PasswordPolicy.
- Alternative authentication mechanisms that do not rely on a unique ID and password mustbe formallyapproved.
  - Remote access to Company's systems and applications must use two-factor authenticationwhere possible.
  - System and application sessions must automatically lock after 15 minutes ofinactivity.

Roles and Responsibilities

STAKEHOLDER	RESPONSIBILITIES
Board of Director	• Approve and formally support thispolicy.
President, Administration	• Review and formally support thispolicy.
IT Director/Designated officer	• Develop and maintain thispolicy. • Review and approve any exceptions to the requirements of thispolicy. • Take proactive steps to reinforce compliance of all stakeholders with thispolicy.
Supervisors or Company's Representative	• Support all employees and others in the understanding of the requirementsof thispolicy. • Immediately assess and report to the IT service desk anynon-compliance instance with thispolicy.
Contract Administrators	• Ensure that the responsibilities and security obligations of each party tothe contractua relationship are outlined in the contract executed between the Company's and thecontractor/sub-contractor.
Human Resources	• Present each new employee or contractor with the relevant Company's IT andSecurity Policies, upon the first day of commencing work withCompany's. • Support all employees and other in the understanding of the requirementsof thispolicy.
All users (Employees and contractors, Visitors and or Volunteers)	• Report all non-compliance instances with this policy (observed or suspected)to their Supervisor, Instructor or Company's Representative as soon aspossible.

Exceptions to the Policy

- Exceptions to the guiding principles in this policy must be documented and formallyapproved by the ITDirector/Designated Officer.
- **Policy exceptions must describe:**
  - The nature of the exception
  - A reasonable explanation for why the policy exception is required
  - Any risks created by the policy exception
  - Evidence of approval by the ITD irector
- **Inquiries**
  - Inquiries regarding this policy can be directed to the ITD irector/Designated officer.

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.

Murari Securities Limited

_____

Designated Officer

Dated: -17/01/2024

Murari Securities Limited

LOG RETENTION POLICY

Policy created by	**Designated Officer**
Policy reviewed by	**Technology Committee**
Policy reviewed on	**31/12/2023**
Policy Approved by	**Board of Directors**
Policy approved on	**17/01/2024**

Version – 1.0

Purpose

The purpose of this Log Retention Policy is to establish guidelines and procedures for the retention, management, and secure disposal of logs at our Company. This policy aims to ensure the availability of logs for operational needs, compliance with regulations, and effective response to security incidents.

Scope

This policy applies to all employees, contractors, third-party vendors, and any other individuals who have access to or are responsible for managing logs within the stock brokerage firm.

Definitions

Logs

Records generated by systems, applications, networks, and security devices that capture events, transactions, or interactions.

Log Retention

The period for which logs are stored and maintained.

Policy Guidelines

Identification of Critical Logs

Critical logs, including but not limited to security event logs, system logs, and application logs, will be identified based on their significance to operations, compliance, and security.

Retention Periods

- Retention periods for logs will be determined based on regulatory requirements, legal obligations, and business needs.
- Different types of logs may have different retention periods.

Log Storage

- Logs will be stored in a secure, centralized repository with restricted access.
- Adequate measures will be taken to protect log storage facilities physically and logically.

Encryption of Stored Logs

Logs stored for an extended period will be encrypted to ensure the confidentiality and integrity of the information.

Regular Review of Logs

- Logs will be regularly reviewed to identify anomalies, security incidents, and operational issues.
- Automated tools may be used to assist in log analysis.

Disposal of Obsolete Logs

Logs that have exceeded their retention period or are no longer relevant will be securely disposed of using industry-accepted methods.

Legal Hold

In case of legal proceedings or investigations, a legal hold may be applied to prevent the disposal of relevant logs.

Monitoring and Auditing

The log retention process will be monitored, and periodic audits will be conducted to ensure compliance with this policy.

Compliance and Legal Considerations

Regulatory Compliance

- The log retention policy will comply with relevant financial regulations and industry standards.
- Regular audits will be conducted to verify compliance.

Documentation

Detailed records of log retention periods, disposal processes, and audit results will be maintained for compliance and audit purposes.

Review and Update

This policy will be reviewed regularly and updated as necessary to address changes in regulations, business processes, and emerging risks.

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.

Murari Securities Limited

_____

Designated Officer

Dated: - 17/01/2024

Murari Securities Limited

NETWORK SECURITY POLICY

Policy created by	**Designated Officer**
Policy reviewed by	**Technology Committee**
Policy reviewed on	**31/12/2023**
Policy Approved by	**Board of Directors**
Policy approved on	**17/01/2024**

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.

Murari Securities Limited

_____

Designated Officer

Dated: - 17/01/2024

Murari Securities Limited

PASSWORD POLICY:

Policy created by	**Compliance Team**
Policy reviewed by	**Designated Officer**

Policy reviewed on	**31/12/2023**
Policy Approved by	**Board of Directors**
Policy approved on	**17/01/2024**

Version – 1.2

Purpose:

The purpose of this policy is to establish a standard for creation of strong passwords , the protection fthosepass words,and the frequencyof change of the passwords.

Scope:

The scope of this policy includes all end-users and personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system/service in the NICdomain.Theseincludepersonnelwiththeirdesignateddesktopsystems. The scope also includes designers and developers of individual applications.

Policy:

PolicyStatements

- ✓ For users having account sforaccessing systems/services
- ✓ Users shall be responsible for all activity performed with their personal user IDs. Users shall not permit others toper form any activity with their user IDs or perform any activity with ID sbelonging tooth er users.
- ✓ Alluser-levelpasswords(e.g.,email,web,desktopcomputer, etc.) shall be changed periodically (at leastonce every three months). Users shall not be able toreuseprevious passwords.
- ✓ Password shall be enforced to be of a minimum lengthandcomprisingofmixofalphabets,numbersandcharacters.
- ✓ Passwords shall not be stored in readable form in batchfiles ,automaticlogonscripts,Internetbrowsersorrelateddatacommunicationsoftware,incomputerswithout access control, or in any other location whereunauthorizedpersonsmightdiscoverorusethem.
- ✓ All access codes including user ID passwords, networkpasswords, PINs etc. shall not be shared with anyone,including personal assistants or secretaries. These shallbetreatedassensitive,confidentialinformation.
- ✓ AllPINs(PersonalIdentificationNumbers)shallbeconstructedwiththesamerulesthatapplytofixedpasswords.
- ✓ Passwordsmustnotbecommunicatedthoughemailmessages or other forms of electronic communicationsuchasphoneto anyone.
- ✓ Passwords shall not be revealed on questionnaires orsecurityforms.
- ✓ Passwords of personal accounts should not be revealedto the controlling officer or any co-worker even while onvacationunlesspermittedtodosobydesignatedauthority.
- ✓ The same password shall not be used for each of the systems/applications to which a user has been grantedaccesse.g.aseparatepasswordtobeusedforaWindowsaccountandanUNIXaccountshouldbeselected.
- ✓ The "Remember Password" feature of applications shallnotbe used.
- ✓ Users shall refuse all offers by software to place a cookieon their computer such that they can automatically logon thenexttimethattheyvisitaparticularInternetsite.
- ✓ First time login to systems/services with administratorcreatedpasswords,shouldforcechangingofpasswordbythe user.
- ✓ If the password is shared with support personnel forresolving problems relating to any service, it shall bechangedimmediatelyafter thesupport session.
- ✓ Thepasswordshallbechangedimmediatelyifthepassword is suspected of being disclosed, or known tohavebeendisclosedtoanunauthorizedparty.

- ✓ Fordesigners/developersofapplications/sites
- ✓ No password shall be traveling in clear text; the hashedform of the password should be used. To get around thepossibility of replay of the hashed password, it shall beusedalongwitharandomizationparameter.
- ✓ The backend database shall store hash of the individualpasswordsandneverpasswordsinreadableform.
- ✓ Password shall be enforced to be of a minimum lengthandcomprisingofmixofalphabets,numbersandcharacters.
- ✓ Usersshallberequiredtochangetheirpasswordsperiodicallyandnotbeabletoreusepreviouspasswords.
- ✓ For Password Change Control, both the old and newpasswordsarerequiredtobegivenwheneverapasswordchangeisrequired.

Policy for constructing a password:

All user-level and system-level passwords must conform to the following general guideline sdescribed below.

- ✓ The password shall contain more than eight characters.
- ✓ The password shall not be awordfoundinadictionary (English orforeign).
- ✓ The password shall notbe aderivative oftheuserID,e.g. <username>123.
- ✓ Thepasswordshallnotbeaslang,dialect,jargonetc.
- ✓ The password shall not be a common usage words such asnamesoffamily,pets,friends,co-workers,fantasycharacters,etc.
- ✓ The password shall not be based on computer terms andnames,commands,sites,companies,hardware,software.
- ✓ The password shall not be based on birthdays and otherpersonalinformationsuchasaddressesandphonenumbers.
- ✓ The password shall not be a word or number pattern likeaaabbb, qwerty, zyxwvuts, 123321, etc. or any of theabovespelledbackwards.
- ✓ The password shall not be any of the above preceded orfollowedbyadigit (e.g., secret1,1secret).
- ✓ The password shall be a combination of upper- and lower-case characters (e.g.a-z,A-Z),digits(e.g.0-9)andpunctuationcharactersaswellandothercharacters(e.g., @#$%^&*() _+|~-=\` {} []:";'<>? /).
- ✓ Passwords shall not be such that they combine a set ofcharactersthatdonotchangewithasetofcharactersthatpredictably change.

Suggestions for choosing passwords:

- ✓ Passwordsmaybechosensuchthattheyaredifficult-to-guessyeteasy-to-remember.Methodssuch asthefollowing maybeemployed:
- ✓ String together several words to form a pass-phrase as apassword.
- ✓ Transformaregularwordaccordingtoaspecificmethode.g. making every other letter a number reflecting itspositionin the word.
- ✓ Combinepunctuationand/ornumberswitharegularword.
- ✓ Createacronymsfromwordsinasong,apoem,oranyotherknown sequence ofwords.
- ✓ Bumpcharactersinawordacertainnumberoflettersupordown the alphabet
- ✓ Shiftawordup,down,leftorrightonerowonthekeyboard.

Responsibilities:

- ✓ AllindividualushavingaccountsforaccessingsystemsservicesintheNICdomain,andsystem/networkadministr

ators of NIC servers'/ network equipment shall ensuretheimplementationofthispolicy.

- ✓ Alldesigners/developersresponsibleforsite/applicationdevelopment shall ensure the incorporation of this policy in theauthentication modules, registration modules, password changemodulesoranyothersimilarmodulesintheirapplications.

Compliance

- ✓ Personnel authorized as Internal Audit shall periodically reviewtheadequacyofsuchcontrolsand theircompliance.
- ✓ Personnel authorized as Application Audit shall check respectiveapplicationsforpasswordcomplexityandpasswordpolicyincorporation.

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.

For M/s. Murari Securities Limited

_____

Designated Officer

Dated: -17/01/2024

Murari Securities Limited

WFH ENVIRONMENTPOLICY

Policy created by	**Designated Officer**
Policy reviewed by	**Technology Committee**
Policy reviewed on	**31/12/2023**
Policy Approved by	**Board of Directors**
Policy approved on	**17/01/2024**

Version – 1.0

Purpose

The purpose of this Work from Home (WFH) Policy is to provide guidelines and procedures for employees at our Company, when working remotely. This policy aims to ensure productivity, data security, and the well-being of employees in a WFH environment.

Scope

This policy applies to all employees who have been authorized to work remotely on a temporary or permanent basis.

Eligibility and Approval

Eligibility Criteria

- Employees eligible for WFH arrangements will be determined based on job responsibilities and performance.
- Not all positions may be eligible for remote work.

Approval Process

- Requests for WFH arrangements must be submitted to the employee's supervisor and approved by the respective department head or HR.
- Approvals will be based on business needs and the employee's ability to meet performance expectations remotely.

Work Hours and Availability

Work Hours

- Employees are expected to adhere to their regular work hours unless alternative arrangements are approved.
- Flexibility in work hours may be granted based on business needs and mutual agreement.

Availability

- Employees must be available during agreed-upon working hours and remain reachable through approved communication channels.
- Communication about unavailability must be communicated in advance.

Home Office Setup

Equipment and Technology

- Employees are responsible for providing their own equipment, such as laptops, monitors, and internet connectivity.
- The IT department will provide necessary support and guidelines for setting up a secure home office.

Data Security

- Employees must ensure the security of company data by using secure networks, encrypted connections, and following data protection policies.
- Devices used for work must be password-protected and kept in a secure environment.

Communication and Collaboration

- Employees must use approved communication and collaboration tools for work-related activities.
- Regular check-ins and team meetings will be conducted to maintain communication and collaboration.

Performance and Accountability

- Performance expectations and metrics will remain consistent with in-office arrangements.
- Managers will monitor performance and address any concerns promptly.

Expenses and Reimbursements

- Employees will be responsible for their own internet and utility costs.
- Reimbursement for business-related expenses may be considered on a case-by-case basis.

Health and Well-being

- Employees are encouraged to take regular breaks, maintain a healthy work-life balance, and communicate any concerns about well-being.
- Ergonomic guidelines will be provided for setting up a comfortable workspace.

Security Awareness Training

Employees will undergo security awareness training to recognize and address cyber security threats in a remote work environment.

Termination of WFH Arrangements

- WFH arrangements may be terminated based on business needs or if there is a violation of company policies.
- Notice will be given, and a discussion will be held before terminating WFH arrangements.

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.

Murari Securities Limited

_____

Designated Officer

Dated: - 17/01/2024

Murari Securities Limited

POLICY ON DATA SECURITY

Policy created by	**Designated Officer**
Policy reviewed by	**Technology Committee**
Policy reviewed on	**31/12/2023**
Policy Approved by	**Board of Directors**
Policy approved on	**17/01/2024**

Version – 1.0

Purpose

The purpose of this Data Security Policy is to establish guidelines and procedures for protecting the confidentiality, integrity, and availability of data at our Company. This policy aims to mitigate the risk of unauthorized access, disclosure, alteration, and destruction of sensitive financial information.

Scope

This policy applies to all employees, contractors, third-party vendors, and any other individuals who have access to the stock brokerage firm's data and information systems.

Policy Guidelines

Data Classification

- Data will be classified based on its sensitivity and importance to the business.
- Each classification level will have corresponding security controls and access restrictions.

Access Control

- Access to sensitive data will be restricted based on job responsibilities and the principle of least privilege.
- User access will be reviewed regularly, and adjustments will be made as needed.

Data Encryption

- Encryption will be applied to sensitive data in transit and at rest.
- Encryption protocols will comply with industry standards.

Secure Transmission

- Secure communication protocols, such as HTTPS, will be used for transmitting sensitive data over networks.
- Public networks, including the internet, will be avoided for transmitting sensitive information.

Secure Storage

- Sensitive data will be stored securely in designated repositories with access controls.
- Physical and logical security measures will be implemented to protect data storage facilities.

Data Backup and Recovery

- Regular backups of critical data will be conducted to ensure data availability in the event of system failures or disasters.
- Backup and recovery procedures will be tested periodically.

Endpoint Security

- Endpoint security solutions, including antivirus software and endpoint detection and response (EDR) tools, will be deployed and regularly updated.
- Mobile devices used for work purposes will adhere to the same security standards.

Incident Response Plan

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

Vendor Security

- Third-party vendors with access to sensitive data will be evaluated for security controls and compliance with data security standards.
- Contracts with vendors will include data security requirements.

Compliance and Legal Considerations

Regulatory Compliance

- The data security policy will comply with relevant financial regulations and industry standards.
- Regular audits will be conducted to verify compliance.

Review and Update

This policy will be reviewed regularly and updated as necessary to address emerging security threats and technological advancements.

Employee Responsibilities

Employees are responsible for using data in accordance with this policy and reporting any suspicious activities promptly.

Confidentiality Agreement

Employees will sign a confidentiality agreement, acknowledging their responsibility for protecting sensitive data.

Training and Awareness

- Employees will undergo regular training on data security best practices.
- Awareness campaigns will be conducted to ensure a culture of security.

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

Murari Securities Limited

_____

Designated Officer

Dated: - 17/01/2024

Murari Securities Limited

POLICY ON IDENTIFICATION OF CRITICAL ASSETS BASED ON SENSITIVITY

Policy created by	**Designated Officer**
Policy reviewed by	**Technology Committee**
Policy reviewed on	**31/12/2023**
Policy Approved by	**Board of Directors**
Policy approved on	**17/01/2024**

Version – 1.0

Purpose

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

Scope

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

Policy Guidelines

Asset Identification Criteria

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

Data Sensitivity Classification

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

Identification Process

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

Asset Inventory

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

Access Control

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

Data Encryption

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

Physical Security Measures

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

Incident Response Plan for Critical Assets

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

Compliance and Legal Considerations

Regulatory Compliance

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

Review and Update

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

Employee Responsibilities

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

Training and Awareness

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

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

Murari Securities Limited

_____

Designated Officer

Dated: - 17/01/2024

Murari Securities Limited

POLICY ON UNUSUAL REPORTING OF ACTIVITIES

Policy created by	**Designated Officer**
Policy reviewed by	**Technology Committee**
Policy reviewed on	**31/12/2023**
Policy Approved by	**Board of Directors**
Policy approved on	**17/01/2024**

Version – 1.0

Purpose

The purpose of this policy is to establish guidelines and procedures for reporting unusual activities atour Company. This policy aims to encourage employees to promptly report any suspicious or irregular activities that could potentially impact the firm's operations, regulatory compliance, or the integrity of financial markets.

Scope

This policy applies to all employees, contractors, third-party vendors, and any other individuals who have knowledge of or suspect unusual activities within the stock brokerage firm.

Definitions

Unusual Activities

Any activity that deviates from the normal or expected behaviour and may indicate potential risks, fraud, or regulatory non-compliance.

Reporting Party

Individuals who witness or have knowledge of unusual activities and are responsible for reporting such activities.

Reporting Process

Identification of Unusual Activities

Employees are encouraged to be vigilant and promptly report any unusual activities they observe or become aware of during the course of their duties.

Reporting Channels

- Unusual activities can be reported through designated reporting channels, including but not limited to:
  - Direct supervisors or managers
  - Compliance department
  - Internal audit
  - Whistle-blower hotline or reporting platform

Anonymous Reporting

To encourage transparency, the firm provides anonymous reporting options, such as a confidential hotline or online reporting system.

Whistle-blower Protection

The firm is committed to protecting whistle-blowers from retaliation and ensuring confidentiality to the extent permitted by law.

Investigation Process

Designated Investigation Team

An investigation team will be designated to assess and investigate reported unusual activities promptly.

Confidentiality

Information related to the reported unusual activities will be treated with the utmost confidentiality during the investigation process.

Communication

Regular updates on the status of investigations will be communicated to the reporting party to the extent possible without compromising the investigation.

Non-Retaliation

The firm strictly prohibits retaliation against any individual who, in good faith, reports unusual activities. Retaliation is a violation of company policy and may result in disciplinary action.

Training and Awareness

Employees will receive training on recognizing and reporting unusual activities as part of their compliance and ethics training.

Compliance and Legal Considerations

Regulatory Compliance

The reporting process will comply with relevant financial regulations and industry standards.

Documentation

Detailed records of reported unusual activities, investigations, and outcomes will be maintained for compliance and audit purposes.

Review and Update

This policy will be reviewed regularly and updated as necessary to address changes in regulations, business processes, and emerging risks.

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.

Murari Securities Limited

_____

Designated Officer

Dated: - 17/01/2024

Murari Securities Limited

STANDARD OPERATING PROCEDURE

Policy created by	**Compliance Team**
Policy reviewed by	**Designated Officer**
Policy reviewed on	**31/12/2023**
Policy Approved by	**Board of Directors**
Policy approved on	**17/01/2024**

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 weable to recognize, analyses 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 organizationare also important elements to take into consideration.

Important terms to be known forCyber Security incident handling:

- ✓ **Cyber Security Event** - A cyber security change that may have an impact on ouroperations (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 ouroperations.
- ✓ **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 foruswill 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 companyto 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 ofcompanyhave great potential to help detect and identify cyber security incidents. Make sure that every employee of our companyis 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 companyto 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 allowlooking 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 ofcompanydepend 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 companyto 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 bein 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.

  <u>Especially needed documents are:</u>

➢ **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.

SKILLS	RESPONSIBILITIES	ROLES
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	IT technical support staff

	• the physical access to the premises • The physical protection of the cyber infrastructure.	

- ✓ **CYBER INCIDENT RESPONSE TEAM-** In an ideal world, every companyshould 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 thesystems 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 areinfected 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.

- ✓ Weshall 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

Weshould always seriously consider reporting cyber-security incidents to the IndianComputerEmergency 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?
- ✓ Doescompany have logs or other useful data?
- ✓ Who have company already informed?
- ✓ What companyexpecting 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 companyis 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, wewill 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 weshall 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	POSSIBLETARGET	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 XYZ Company.	Management	As deems fit.	As deems fit.
Unauthorised access	When a person gains logical or physical access without permissionto a network, system, application, data, or other IT resource.	Customer information Credit card information Applications creating or processing payments Websites and services	Passwordcracked orsniffedUnpatched 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	Mail system Network	Spam filter weaknesses	Block traffic Contact ISP

	networks, systems or applications byexhausting resources.	appliances Application servers Web sites and services	Unpatched system vulnerabilities Weak configuration of systems or appliances	Disconnect 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 userworkstations 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 dateInappropriate 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 carelesslyor even be completely unaware	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	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

	of the standard operating procedure or code of conducthe / she has infringed. The inappropriate behaviour will sometimes constitute a serious security incident in itself, but it can also be the cause or trigger ofa serious incident (like malware infection, loss of critical data)		monitoring Lack of procedures or control to enforce policies and codes of conduct	information to trace and prove what happened 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 is 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	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

		strategy, on-going projects and decisions, etc		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. Murari Securities Limited

_____

Designated Officer

Dated:-17/01/2024

Murari Securities Limited

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	**31/12/2023**
Policy Approved by	**Board of Directors**
Policy approved on	**17/01/2024**

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

- Wewill 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 and 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

Murari Securities Limited

Designated Officer

Dated: - 17/01/2024