Murari securities Limited

POLICY ON CAPACITY MANAGEMENT

CONFIDENTIAL

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 and Scope

This Capacity Management Policy outlines the procedures and guidelines for effectively managing the capacity of company's systems and infrastructure. The objective is to ensure that the organization's technical capabilities can meet current and future demands, maintaining optimal performance, reliability, and compliance with regulatory standards.

Capacity Planning

Demand Forecasting

Implement a process for forecasting future demand on the trading platform and related systems.

Resource Allocation

Allocate resources based on demand forecasts, ensuring that system capacity aligns with anticipated usage.

System Performance Monitoring

Real-time Monitoring

Utilize real-time monitoring tools to track system performance, including server utilization, latency, and throughput.

Proactive Alerts

Configure proactive alerts to notify IT and operations teams of potential capacity issues before they impact performance.

Scalability

Vertical Scaling

Assess the ability to vertically scale existing infrastructure to handle increased loads efficiently.

Horizontal Scaling

Evaluate options for horizontal scaling to distribute workloads across multiple servers or systems.

Load Testing

Regular Testing

Conduct regular load testing to simulate peak usage scenarios and identify potential bottlenecks.

Performance Benchmarks

Establish performance benchmarks to measure and compare system performance under various load conditions.

Capacity Upgrades and Enhancements

Timely Upgrades

Implement a process for timely upgrades of hardware, software, and network components to meet growing capacity demands.

Technology Refresh

Regularly assess and refresh technology to ensure compatibility with the latest industry standards and advancements.

Disaster Recovery and Business Continuity

Integrate capacity management considerations into the organization's disaster recovery and business continuity plans.

Compliance with Regulatory Requirements

Ensure that capacity management practices comply with regulatory requirements in the financial industry.

Reporting and Communication

Develop a reporting framework to communicate capacity management status to relevant stakeholders, including senior management and regulatory authorities.

Documentation

Maintain comprehensive documentation of capacity planning, monitoring procedures, and actions taken in response to capacity-related incidents.

Training and Awareness

Provide training to relevant staff members on the importance of capacity management and adherence to established procedures.

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 THIRD PARTY INFORMATION SECURITY MANAGEMENT

CONFIDENTIAL

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 and Scope

This Third-Party Information Security Management Policy outlines the procedures and guidelines for managing information security risks associated with third-party relationships within our Company. The objective is to ensure the confidentiality, integrity, and availability of information assets shared with or accessed by third parties.

Third-Party Information Security Risk Assessment

Due Diligence

- Perform thorough due diligence before engaging with third parties.
- Assess the information security practices and controls of potential third-party partners.

Risk Categorization

- Categorize third-party relationships based on the level of information security risk they pose.
- Tailor risk assessments to the specific nature of the relationship.

Contractual Obligations

Information Security Clauses

- Include specific information security clauses in contracts with third parties.
- Clearly define security requirements, responsibilities, and compliance expectations.

Compliance Audits

- Reserve the right to conduct periodic audits to verify third-party compliance with information security requirements.
- Establish protocols for notifying third parties about upcoming audits.

Security Controls and Monitoring

Security Controls

- Specify minimum information security controls that third parties must implement to safeguard shared information.
- Examples include encryption standards, access controls, and data protection measures.

Monitoring Mechanisms

- Implement monitoring mechanisms to track third-party compliance with security controls.
- Establish reporting mechanisms for anomalies or security incidents.

Incident Response and Notification

Incident Response Plans

- Ensure that third parties have incident response plans in place to address security incidents promptly.
- Collaborate on aligning incident response processes.

Notification Requirements

- Define notification requirements in the event of a security incident that impacts shared information.
- Establish clear timeframes for reporting incidents.

Confidentiality and Non-Disclosure

- Emphasize the importance of maintaining the confidentiality of shared information.
- Implement non-disclosure agreements as necessary to protect sensitive data.

Data Handling and Retention

- Define data handling and retention policies for shared information.
- Specify data disposal procedures at the conclusion of the third-party relationship.

Training and Awareness

- Provide training to third-party personnel on information security policies and best practices.
- Promote awareness of the importance of information security within the third-party organization.

Continuous Monitoring and Improvement

- Implement continuous monitoring mechanisms to assess the ongoing effectiveness of third-party information security controls.
- Periodically review and update this policy to reflect changes in technology and regulatory requirements.

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 TO CONTROL RISK PARAMETERS

CONFIDENTIAL

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 and Scope

This Risk Parameters Control Policy outlines the procedures and guidelines for managing and controlling risk parameters within our company. The objective is to establish a framework for monitoring and managing risk exposures to ensure the stability and integrity of our trading platform, while adhering to regulatory requirements.

Identification of Risk Parameters

Market Risk Parameters

Identify and define market risk parameters, including price volatility, margin requirements, and exposure limits.

Credit Risk Parameters

Define credit risk parameters, covering client credit limits, concentration risk, and counterparty risk.

Operational Risk Parameters

Identify operational risk parameters, such as system downtime limits, error rates, and contingency plans.

Setting Risk Tolerance Levels

Establish risk tolerance levels for each identified risk parameter, considering the overall risk appetite of the organization.

Monitoring and Surveillance

Real-time Monitoring

Implement real-time monitoring tools to continuously assess risk exposures against established parameters.

Alerts and Notifications

Configure alerts and notifications to promptly notify risk management teams of breaches or potential breaches of risk parameters.

Risk Mitigation Strategies

Automatic Triggers

Define automatic triggers that initiate risk mitigation actions when predefined risk levels are reached.

Manual Intervention Protocols

Establish procedures for manual intervention by risk management teams in the event of significant risk breaches.

Stress Testing

Regularly conduct stress testing to assess the resilience of risk parameters under extreme market conditions.

Reporting and Communication

Develop a reporting framework to communicate risk parameter status to relevant stakeholders, including senior management and regulatory authorities.

Compliance with Regulatory Requirements

Ensure that risk parameters and monitoring practices comply with regulatory requirements in the financial industry.

Periodic Review

Conduct periodic reviews of risk parameters, taking into account changes in market conditions, regulatory requirements, and internal risk management strategies.

Documentation

Maintain comprehensive documentation of risk parameters, monitoring procedures, and actions taken in response to breaches.

Training and Awareness

Provide training to relevant staff members on the importance of adhering to risk parameters and the procedures for managing 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

POLICY TO ENSURE COMPLIANCE WITH LEGAL, STATUTORY, REGULATORY AND CONTRACTUAL OBLIGATION AND AVOID COMPLIANCE BREACHES

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 and Scope

This Compliance Policy outlines the procedures and guidelines for our company to ensure strict adherence to legal, statutory, regulatory, and contractual obligations. The objective is to prevent compliance breaches, maintain the integrity of operations, and safeguard the reputation of the organization.

Compliance Framework

Legal and Regulatory Landscape

- Conduct regular reviews to stay informed about changes in applicable laws, regulations, and industry standards.
- Establish a framework for interpreting and applying legal and regulatory requirements.

Contractual Commitments

- Maintain a repository of all contracts and agreements relevant to the business operations.
- Periodically review contracts to ensure compliance with agreed-upon terms.

Regulatory Compliance

Regulatory Authorities

- Identify and designate responsible personnel for monitoring compliance with relevant regulatory bodies.
- Establish communication channels with regulatory authorities for timely updates and reporting.

Compliance Reporting

Develop a system for the timely and accurate reporting of compliance matters to regulatory bodies as required.

Internal Compliance Controls

Compliance Risk Assessment

- Conduct regular risk assessments to identify and evaluate compliance risks associated with business activities.
- Develop strategies to mitigate identified risks.

Compliance Monitoring

- Implement a robust monitoring system to track ongoing compliance with internal policies and external obligations.
- Regularly audit and assess compliance controls.

Policies and Procedures

Documented Policies

- Develop and maintain comprehensive policies and procedures that clearly articulate compliance requirements.
- Ensure that all employees have access to and understand these policies.

Employee Training

- Provide regular training to employees on compliance policies, laws, and regulations relevant to their roles.
- Establish a system for tracking employee training and awareness.

Reporting and Escalation

Incident Reporting

Establish a confidential reporting mechanism for employees to report suspected compliance breaches without fear of reprisal.

Escalation Procedures

Develop procedures for escalating reported compliance breaches to the appropriate authorities for investigation and resolution.

Recordkeeping and Documentation

Maintain accurate and up-to-date records related to compliance activities, including audit trails, reports, and communication records.

Continuous Improvement

- Regularly review and update compliance policies and procedures based on changes in laws, regulations, and industry standards.
- Conduct post-incident reviews to identify areas for improvement in the compliance framework.

Compliance Officer

- Appoint a Compliance Officer or team responsible for overseeing and enforcing compliance measures.
- Ensure they have the authority to implement corrective actions and make necessary changes.

Legal Counsel

Retain legal counsel to provide guidance on legal matters and ensure compliance with all applicable laws and regulations.

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

REMOTE ACCESS POLICY

CONFIDENTIAL

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 and Scope

This Remote Access Policy outlines the guidelines and procedures for remote access to our company's systems and data. The objective is to ensure secure and compliant remote access while safeguarding sensitive information and maintaining the integrity of our trading platform.

Authorized Remote Access

Eligibility

- Remote access is limited to authorized employees, contractors, and partners whose roles require it for business purposes.
- Approval for remote access will be granted based on job responsibilities and security considerations.

Approval Process

- Users must submit a remote access request, detailing the need for access and the duration.
- Approval will be granted by the IT Department after a review of the request.

Security Measures

Multi-Factor Authentication (MFA)

- Remote access requires the use of multi-factor authentication to enhance security.
- Users must configure and use approved MFA methods.

Secure Connection

- Remote access must be established through secure and encrypted channels (e.g., VPN or other approved methods) to protect data in transit.

Device Security

- Devices used for remote access must comply with the organization's security policies, including up-to-date antivirus software and operating system patches.

Data Protection and Confidentiality

- Users accessing company systems remotely must adhere to data protection and confidentiality policies.
- Sensitive information should not be stored locally on remote devices.

Logging and Monitoring

- Remote access activities will be logged and monitored for security and compliance purposes.
- Any suspicious or unauthorized activity will be investigated promptly.

Termination of Access

- Remote access will be revoked immediately upon the termination of employment or when access is no longer required for business purposes.

Compliance with Regulatory Requirements

- Remote access practices must adhere to all relevant regulatory requirements in the financial industry.
- Periodic reviews will be conducted to ensure ongoing compliance.

User Training and Awareness

- Users with remote access privileges will undergo training on security best practices and the organization's remote access policies.
- Regular awareness campaigns will be conducted to reinforce security protocols.

Reporting Security Incidents

- Users must report any suspected security incidents or unauthorized access immediately to the IT Department.

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

APPLICATION SOFTWAREPOLICY

CONFIDENTIAL

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 and Scope

This Application Software Policy outlines the guidelines and procedures for the selection, usage, and management of application software within our company. The objective is to ensure the security, stability, and compliance of our trading platform while providing a seamless user experience.

Authorized Software

Approval Process

- All application software used within the organization must be approved by the IT Department.
- Users must submit requests for new software, and approvals will be granted based on security, compatibility, and regulatory compliance.

List of Authorized Software

- A maintained list of authorized application software will be available to all users.
- Regular updates to the list will be provided by the IT Department.

Security and Compliance

Encryption Standards

All application software must comply with industry-standard encryption protocols to ensure the security of user data and transactions.

Compliance with Regulations

Application software must comply with all relevant regulatory requirements in the financial industry.

Compatibility and System Requirements

- Users must ensure that their systems meet the specified requirements for accessing and using the stock broker's trading platform.
- The IT Department will communicate compatibility guidelines and system requirements.

Software Updates

- Users are responsible for keeping their application software up-to-date.
- The IT Department will communicate updates and provide guidance on the installation process.

Risk Management

- Users are encouraged to utilize built-in risk management features within the application software, such as stop-loss orders, to mitigate financial risks.

User Responsibilities

Responsible Use

- Users must use application software responsibly and adhere to all terms of service and user agreements.
- Unauthorized modification or distribution of software is strictly prohibited.

Credential Security

- Users are responsible for maintaining the confidentiality of their login credentials.
- Report any suspected unauthorized access immediately to the IT Department.

Technical Support

- The IT Department provides technical support for issues related to authorized application software.
- Users should contact the IT support team for assistance.

Market Data Usage

Guidelines on the appropriate use of market data through the broker's application software, including adherence to real-time data policies.

Terms of Service

Users must read and agree to the terms of service and user agreements associated with the broker's application software.

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

AUDIT TRAILPOLICY

CONFIDENTIAL

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

Overview

This Audit Trail Policy is an internal IT policy which provides guidance about what events on computer systems should be logged, how long logs should be retained, who can access the logs, what kind of access to logs should be granted.

Purpose

This Audit Trail Policy is required to help ensure the security of servers and the network by providing guidance about the events to be logged, how long logs should be retained, and what access to logs should be granted.

Scope

This Audit Trail Policy applies to all servers, network devices, and network security devices which are capable of producing event logs. This policy is effective as of the issue date and does not expire unless superseded by another policy.

Audit Log Requirements

- Security related activity on all servers, firewalls, routers, and workstations must be logged. Examples include: o Unsuccessful login including details such as IP address where the login was attempted from.
    - Successful login including details such as IP address where the login was done from.
    - Account management events when accounts are added, modified, renamed, or deleted.
    - Changes to policy.
    - System shutdown, system startup, or other system security events.
    - User privilege use and attempted use of privileges not granted.
    - Object access.
- If possible, the user name or ID should be recorded, time of the event, computer or IP address the action was performed from, and success or failure of the action or event.
- Audit logs must be retained on all firewalls, routers, and servers for a minimum of six months and recommended for one year. Where laws or regulations apply, logs may need to be retained longer. Business managers are responsible for informing IT management about any laws that apply to data stored on their servers. On workstations, audit logs should be allowed sufficient space to be retained six months if possible.
- Audit logs are normally reviewed daily as a part of normal maintenance on servers. This especially applies to firewalls, routers, and servers with sensitive data on them. Servers that have publically available data may be

audited less often with permission but this is not recommended since any compromised server is a serious security threat.

- All suspicious activity found in logs shall trigger the incident response plan according to policy and shall be investigated.
- All activity that indicates violation of policy shall be investigated.
- Audit logs shall not be accessible to users and shall only be writeable by programs with valid reason to write to them. Where possible programs should be able to amend the logs but not delete entries
- Permissions on audit logs must be set to prevent unauthorized access to them. The distribution of audit files, in electronic form or printed form is limited to only those who require access and have clearance to view the information.
- Sensitive information such as social security numbers, credit card numbers, and passwords should either not be retained in logs or should be masked so they cannot be read.
- Where possible without reducing security, tools should be used to automate auditing and locate patterns in audit files which would point to something requiring attention.
- Only administrators of the systems and their management should be able to review logs. In the event of a security incident, investigators may be granted full or partial access. Auditors may also be granted access to logs.
- Sufficient storage must be made available to keep audit logs for the required times at the level of detail specified.
- All security events that should be invested are to be included in the audit log and include enough information to properly investigate the event including but not limited to the time of the event and the process associated with the event.

Audit logs must be sufficient to support investigations of inappropriate use, intrusions. or any security incidents. Auditing of printer access for forensic investigation of inappropriate use is recommended.

Since audit logs are important to check events that affect the security of the organizational network and prevent unauthorized data disclosure, employees that purposely violate this policy may be subject to disciplinary action up to and including denial of access, legal penalties, and/or dismissal. Any employee aware of any violation of this policy is required to report it to their supervisor or other authorized representative.

Other Requirements

- Procedures for ensuring that automated tools comply with security requirements and auditing requirements must be developed.
- More detail about what is audited for each system type must be provided. This includes what system, security, and application events are logged on each type of server such as mail server, print server, file server, web server, and others.

- Additional detail about the level of access for the business need and based on system type and interoperability must be created.

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

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 pass codes 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

CHANGE MANAGEMENTPOLICY

CONFIDENTIAL

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 and Scope

This Change Management Policy outlines the procedures and guidelines for managing changes to systems, processes, and technologies within our company. The objective is to ensure that changes are implemented in a controlled and efficient manner, minimizing risks and disruptions to the trading platform.

Roles and Responsibilities

Change Management Team

- Designated Officer (DO): Responsible for overseeing the entire change management process.
- Technology Committee (TC): A group responsible for reviewing and approving proposed changes.

Stakeholders

- Business Units: Responsible for identifying and communicating business requirements.
- IT Department: Responsible for implementing and testing changes.
- Quality Assurance Team: Conducts testing to ensure changes meet quality standards.
- Regulatory Compliance Team: Ensures changes comply with industry regulations.

Change Request Process

Submission

- Users submit change requests using the designated form.
- Include details such as the nature of the change, justification, and potential impact.

Review

- TC reviews the change request for completeness.
- If necessary, additional information may be requested from the submitter.

Change Evaluation

Technical Feasibility

- IT Department assesses the technical feasibility of the proposed change.
- Evaluates potential impact on existing systems and infrastructure.

Impact Analysis

- Conducts a thorough impact analysis to assess the effects of the change on business processes, users, and the trading platform.

Risk Assessment

- Identifies and assesses potential risks associated with the change.
- Develops strategies to mitigate and manage risks.

Approval Process

Technology Committee

- TC reviews change requests, impact analysis, and risk assessments.
- Approves or rejects change requests based on established criteria.

Communication Plan

- Develops a communication plan to inform stakeholders about approved changes.
- Includes internal teams, customers, and regulatory bodies as applicable.

Testing and Quality Assurance

- IT Department and Quality Assurance Team collaborate to conduct comprehensive testing.
- Ensures changes meet quality standards before implementation.

Documentation and Record-keeping

- Maintains detailed records of change requests, approvals, and implementation details.
- Ensures documentation is accessible for audits and reviews.

Monitoring and Review

- Regularly monitors the performance of implemented changes.
- Conducts post-implementation reviews to identify lessons learned and areas for improvement.

Regulatory Compliance

- Ensures all changes comply with relevant industry regulations and standards.

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

ORDER LEVEL MANAGEMENT POLICY

CONFIDENTIAL

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 and Scope

This Order Level Management Policy outlines the procedures and guidelines for managing orders within our company. The objective is to ensure the fair, secure, and efficient execution of client orders, maintaining market integrity and compliance with regulatory standards.

Order Types

Market Orders

- Market orders are executed at the best available price in the market.
- Clients should be aware of potential price fluctuations during fast-moving markets.

Limit Orders

- Limit orders are executed at a specified price or better.
- Clients are responsible for setting realistic limit prices and understanding potential execution risks.

Stop Orders

- Stop orders are activated when the market reaches a specified trigger price.
- Clients must be aware of the potential for slippage, especially in volatile markets.

Execution Quality

Best Execution

- The broker is committed to achieving best execution for client orders.
- Regular reviews of execution quality will be conducted to ensure compliance with industry standards.

Order Routing

- Orders will be routed in a manner that seeks to achieve the best possible outcome for clients.
- The broker will disclose its order routing practices to clients.

Client Communication

- Clear communication will be provided to clients regarding the different order types and potential risks associated with each.
- Clients will be informed of any changes to order execution procedures.

Monitoring and Surveillance

Real-time Monitoring

- Orders will be monitored in real-time to identify any unusual patterns or potential issues.
- Automated surveillance tools will be employed to enhance monitoring capabilities.

Post-trade Analysis

- Regular post-trade analysis will be conducted to assess the effectiveness of order execution and identify areas for improvement.

Regulatory Compliance

- The broker will adhere to all relevant regulations governing order execution and market integrity.
- Policies and procedures will be regularly reviewed and updated to ensure compliance.

Order Handling Procedures

Order Validation

Orders will undergo validation checks to ensure accuracy and compliance with market rules.

Order Rejections

Clear guidelines will be established for order rejections, with reasons communicated to clients promptly.

Market Access Controls

Robust controls will be implemented to prevent erroneous orders and to manage the risk associated with market access.

System Reliability and Redundancy

Systems will be designed for reliability and redundancy to minimize the risk of system failures impacting order execution.

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 DEFINING ROLES & RESPONSIBILITIES AND PLAN OF ACTION IN ORDER TO DEAL WITH DOS/DDOS ATTACKS

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 and Scope

This DDoS Attack Response Policy outlines the procedures, roles, and responsibilities, along with a plan of action to mitigate and respond to Distributed Denial of Service (DDoS) attacks against our company. The objective is to ensure the availability, integrity, and security of our systems during and after an attack.

Roles and Responsibilities

Incident Response Team

- Incident Response Manager: Appointed individual responsible for overseeing the response to DDoS attacks.
- Incident Response Team (IRT): A team of cybersecurity experts responsible for implementing the DDoS response plan.

IT Operations

- Network Administrators: Responsible for monitoring and analyzing network traffic during an attack.
- System Administrators: Tasked with securing and optimizing server performance during and after an attack.

Communication Team

- Public Relations (PR): Manages external communication to clients, stakeholders, and the public.
- Internal Communication: Coordinates internal communication among teams and management.

DDoS Attack Response Plan

Detection and Identification

- Implement monitoring tools to detect abnormal traffic patterns and identify potential DDoS attacks.
- Collaborate with Internet Service Providers (ISPs) to identify and confirm DDoS attacks.

Activation of Incident Response Team

Once a DDoS attack is confirmed, the Incident Response Manager activates the Incident Response Team.

Traffic Diversion and Filtering

- Initiate traffic diversion through DDoS protection services or Content Delivery Networks (CDNs).
- Apply traffic filtering mechanisms to mitigate the impact of the attack.

System and Network Monitoring

Intensify monitoring of system and network performance to detect anomalies and assess the effectiveness of mitigation measures.

Communication Plan

Activate the communication team to inform clients, stakeholders, and the public about the ongoing situation, impact, and resolution efforts.

Collaboration with ISPs

- Collaborate with ISPs to implement network-level filtering and blocking of malicious traffic.
- Share attack information with law enforcement agencies if required.

Incident Documentation

Document all aspects of the DDoS attack, including the attack vector, duration, impact, and response actions taken.

Recovery and Post-Incident Analysis

System Recovery

- Gradually restore normal services once the attack has been mitigated.
- Conduct thorough testing to ensure the integrity and security of restored services.

Post-Incident Analysis

- Conduct a comprehensive analysis of the DDoS attack, identifying vulnerabilities and areas for improvement.
- Document lessons learned and update the DDoS response plan accordingly.

Legal and Regulatory Compliance

- Ensure compliance with legal and regulatory requirements related to reporting and managing cybersecurity incidents.
- Engage legal counsel to provide guidance on compliance matters.

Training and Awareness

Conduct regular training sessions to educate staff about DDoS threats, prevention measures, and response protocols.

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

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 cybersecurity 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