RISK MANAGEMENT POLICY AND FRAMEWORK

Introduction and Purpose

This policy establishes a structured framework for identifying, assessing, mitigating, and monitoring risks faced by qualified stock brokers. It ensures compliance with regulatory requirements, protects client interests, and promotes operational resilience.

A Risk Management System is integral to an efficient Risk system. We have put in place a comprehensive risk management system, which is constantly upgraded as per the Exchange, SEBI & PMLA norm and also as per Market Movement.

The Model of Risk Management & Surveillance System in Jainam Broking Limited (Now onward refer as JBL) consists of JBL Owned Branches & Authorised Persons.

The RMS system is setup to minimize the risk of loss through a dynamic risk management policy which is an essential feature of our operations.

It is important to note that our Risk Management Policy is not an insurance against losses but these are measures and precautions that are adopted by us to minimize the risk.

All the staff related to Operations, KYC, IT, RMS, Dealing, Clients Funds and Securities, and related Branches, Branch Managers, and Authorised Persons (Sub-broker) needs to understand and follow the policy as it is the integral part of company.

Senior management including COO, CTO, CFO, CO shall actively promote risk awareness and risk management practices, including providing appropriate training to all associates, incentivizing them to identify risk, and providing appropriate recognition.

The Clients have to be aware of the RMS Policy of Jainam Broking Ltd (JBL) and how the Policy of JBL shall operate to regulate and monitor their transactions of its Clients to mitigate Risks and their responsibilities thereof. JBL shall intimate its Clients vide Circulars and updation on the official website of JBL (www.jainam.in) regarding Risk Management Policy and Surveillance Policy of JBL. Clients are advised to follow the Circulars and the official website of JBL (www.jainam.in) and those of Securities & Exchange Board of India (www.sebi.gov.in), National Stock Exchange of India Limited (www.nseindia.co.in), Bombay Stock Exchange of India Limited (www.bseindia.com), Multi Commodity Exchange of India Limited (www.mcxindia.com), Central Depository Services (India) Limited (i.e. www.cdslindia.com), National Securities Depository of India Limited (i.e. www.nsdl.co.in) and/or any other relevant websites.

The client shall invest/ trade in those securities/ contracts/ other instruments admitted to dealings on the Exchanges as defined in the Rules, Byelaws and Regulations of Exchanges/ Securities and Exchange Board of India (SEBI) and circulars/notices issued there under from time to time. JBL, its Authorized Person(s) and the client(s) shall be bound by all the Rules, Byelaws and Regulations of the Exchange and circulars/notices issued there under and Rules and Regulations of SEBI and relevant notifications of Government authorities as may be in force from time to time. The client shall satisfy itself of the capacity of J B L to deal in securities and/or deal in derivatives contracts and wishes to execute its orders through JBL and the client shall from time to time continue to satisfy itself of such capability of JBL before executing orders through JBL. JBL shall continuously satisfy itself about the genuineness and financial soundness of the client and investment objectives relevant to the services to be provided. The Authorized Person(s) shall provide necessary assistance and co-operate with JBL in all its dealings with the client(s).

JBL shall ensure to place orders and execute the trades of the client as per the order/trade received from client/s, only in the Unique Client Code assigned to that client. JBL shall inform the client and keep him apprised about trading/settlement cycles, delivery/payment schedules, any changes therein from time to time from various circular on its website / email/ SMS/ trading application or any other modes, and it shall be the responsibility in turn of the client to comply with such schedules/procedures of the relevant stock exchange where the trade is executed. JBL shall ensure that the funds received from the client of JBL shall be kept in a separate Client Upstream bank account only, distinct from his/its own account or account of any other client and shall not be used by JBL for itself or for any other client or for any purpose other than the purposes mentioned in Rules, Regulations, circulars, notices, guidelines of SEBI and/or Rules, Regulations, Bye-laws, circulars and notices of Exchange. Where the Exchange(s) cancels trade(s) suo moto all such trades including the trade/s done on behalf of the client shall ipso facto stand cancelled, JBL shall be entitled to cancel the respective contract(s) with client(s). The transactions executed on the Exchange are subject to Rules, Byelaws and Regulations and circulars/notices issued thereunder of the Exchanges where the trade is executed and all parties to such trade shall have submitted to the jurisdiction of such court as may be specified by the Byelaws and Regulations of the Exchanges where the trade is executed for the purpose of giving effect to the provisions of the Rules, Byelaws and Regulations of the Exchanges and the circulars/notices issued thereunder.

The Client shall pay to JBL brokerage and statutory levies as are prevailing from time to time and as they apply to the Client's account, transactions and to the services that stock broker renders to the Client. JBL shall not charge brokerage more than the maximum brokerage permissible as per the rules, regulations and bye-laws of the relevant stock exchanges and/or rules and regulations of SEBI

The Client acknowledge's and accept's that there can be "<u>no guarantee of profits</u>" or no exception from losses while executing orders for purchase and/or sale of any Securities Transactions being traded on Stock Exchanges. The client agrees that the Employees and/or Authorized Person(s) has NOT been authorized to give any advice or recommendation and the Company is neither bound by any loss caused to the client by any such advice.

The Client agrees and voluntarily accepts the Risk Management Policy of JBL and undertakes the responsibility to avail the Securities trading through JBL adhering to the Policies of JBL and the Rules, Bye-Lays, Circulars of the Stock Exchanges where JBL is a Trading cum Clearing Member.

The Compliance Officer shall be Responsible for the implementation of the Risk Management Policy. The Compliance Officer shall be assisted by the RMS and Surveillance Team / Officer. The Compliance Officer shall have the discretion to take assistance/help from any professionals and/or software for the better Monitoring of Risk Management Policy, with prior approval of the Board of Directors, without diluting the accountability and responsibility of the Compliance Officer. All the Employees, Branches, Branch Manager, and Authorized Person of the Company needs to understand the risks involved in Securities trading on the Stock Exchange(s) and follow the policy as it is the integral part of company and it is important for them to communicate the same to the Clients'.

<u>Objective :</u>

The main objective of this Policy is to ensure sustainable business growth with stability and to promote a proactive approach in reporting, evaluating and resolving risks associated with the Company's business.

In order to achieve the key objective, this Policy establishes a structured and disciplined approach to Risk Management. In order to guide decisions on risk related issues, the specific objectives of this Policy inter alia are:

1. To ensure that all the current and future material risk exposures of the Company are identified,
2. assessed, quantified, appropriately mitigated, minimized and managed i.e. to ensure adequate

systems for risk management.

3. To establish a framework for identification of internal and external risks specifically faced by the Company, in particular including financial, operational, sectoral, sustainability (particularly, trading related risks), information, cyber security risks or any other risk as may be determined by the Risk Management Committee ("the Committee") for the company's risk management process and to ensure its implementation.
4. To measure risk mitigation including systems and processes for Internal Control of identified risks.
5. To enable compliance with appropriate regulations, wherever applicable, through the adoption of best practices.
6. To assure business growth with financial stability.

Responsibility of Risk Management and Surveillance Team:

The Designated Director, Compliance Officer and CXO level shall be responsible for the day to day supervision, monitoring and implementation of this RMS Policy. The Designated Director/ Compliance Officer shall be assisted by a Team of Risk Management and Surveillance Officers (in short the "RMS Officers"), for the monitoring and implementation of the RMS Policy. The Risk Management and Surveillance Team shall have a Team leader who shall Report to the Designated Director/ Compliance Officer for the fast and optimum decision making process.

The Risk Management Officers shall be responsible to prepare the available Collateral Deposits of each and every Client at the Beginning of the Day based on the Margin available and check capital adequacy for exposure and requirements of Clients and also monitor Client's Orders, Patterns of Trades, Order Rejections, the MTM Profit/Loss incurred out of trades and benchmark Margin v/s Exposure of Clients. Decisions with regard to debarring a Client for fresh open positions, subjecting client on risk reduction mode, squaring off positions on account of MTM Loss or Margin Shortfalls and Continuous Debits which breach the threshold mandate of debit balances continues beyond the fifth trading day, as reckoned from date of pay-in shall be reported to the Designated Director/ Compliance Officer.

The Risk Management Officers (RMS Officer) shall assist and report to the Compliance Officer on a daily basis in respect of the Client Codes Modified/Transferred.

The Compliance Officer shall take all necessary steps to monitor, document, analyze and report the findings to the Board Members / Risk Management Committee as well as the relevant Stock Exchanges and/or regulatory bodies, in a time bound manner, as detailed hereunder and/or as mandated by the Stock Exchanges and/or regulatory bodies and report the same to the Designated Director.

The Compliance Officer shall exercise his/her independent judgment and take adequate precautions to ensure implementation of an effective monitoring mechanism, based on the day-to-day activities of the clients, general market information and the facts and circumstances and report the same to the Designated Director.

The Board of Directors and Risk Management Committee shall peruse, review and provide necessary guidance with regard to the "Risk Management and Surveillance Policy", periodically, for strengthening the processes.

RMS Function includes:

- To check capital adequacy for exposure and requirements of the client
- Allocate Margin in CC according to client available collateral with JBL
- Set Client Exposure / limits for dealing in various segments
- Monitoring of Clients Order, Patterns of Trade, Order rejections, increasing of Exposure/limits.

JAINAM BROKING LIMITED

- Monitoring MTM profit/loss incurred out of trades.
- Benchmarking Margin v/s Exposure of client
- Decision taking with regard to squaring off positions on account of MTM loss or Margin shortfalls or any other reasons that may come across
- Ensure other Trading compliances

Risk management works by identifying potential risks, assessing their likelihood and potential impact, and implementing strategies to mitigate or avoid those risks.

The risk management process typically involves several steps:

Comprehensive Risk Management Framework

Securities & Exchange Board of India by its Circular No. MRD/DoP/SE/Cir-07/2005 dated February 23, 2005 has laid the Comprehensive Risk Management Framework for Cash market

Overview

The core of the risk management system is the liquid assets deposited by members with the exchange/clearing corporation. These liquid assets shall cover the following four requirements:

A. Base Minimum Capital: Capital required for all risks other than market risk (for example, operational risk and client claims).

B. VaR Margins: Value at risk margins to cover potential losses for 99% of the days.

C. Extreme Loss Margins: Margins to cover the expected loss in situations that lie outside the coverage of the VaR margins.

D. MTM (Mark To Market) Losses: Mark to market losses on outstanding settlement obligations of the member. At all points of time, the liquid assets of the Trading Member shall be adequate to cover all the above four requirements. There are no other margins in the risk management system. JBL shall abide by the provisions laid by the SEBI Circular No. MRD/DoP/SE/Cir-07/2005 dated February 23, 2005.

Risk Identification, Risk Categories

Regulatory & Compliance Risk

- Maintain valid licenses and registrations with regulators (e.g., SEBI, SEC).
- Implement robust AML/KYC procedures.
- Conduct quarterly compliance audits.
- Immediate reporting of breaches to regulators.
- Major Risks associated with non-compliance with regulations, laws, and industry standards.

Financial Risk

- Monitor market volatility and stress test portfolios.
- Maintain liquidity buffers to meet margin calls.
- Diversify exposures across sectors and instruments.
- Establish credit limits for clients and counterparties.

Operational Risk

- Ensure redundancy in trading platforms and settlement systems.
- Document standard operating procedures (SOPs).
- Conduct regular disaster recovery (DR) drills.
- Vendor risk assessments before onboarding.

- Risk such as faulty systems which can cause erroneous execution of orders from client's account and/or unauthorised trading on behalf of the client and misutilisation of client's sensitive information by any employee of the organisation.
- Risks arising from internal processes, systems, human errors, and external factors like fraud or technology failures.

Cybersecurity Risk and Technology Risk :

- Enforce multi-factor authentication (MFA) for all systems.
- Encrypt client data and trading records.
- Conduct annual penetration testing.
- Maintain an incident response plan with defined escalation protocols.
- Technology Risk
- To mitigate these technology-related risks, management should implement robust technology risk management strategies. This includes conducting regular technology risk assessments, developing disaster recovery plans, enhancing cybersecurity measures, ensuring compliance with technology-related regulations, and maintaining vigilant monitoring of technology systems and processes.

Reputational Risk

- Transparent communication with clients regarding risks and fees.
- Ethical sales practices; avoid mis-selling.
- Crisis communication plan for adverse events.
- Regular monitoring of media and client feedback.

Risk Assessment & Monitoring

- Risk Register: Maintain a live document scoring risks by likelihood and impact.
- Reporting Frequency: Risk register/ assessment to present RMC meeting; quarterly updates to the Board.

Mitigation Strategies

- Preventive controls (e.g., compliance training, system safeguards).
- Detective controls (e.g., monitoring, audits, alerts).
- Corrective actions (e.g., incident response, remediation plans).
- Insurance coverage for operational and cyber risks.

Other Related Risk includes as under :

Market Risk: This includes risks associated with fluctuations in stock prices, interest rates, currency exchange rates, and overall market volatility.

Credit Risk: The risk that clients or counter parties may fail to meet their financial obligations, such as failing to pay for securities purchased.

Fraud Risk: The risk of financial loss due to deceptive or illegal activities, including internal fraud by employees or external fraud perpetrated by clients or other parties.

Risk due to outsourcing of activities to third parties:-The risk associated with delegating activities to third-party vendors or service providers, which can introduce operational, security, and compliance risks.

Risk in KYC & Account opening process:

Risk arising during KYC and account opening process such as submission of incomplete KYC forms by the Clients, submission of fake information with an intention to commit frauds and non-updation of information submitted as and when there is any change in the information submitted during KYC.

Common Tactics in KYC Frauds :

There are several methods employed by scammers in committing KYC scams. These include:

1. Fake KYC updates: This involves contacting individuals under false pretences, claiming that their accounts require immediate KYC verification.
2. Phishing: Cybercriminals use deceptive means, like sending links to fraudulent websites or apps, to trick individuals into disclosing sensitive information.
3. Identity theft: Cybercriminals use another individual's identity for financial gain, often leading to the individual's financial losses and credit score damage.
4. Smishing: Smishing involves sending malicious messages with dangerous links or attachments, disguised as legitimate communication from reputable sources.

KYC scam detection involves being vigilant about unsolicited communication from unknown sources, claiming to represent financial institutions. It's important to remember that Jainam Broking Ltd will never ask for sensitive information like OTP or passwords over the phone or via email.

Measures to Mitigate Risks for KYC (Know Your Customer) and account opening process :

Measures to mitigate risks during the stock broker KYC (Know Your Customer) and account opening process are comprehensive and practices focused on preventing financial crimes, fraud and protecting investors. These include identity verification, risk profiling, ongoing monitoring, and regulatory compliance.

Mitigation Measures During Account Opening (Onboarding Checks) :

Risk Profiling and Due Diligence:

- **Assigning a risk score** (low, medium, or high) to each customer based on various factors like geographical location, customer type (e.g., Politically Exposed Persons (PEPs) are high-risk), occupation/source of income, and the nature of intended transactions.
- Conducting **Enhanced Due Diligence (EDD)** for high-risk customers, involving verification of source of funds, beneficial ownership structures, and economic purpose of the account.
- Performing **sanctions and anti-money laundering (AML) screening** to check if the potential client is on any watchlists or in adverse media.

Process and System Controls:

- Ensuring clients fill out KYC forms completely and striking off blank fields to prevent later misuse.
- Implementing **real-time bank account verification** to ensure the bank details provided belong to the legitimate owner.
- Using secure, potentially automated, systems to manage data, reducing manual errors and protecting sensitive customer information from data breaches.
- Obtaining a clear understanding of all brokerage, commissions, fees, and other charges to ensure transparency and prevent disputes later.

Mitigation Measures for Ongoing Measures (Continuous Monitoring) :

Transaction Monitoring:

- Continuously monitoring customer activities and transactions for unusual patterns that deviate from their established risk profile or declared income.
- Using systems automated systems to flag suspicious activities, such as large, unexplained transactions, or activities inconsistent with the client's profile.

Regular Reviews and Updates:

- Periodically updating KYC records and client information, with the frequency depending on the assigned risk category (e.g., high-risk clients require more frequent review).

Reporting and Compliance:

- Establishing clear internal policies and procedures for identifying and reporting suspicious transactions to relevant regulatory bodies like the Financial Intelligence Unit (FIU-IND).
- Conducting regular internal /external audits to assess the effectiveness of the AML/KYC program.
- Providing ongoing training to employees on compliance requirements on AML.

By implementing these measures, JBL can effectively manage and mitigate the risks associated with the KYC and account opening processes, ensuring compliance with regulations and protecting both the firm and its clients

Mitigation Measures for Operational Risks :

JBL mitigates operational risks through robust internal controls, a strong compliance culture, leveraging technology, and adhering to strict regulatory guidelines to protect clients and the company.

Internal Processes and Controls

- **Segregation of Duties:** Ensure that activities involving potential conflicts of interest are handled by different individuals and functions (e.g., front office, back office, fund pay in and payout, securities payin and payout, depository process, billing process and related control and operational functions).
- **Mandatory Record-Keeping**: Maintain verifiable records of all client orders, trades including physical signed records, telephone recordings, emails or logs for internet based and mobile based transactions.
- **Order Confirmation**: Clients must receive timely confirmation of their trades via email/SMS directly from the exchange/depository at the end of the day. Also JBL to send timely confirmation of their trades via email/SMS and to send contract notes.
- **Daily Reconciliation**: Conduct daily reconciliation of client positions, cash funds, clients margin pledge securities, and internal ledgers with external parties (clearing corporations/depositories) to quickly identify and resolve any anomalies.
- **Account Opening Due Diligence**: Strictly follow Know Your Customer (KYC) guidelines and conduct thorough client due diligence, including in-person verification and assessing financial capability, to prevent fraudulent activities.
- **Internal Audit**: Internal audit to be conducted to review and test the effectiveness of existing risk management procedures and internal controls.

Systems and Technology

- **Automation**: Automate routine tasks to reduce human error and increase efficiency.
- **System Controls**: Implement robust system controls, including order tracking with time-stamping, client Id verification, and real-time monitoring systems to detect and prevent unusual trading activities.
- **Business Continuity Planning (BCP)**: Regularly test BCPs and IT disaster recovery plans to ensure critical functions can continue during and after a disruption.
- **Cybersecurity**: Implement / Enhance robust cybersecurity measures, such as multi-factor authentication and regular penetration testing, to protect against data breaches and system failures.

People and Culture

- **Risk Culture**: Promote a strong risk culture where employees are encouraged to speak up about potential risks without fear of blame.
- **Employee Training**: Provide regular and comprehensive training on risk management practices, regulatory requirements (like anti-money laundering (AML) and KYC), and the code of conduct.
- **Performance Measurement**: Ensure that an individual's or business unit's performance assessment and remuneration (especially in the front office) consider their adherence to risk limits and the level of operational risk generated.

External Events and Compliance

- **Client Fund Segregation**: Hold client funds in separate client Upstream bank account and securities in separate CUSPA account and emarked as client securities towards Margin Pledge, strictly segregated from the broker's own assets, to prevent misutilisation.
- **Monitoring and Reporting**: Use Key Risk Indicators (KRIs) to monitor risk levels in real-time and report significant incidents and overall risk exposure to Senior management and the Board of directors regularly.
- **Investor Protection Fund (IPF)**: Be a member of stock exchange IPF trusts, which provide compensation to investors in case of broker default, thus building client confidence.

By implementing these integrated measures, stock brokers can build operational resilience and protect the interests of their clients.

Risk Governance Structure:

Risk management is a collaborative effort with clear accountability assigned across the organization.

CXO Level Roles and Responsibilities:

The risk management framework specifies the roles of various CXOs, who are the primary owners of risks in their respective functional areas.

Chief Executive Officer (CEO)

Overall Responsibility: Bears ultimate responsibility for all risks at the company level.
Framework Oversight: Ensures the risk management framework is effective and aligns with the firm's business objectives and risk appetite.

Decision Making: Approves major corrective actions and escalations.
Reporting: Ensures risk management outcomes are reported to the Board and relevant committees monthly or quarterly.

Chief Risk Officer (CRO) / Risk Officer / Head of RMS

Independent Function: Leads the independent risk management function.
Framework Implementation: Responsible for the implementation and ongoing review of the enterprise-wide Risk Management Framework (RMF).
Monitoring & Reporting: Puts in place mechanisms for risk reporting, including stress testing, defining risk metrics, generating early warning signals, and escalating material incidents to the Board/CEO.
Coordination: Reviews and coordinates specific risk management responsibilities of other CXOs.

Chief Operating Officer (COO) / Head of Operations

Operational Governance: Oversees and is responsible for the governance of risks pertaining to the operations department, including administration and processing risks.

Process Management: Ensures proper implementation and formulation of Standard Operating Procedures (SOPs), adequate due diligence of outsourced vendors, and the implementation of integrated management systems.

Incident Management: Takes immediate corrective action for operational non-compliance or findings and reports to the CRO.

Chief Financial Officer (CFO)

Financial Risk Governance: Responsible for the governance of financial accounting and the company's financial risks.

Liquidity & Credit Oversight: Provides inputs to the CRO on liquidity and credit risk thresholds and ensures adequate capital/liquidity is maintained.

Reporting: Ensures accurate financial reporting and manages the risks associated with financial controls.

Compliance Officer (CO)

Regulatory Adherence: Responsible for the governance of regulatory and compliance risks.

Policy Implementation: Ensures adherence to all relevant SEBI/Exchange guidelines and circulars, including AML and KYC procedures.

Monitoring: Monitors for mis-selling incidents and ensures all staff adhere to a strict code of conduct.

Chief Information Security Officer (CISO) / Chief Technology Officer

Cybersecurity Governance: Responsible for the governance of technology, information security, and cyber risks.

System Integrity: Ensures the implementation of a robust cybersecurity and cyber resilience framework, including BCP (Business Continuity Plan) and DR (Disaster Recovery) drills.

Monitoring: Identifies, analyzes, and reports on system-related near misses, loss events, and fraud incidents.

Process of Risk Identification, Assessment, Evaluation and Treatment

The organization adopts a systematic approach to risk management involving the following steps

Risk Identification: Proactively identifying potential internal and external events that could impact objectives. This involves input from all functional heads and a review of past incidents.

Risk Assessment: Once the potential risks have been identified, they are assessed based on their likelihood of occurrence and potential impact. This step involves analyzing the severity of the risk and the probability of its occurrence. Evaluating the likelihood and potential impact (financial, reputational, operational) of identified risks to prioritize them.

Risk Evaluation: After the risks have been assessed, they are evaluated based on their priority and importance. This step involves determining which risks are the most critical and require immediate attention.

Risk Treatment & Mitigation: The final step in the risk management process is to implement strategies to mitigate or avoid the identified risks. Developing and implementing strategies to avoid, reduce, transfer (e.g., through insurance), or accept risks, in line with the defined risk appetite

Monitoring and Review: Continuously tracking risks and the effectiveness of mitigation plans, adapting to changes in the internal and external environment

Communication and Reporting: Ensuring transparent and timely communication of risk information and the status of mitigation efforts to relevant stakeholders, from employees to the Board

RMS Policies and Procedures

Risk management policy should strive to address the root cause of the risks and try to prevent recurrence of such risks. The policy shall assess the likely impact of a probable risk event on various aspects of the function of Jainam Broking Limited such as impact on investors, financial loss to the Company, impact on other stakeholders in the market, reputational loss and lay down measures to minimize the impact of such event in relation to all the trading activities for Clients is handled by RMS & Surveillance Dept.

A. Setting up client's exposure limits

The Exchange may from time to time fix client exposure limits in the interest of orderly working of the markets. Within that overall ceiling, a client can trade within the exposure limit set from time to time by the Broker for the client.

Exposure Limit is fixed on the basis of the funds and value after hair cut of the securities provided by the client for margin. Clients are requested to adhere to the exposure limits as crossing the limit may involve either a call for margin or restriction on further position / exposure.

JBL may need to vary or reduce or impose new limits urgently on the basis of risk perception, risk profile of the client and other factors considered relevant including but not limited to limits on account of exchange / SEBI directions / limits (such as broker level / market level limits in security specific / volume specific exposures etc.).

Sometimes the JBL may be unable to inform the client of such variation, reduction or imposition in advance. JBL shall not be held responsible for such variation, reduction or the client's inability to route any order through trading system on account of any such variation, reduction or imposition of limits.

In the sole discretion of the JBL, a client may be allowed to trade by increasing limit against margin provided by client during market time on ongoing basis in form of Fund Transfer or pledging security in favour of Broker to repledge further to Clearing Corporation.

1. **While computing the available margin following parameter consider-**

Margin based limit is set on combined basis for Cash & F&O & CD Segments clear credit lying in client's settlement and margin ledger account

Beneficiary holdings and collateral holdings (after deduction of applicable h/ c)

Any Online funds transfer or hold amount through bank gateway

Credit received against sale of- securities

Margin amount of open positions (in case of derivatives)

All the cheques collected against trading positions, preferably carry a valid MICR number.

All the cheque dishonor cases are viewed seriously and debit amounts in such accounts will be cleared from surveillance dept. The normal rule for 5 days debit will not be applicable while selling the shares in cheque dishonor issues.

1. Exposure limits shall be only against approved securities as decided by the Exchanges/JBL from time to time. JBL may from time to time change the applicable hair cut or apply a haircut higher than that

specified by the Regulators/Exchanges.

2. In case of derivatives, Clients shall be allowed to trade only up to the applicable client wise position limits set by the Exchanges/Regulators from time to time

3. List of approved collaterals / securities along with applicable haircut, is subject to revision from time to time based on Exchange approved list,

4. In order to ensure smooth settlement on T + 1 day, client has to ensure that entire balance payment against purchase and entire delivery against sale orders reaches the broker's specific bank and DP a/c on T + 1 day.

5. In case of clients' failure to deposit funds against their purchases by above mentioned time schedule, penal action against the clients at the discretion of the stock broker will be taken, which will include non-delivery of shares to them and transfer it to CUSPA Account, sale of shares in the market.

6. In case of clients' failure to deliver shares against their sale orders by the above time schedule, penal action will be taken by the stock broker at his discretion which will include penalty for short delivery as imposed by the Exchange, auctioning of shares by the Exchange, debiting on account of internal shortage. Additionally, a penalty @1% will be charged on auction value.

B. Setting up Terminal/Branch Level limits

Trading Terminals are allotted to Members by exchanges. These terminals enable members to place, modify and execute orders on behalf of clients. There may be instances where due to punching error unusual orders may be placed at high prices which might lead to execution of unrealistic orders or orders being executed at unrealistic prices. In cases where the order/price of such orders is high, it might lead to huge losses to broker. In order to avoid such a situation it is imperative that certain limits are prescribed for each terminal allotted to member broker.

We ensure documentation of internal controls on areas like order modification / cancellation, client code changes and post-trade activities are in place and are being updated from time-to- time.

We ensure monitoring mechanism for client's debits / obligations and appropriate collection procedures.
The following limits shall be defined for each terminal:
Quantity Limit for each order
Value Limit for each order
User value limit for each user ID
User quantity limit for each user ID
Branch value limit for each Branch ID
Spread Order Quantity and Value Limit (EQ Derivatives & Currency Derivatives segment)

Checks in place

1. We have a dedicated Risk monitoring team who monitor the exposure, limit, etc.
2. We have Terminal which has a facility to block the client as well as restrict to use over exposure. No user/ branch will be provided unlimited limit.
3. Limits shall be monitored on daily basis, taking following criteria's: Turnover, Exposure, Past trends, Location, Fund/Collateral.
4. Trading in illiquid scrip shall not be permitted.
5. 20% probable negative and 17.74% probable positive scenario for clients having larger position
6. Single Order Quantity
7. Single Order Value
8. Restrict illiquid Options Strikes

9. Restrict far month illiquid Contracts
10. Restrict BAN securities
11. Client wise, Member wise Limit
12. Unfavorable Order Price restriction

C. Order Receipt and Execution

All Orders routed through Odin / Nest / Greek / Neat / Bolt & Now are monitored by our risk department and after their confirmation about client's financial and margin status order get executed.

The dealers take utmost care while executing the trades of the clients regarding the accuracy of Client Code, Quantity and Price etc. The orders from the client's are promptly executed by the dealers and the oral confirmation of the placement of the orders is immediately provided to the clients. Moreover, only registered clients are allowed to enter the dealing room for placing the orders.

The clients are divided into groups among the dealers and sub brokers at head office level, so that particular dealer can serve a particular group of clients which helps dealer to understand the client investment strategy in a better way & serve them accordingly. The orders are entered instantly by the dealer on the instruction given by the client. On execution of valid order into trade, dealers confirm the trade with the client so as to avoid any future dispute.

At the end of the trading hours, the dealer informs the clients about the execution of the orders placed by the clients. Also a trade confirmation SMS message covering details of all the trades executed is forwarded to client after completion of trading hours on registered Mobile No. of the client.

D. Client Code Modification:

Trades are done only on the exchange platform and if any trades need to be transfer become of wrong punching code it is done in the exchange platform system. Client code modification is accepted only prior to post closing session. Client code modification will be done within the time limit given by the respective exchange.
Every request for client code modification is to be sent to RMS dept in the predefined format and proper care should be taken in filling the Exchange order number, trade number, old client code, new client code, and the reasons for wrong Punching.

The reason for the modification is to be analyzed by the risk management department with regards to clients ledger a/c; Demat a/c; trading pattern etc. & if found to be genuine then modification will be approved / Modification will be allowed only in which error was occurred genuinely.

Penalties & actions taken by the exchange against the broker / member shall be passed on to the respective client & in addition penalties & action shall be taken against the Sub-Broker's /AP's / Branches / Dealers.

E. Margin Collection Procedure

The JBL has RMS department at its corporate office situated at Jainam House, New Passport Office Road, Piplod, Surat - 395007. The JBL has a RMS (RISK Management System) Team, who is responsible for setting up the Client wise Trading limits, Margin collection & Reporting procedure as described below:

Client Limits are allowed as per margin norms of the relevant exchanges. Clients are required to provide upfront margin in the form of funds / securities (after appropriate haircut as prescribed by Exchange from time to time) before any trade.

RMS department monitor all orders & trades given by clients and executed in the trading terminal. The departments are also vigilant about all order rejections and spurt in exposures. The JBL takes proper and

adequate margin from clients as per the exchange/SEBI norms in the form of funds/Securities and report the same to the exchange as per the guideline of exchange.

We take Margin in the form of Funds through Account Payee Cheque, Electronic Fund Transfer and Securities. We have at most monitoring system which bars the acceptance of third party cheque. In case, client provide securities towards margin, we accept only from registered DP ID of client. On receipt of securities, RMS applied the required hair cut as per exchange VAR.

At the end of the day, Shortage of Client margin is calculated and reported to the Exchange. During the trading hours if any short margin observed in Peak Snap shot, RMS team follow internal RMS policy, due diligence and update the status to the respective branch/ SB/AP and to clients .In case client doesn't respond RMS team Sq-off the open position and subsequently intimate to the client.

Trading limit is set by RMS based on the available margin amount and calculated by considering the trading price prior to trading day (T—1 day) on daily basis. The RMS team do monitor the debtors and if client exceeding the exchange norms of T+5 day the trading is been halt.

F. <u>Margin Reporting Procedure:</u>

On a daily basis Exchange provides Margin Files to the Trading member in F&O, Currency and Commodity Segment. Accordingly Margin reporting done on various exchanges.

Mechanism for regular reporting of Margin

Security pledged in favour of JBL on current day (prior to placing order on T Day) by client in different segments (BSE/NSE/FO/CURR) of the Exchange will be consider for margin collection.

Only exchange approved stock will be considered for margin collection with subject to a haircut of VAR margin as per Exchange.

Margins taken in the form of securities in the approved list to be valued as per the closing rate on the previous trading day and not the trading day, with an appropriate hair-cut

Only pledged securities available with the Member for respective client in different segments of the Exchange shall be considered for margin collection and reporting.

Accordingly, only securities received in pay out shall be considered only after it is actually received from the clearing corporation and pledged in favour of JBL. However pay-in received from clients for such securities may be considered while calculating the ledger balance for the purpose of reporting of margins if EPI Margin benefit received from Clearing Corporation for early pay-in of the securities is done through UCC Block mechanism.

Cheques dishonored/reverse or not cleared up to T+5 working days should not be considered for Margin Money.

After preparing margin report file, RMS person forward reporting file to person who is authorized to recheck the report file before uploading on Collateral Interface for Members. Status of the file uploaded shall be checked regularly on the day of uploading after a few hours of uploading the same.

Penalty if any occurring out of the short payment will be debited to the respective client's account after T+5 days information related to margin applicable, utilized and required / balance in respect of each client is to be sent on a daily basis to the respective clients in both the segments.

Client code and name, Trade day (T)

Total margin deposit placed by the client up to T day
Margin utilized up to the end of day T

Margin deposit placed by the client on day T
Margin adjustments for day T

Margin status (balance with the member/due from the client) at the end of day T.
We maintain proper records of collateral received from clients.

Margin Shortfall Penalty

We charge upfront margin short penalty to respective client only as levied by Exchange.

G. Right of Sale of client's securities or closing the client's open position without giving notice

JBL maintains specific banking and depository accounts, informed to the clients from time to time, for handling clients' funds and securities. The clients shall ensure timely availability of funds /securities in required form and manner, within stipulated time and in the designated bank and depository account(s) for meeting their liabilities and obtaining proper credit thereof. JBL does not undertake responsibility for any delay or other consequences arising from payment to any other account or non receipt in time and manner in the designated account(s).

In the event of the Client failing to maintain / supply applicable margin money required to sustain the outstanding market positions of the Client, the company shall be entitled, at its option and liberty, to liquidate / close out all outstanding market positions or any part there of such that the outstanding market positions are either zeroed out or reduced to an extent where available margin covers the market positions remaining after such square off.

Any and all losses and financial charges on account of such liquidation/closing-out shall be charged to and borne by the client. The company shall also have right to close out any intraday positions taken by the client, in above circumstances. Such liquidation/ close out may be without any prior reference or notice to the client.

RMS Team may initiate liquidation of securities in following circumstances:

In case of Margin Trades, if the open position is neither squared off nor converted to Delivery by Client(s) within the stipulated time.

In case of Margin Trades, where Mark to Market Loss on the open position has reached the 80% of the margins placed with JBL and the Client(s) have not taken any steps either to replenish the margin or reduce the Mark to Market Loss.

In all other cases where the margin or security placed by the Client(s) falls short of the requirement or the limits given to the Client(s) have been breached where the Client(s) have defaulted on their existing obligation/ failed to make payments/deliver securities to JBL with the stipulated time Extreme volatility in the market in particular scrip of both the segment

There are any restrictions imposed by exchange or regulator on the contract(script)

The client is undertaking any illegal trading practice or the client is suspected to be indulging in the money laundering activities or suspicious trade or trading in illiquid stock

The client has taken or intends to take new position in a security which is in the banned period

There are any unforeseen adverse market conditions or any natural calamity affecting the operation of the market.

H. Refusal of orders for "Penny Stocks" (Illiquid stocks)

A Security that trades at a relatively low price and has small market capitalization is a penny stock. These types of stocks are generally considered to be highly speculative and high risk because of their lack of liquidity, large bid-ask spreads, small capitalization and limited following and disclosure. Depend on the market condition and RMS policy of the company RMS reserve the right to refuse to provide the limit in Penny stocks and losses if any on account of such refusal shall be borne by client only.

I. KYC & ACCOUNT OPENING PROCESS

JBL likes to pay special attention to dealing in "Penny Stocks". To this end:

JBL may refuse to execute any client's orders in "Penny Stocks" without assigning any reason or the same.

Any large order for purchase or sale of any penny stock shall be taken prior approval from RMS and the dealing of such stock will only be allowed through Head Office. It will be client responsibility and respective Branch Manager/Dealer or RM duty to ensure that trading in "Penny stocks" does not result in creation of artificial volume or false or misleading appearance of trading. Further it also does not operate as a device to inflate or depress or cause fluctuations in the price of such stocks Dealer/RM/Branch Manager should ensure that the Clients should not place orders in "Penny stocks" at prices which are substantially different from the prevailing market prices. Any such order is liable to be rejected at the sole discretion of JBL. In case of sale of penny stocks as approved by RMS, clients shall ensure the delivery of shares to JBL before the pay-in date. The Company shall not be responsible for non-execution / delay in execution of such orders and consequential opportunity loss or financial loss to the client

The Company has the right to revise the list of such securities / contracts on a periodic basis. Client can obtain the information about the updated list of securities from the Relationship Manager/Dealing office.

I. Conditions under which a client may not be allowed to take further position or his existing position may be closed

JBL shall have absolute discretion and authority to limit client's volume of business or to close any existing position of a client without giving any prior notice to the client under following conditions:

SEBI or Exchange imposing restrictions on further exposures in cases of extreme volatility in the market or in a security or group of securities.

Client or the Broker exceeding or touching exposure limits set by the Exchange in the particular scrip.

Reasonable doubt as to bonafide of the transaction or identity of the client in the light of the financial status and objectives as disclosed in the KYC form.

Reasonable doubt as to the transaction being cross trade, circular trade, fraudulent practice or connected with price manipulation or market rigging.

SEBI or other competent authority issuing a debarment order against the client from buying, selling or dealing in securities, unless the order is vacated.

The client has taken or intends to take new position in a security which is in the banned period
Due to abnormal rise or fall in the market, the markets are closed.

JBL shall also have a right to close existing positions of the clients in the above mentioned circumstances

JBL shall not be responsible for any loss incurred and the client shall indemnify JBL in this regard.

J. De-registering a client

JBL may, at its absolute discretion, decide to deregister a particular client if found that:
SEBI or any other regulatory body has passed an order against such client, prohibiting or suspending such client from participating in the securities market. Such client has been indicted by a regulatory body or any government enforcement agency in case of market manipulation or insider trading or any other case involving violation of any law, rule, regulation, guideline or circular governing securities market. Such client is suspected of indulging in illegal or criminal activities including fraud or money laundering.

Such clients name appears in the UN list of prohibited entities or in the SEBI debarred list On the death / lunacy or other disability of the Client

Such clients account has been lying dormant for long time or the client is not traceable If the Client being a partnership firm, if any steps have been taken by the Client and / or its partners for dissolution of the partnership

Such client has been irregular in fulfilling obligations towards margin or settlement dues

Such client has been declared insolvent or any legal proceedings to declare him / her as insolvent have been initiated.

Such client has a tainted reputation and any business relationship with such clients is likely to tarnish the reputation of JBL or may act as detriment to JBL's prospects.

J. Treatment of Inactive Trading account

In order to provide guidelines regarding treatment of inactive account and ensure uniformity across all the members, the following guidelines, framed in joint consultation with other Exchanges.

i. Definition of Inactive Trading accounts: In case of trading account, the term inactive account refers to such account wherein no trades have been carried out since last 12 (Twelve) months across all Exchanges

ii. Transaction in Inactive Trading accounts: The inactive accounts identified based on the above criteria shall be flagged as 'Inactive' by the Trading Member in UCC database of all the respective Exchanges. The Members are also required to ensure that any further trading by such client should be allowed only after undertaking sufficient due diligence (including IPV) and obtaining the updated information related to KYC from the concerned Client. Appropriate disciplinary actions may be initiated in case of any trades are executed in any account flagged as 'Inactive'. Members shall be required to undertake the fresh documentation, due diligence and IPV where a client is coming for reactivation after a period of 1 year of being flagged as inactive. However, in case a client has undertaken transaction through the Member, with respect to IPO/Mutual Fund subscription and DP operations (if the Member is a DP) during this period, the same can be considered and the requirement for fresh documentation, due diligence, and IPV may not be required.

Further, in the below mentioned conditions, as stipulated in SEBI circular dated April 24, 2020 bearing reference number SEBI/HO/MIRSD/DOP/CIR/P/2020/73, the requirement for undertaking an IPV shall not be required:-

□* Where the KYC of the investor is completed using the Aadhaar authentication / verification of UIDAI.
* When the KYC form has been submitted online, documents have been provided through Digi locker or any other source which could be verified online.

Notwithstanding anything contained above, in case a client seeks re-activation before a period of 1 year of being flagged as inactive, Member shall, while reactivating the client, ensure that the basic details of such client like Address, Mobile number, Email ID, Bank/DP account are updated in its records as well in the UCC records of the Exchange. In case of any changes, necessary documents shall be collected.

Members shall also ensure that appropriate due diligence of the client is conducted on an ongoing basis in compliance with the provisions of the PMLA guidelines issued from time to time and in accordance with their respective KYC policies.

iii. All trading members are advised to upload correct status of the client code in the UCC database of the Exchanges prior to the execution of the trades.

iv. Return of Clients assets: Members are required to ensure that all client accounts are settled on monthly or quarterly basis (as per the client preferences) in the manner prescribed from time to time.

In case a member is unable to settle the client accounts due to non-availability of client's bank account and demat account details and non-traceability of client, Members are advised to make all efforts to trace the clients to settle their funds and securities lying with them and maintain an audit trail for such efforts made for tracing such clients and settling funds and securities of such clients.

Further in cases where Members are unable to trace such clients in spite of all efforts taken, members are directed to take the following steps:

i. Open one separate Client Bank account and immediately set aside the funds in such account.
ii. Maintain audit trail of UCC wise client funds transferred to/from such bank account.
iii. Submit UCC wise fund information of such account to the Exchange on weekly basis.
iv. In case of receipt of any claims from such clients, members are advised to settle the accounts immediately and ensure that the payment/delivery is made to the respective clients only.

K: <u>Ease of doing Investment by investors- Facility of voluntary freezing/blocking the online access of the trading account to the clients:-</u>

As per the provision of SEBI Circular no. SEBI/HO/MIRSD/POD-1/P/CIR/2024/4 dated January 12, 2024, JBL disclose on their website, the process and mode(s) through which the client can place the request to freeze / block & unfreeze / unblock the trading account along with the timelines that will be followed by JBL for the same.

1. JBL providing internet based trading/ mobile trading/ other online access for trading shall make available to the clients at least two modes of the following communications through which the client may request for voluntary freezing/ blocking the online access of trading account if any suspicious activity is observed in the trading account: -

a) Email from registered e-mail ID
b) SMS from registered mobile number
c) IVR/tele calling
d) Chatbot
e) Trading Member's App / website
f) Any other legally verifiable mechanism

2. Where an e-mail ID and/or telephone number is provided by JBL for this purpose, the said e-mail ID/ telephone number should be dedicated for receipt of communication for voluntary freezing/ blocking of the online access of the clients' trading account. The nomenclature of the dedicated e-mail Id shall be stoptrade@jainam.in.

3. JBL shall take the following actions on the receipt of request through any modes of communications as provided by JBL for freezing/blocking of the online access of thetrading account from the client:

a) Validate that the request is received from the client as per below point no. 4 and issue the acknowledgement as well as freeze/block the online access of the client's trading account and simultaneously cancel all the pending orders of the said client. The timelines for freezing/ blocking of the online access of the clients' trading account is as under: -

Scenario	Timelines for issuing acknowledgement as well as freezing / blocking of the online access of the trading account.
Request received during the trading [1] and within 15 minutes before the start oftrading.	Within 15 minutes [2]
Request received after the trading hours and15 minutes before the start of trading.	Before the start of next trading session

Note:-
[1] Trading hours as follows:
Capital Market Segment: 9.15 a.m. to 3.30 p.m.,
Equity Derivatives Segment: 9.15 a.m. to 3.30 p.m.,
Currency Derivatives Segment: 09.00 a.m. to 05.00 p.m.,
Commodity Derivatives Segment: 09.00 a.m. to 11:30 p.m.

[2] To begin with, the time limit of 15 minutes is being specified for the purpose of issuing acknowledgement as well as freezing/blocking of the online access of the trading account. This time limit shall be contracted after a review in next six months after the date of its applicability to enhance protection of investors from suspicious activities.

b) Post freezing/blocking the client's trading account, send a communication on the registered mobile number and registered e-mail ID of the client, stating that the online access to the trading account has been frozen/blocked and all the pending orders in the client's trading account, if any, have been cancelled along with the process of re-enablement for getting the online access to thetrading account.

c) Details of open positions (if any) should also be communicated to the client along with contract expiry information within one hour from the freezing/blocking of the trading account. This will eliminate the risk of unwanted delivery settlement. This time limit shall be contracted after a review in the next six months after the date of its applicability to enhance protection of investorsfrom suspicious activities.

4. JBL shall have a mechanism in place to validate that the request for freezing/blocking of the online access of the trading account is received from the respective client only. This can be done by:-

a) verifying whether request is received from the registered phone number/e-mail Id of the client; or where request is received from other than registered phone number/e-mail Id of the client, the Trading Member should have a client authentication procedure (2 Factor Authentication) in place or

b) Following any other process as may be prescribed by the Exchange(s) uniformly in consultation with SEBI, from time to time.

2. JBL shall maintain the appropriate records/logs including, but not limited to, request received to freeze/block the online access of trading account, confirmation given for freezing/blocking of the online access of the trading account and cancellation of pending orders, if any, sent to the clients.

3. In case of failure of JBL in freezing/ blocking the online access within the prescribed timelines (15 minutes in case the request is received during the trading hours and within 15 minutes before the start of trading / Before the start of the next trading session in case the request is received after the trading hours and 15 minutes before the start of the trading), JBL shall be responsible for any trades executed from the time of receipt of such request till such time the online access is blocked / frozen.

4. Re-enabling the client for online access of the trading account: - JBL shall re-enable the online access of trading account after carrying out necessary due diligence including validating the client request and unfreezing / unblocking the online access of the trading account.

5. It is clarified that:

a. Freezing/blocking is only for the online access to the client's trading account, and there shall be no restrictions on the Risk Management activities of JBL.

b. The request for freezing/ blocking does not constitute request for marking client Unique Client Code (UCC) as inactive in the Exchange records.

Enhanced Obligations and Responsibilities:

Risk Management Committee:

The Risk Management Committee is Board nominated committee consisting of Directors being part of the Committee.

The implementation of strong and effective risk management and controls within the organization promotes
stability throughout the entire financial system. Specifically, internal risk management controls provide four important functions:

- to protect the firm against market, credit, liquidity, operational, and legal risks.
- to protect the financial industry from systemic risk.
- to protect the firm's customers from large non-market related losses (e.g., firm failure, misappropriation, fraud, etc.).
- to protect the firm and its franchise from suffering adversely from reputational risk.

The importance of effective risk management and controls in protecting against serious and unanticipated loss is perhaps best illustrated where risk management and controls broke down or were not properly implemented. To avoid suck risks and to survive in this competitive environment, the Company itself maintains Risk Management system follow up regular basis at the separate client level activities. To protect the capital & interest of the company for good self, the risk of the daily business is ascertained regularly by the organization.

The risk management committee is Head by Shri Milan Parikh. Responsibility includes overseeing the deployment of the Risk Management framework and procedures. The primary role will be to ensure that the Company achieves its objectives of timely anticipation of risks and opportunities and a cohesive and consistent response through the active involvement of process owners. They will review risks, by timely meetings, comprehensive discussions at respective departments, effective escalation, regular monitoring of risks, implementation of the risk management framework, and the various risks faced by the organization.

Risk Reporting:

The Board of Directors of the Company shall periodically review and evaluate the risk management system of the Company so that the management controls the risks through properly defined procedures.

CXO and Head of Departments or such other authorized persons by Board shall be responsible for implementation of the risk management system as may be applicable to their respective areas of functioning and report to the Board / Audit/ Risk Management Committee, as the case may be.

Every Head of Departments or such other authorized persons by Board shall also give details regarding any apparent risk and prospective opportunities relating to their departments on periodic basis to the Board.

Significant risks include those risks that have a high likelihood or significant impact i.e., having risk exposure or where there is limited ability for mitigation by the Company. These risks are identified and assessed based on the Company's expertise, judgement and knowledge.

Organization follows an automated Risk Management System and compliance processes like margin computation, exposure provided to clients vis-à-vis their collaterals with exchanges/ CCs, periodic submissions and all reporting to the exchanges etc.

Review of Policy:

The Risk Management Policy shall be reviewed on ongoing, periodic basis and at least once half yearly basis and the necessary market changes as and when made by SEBI, Exchange or any other regulators or to incorporate the changes necessitated due to changes in the market condition or to strengthen the internal control or for such other reason as deemed fit by the Management and Compliance Officer to ensure that the same is updated in line with market trends, updated regulations, and practices.

Last Review and Version no :

Financial Year	Version	Date (placed in RMS Committee Meeting)	Approved by	Date (placed in Board Meeting)	Approved by
FY 2025-26	Version no 01/2025-26	May 12, 2025	Approved in RMS Committee Meeting	June 20, 2025 April 28, 2025	Approved in Board Meeting
FY 2024-25	Version no 02/2024-25	Nov 13, 2024	Approved in RMS Committee Meeting	Jan 18, 2025	Approved in Board Meeting
FY 2024-25	Version no 01/2024-25	July 22, 2024	Approved in RMS Committee Meeting	July 31, 2024	Approved in Board Meeting
FY 2023-24	Version no 02/2023-24	Sept 15, 2023	Approved in RMS Committee Meeting	Sept 22, 2023	Approved in Board Meeting
FY 2023-24	Version no 01/2023-24	March 20, 2024	Approved in RMS Committee Meeting	April 24, 2024	Approved in Board Meeting

JAINAM
Prosperity with Security

RISK MANAGEMENT STANDARD OPERATING PROCEDURE

Combine collateral and common limit system in place where client common limits set according to ledger balance and approved security pledged by client. Client is allowed to take exposure in various exchange and across segments according to trading preference opted by client. According to margin utilization in one exchange / segment, balance margin will be allowed for another exchange / segment.

1. Retail Offline clients:

1.1 For Equity Cash Segment, Buy / Sell exposure limit will be 5 times (20 % Margin) or according to VAR Margin % applicable on security whichever is higher of ledger balance and approved stock re-pledged with Clearing Corporation.

1.2 For Derivative Segment (Equity, Currency and Commodity) exposure limit will be 1 time of ledger balance and approved stock re-pledged with Clearing Corporation.

1.3 If exposure is not set as per the above standard, then only selling exposure will be allowed if client has DP Account with Jainam Broking Ltd and POA / DDPI authorization given by client to pledge security and Market Pay-in of security sold by client.

1.4 If client has not opened DP Account with Jainam Broking Limited or having Non-POA DP Account with Jainam Broking Limited, Buying and Selling will be allowed if client maintain 50 % Margin in form of clear ledger balance.

1.5 If client has DP Account with POA/DDPI authorization, Buy exposure limit will be allowed 70% of delivery selling value subject to EPI is possible in live market.

2. Retail Online Clients:

2.1 Margin & Exposures

For Equity Cash Segment, Buy / Sell Exposures will be given against the following

- Clear ledger balance
- Pledge-Repledge after hair cut value approved security on which exposure allowed by Exchange / Clearing Corporation.
- Online Fund transferred by the client

For Derivative Segment, Exposures will be given against the following

- Clear ledger balance
- Pledge-Repledged approved security after hair cut value on which exposure allowed by Exchange / Clearing Corporation.
- Buying of Option allowed to extent of premium allowed against amount of premium received against options sold
- Online Fund transferred by the client

Following Debits will be deducted from the margin available:

- Margin utilized
- Booked loss
- Mark-to-market loss

JAINAM BROKING LIMITED

3. MTF Client:

3.1 MTF Client can buy security according to availability of Margin required for Cash segment (20% or Applicable VAR margin whichever is higher). However, funding is allowed if client maintain applicable margin for MTF (VAR+3 ELM on FNO segment MTF Approved security and VAR+5 ELM on Non-FNO segment MTF Approved security)

For MTF Segment, Exposures will be given against the following

- Clear ledger balance
- Pledge-Repledged approved security after hair cut value on which exposure allowed by Exchange / Clearing Corporation.

* As JBL is following combine collateral management, pledged security will be considered for MTF margin. No limit will be allowed on security pledged against funding.

4. NRI – NRE Clients:

4.1 NRI-NRE client buy exposure will be allowed against client NRE Saving / PIS balance only.

4.2 NRI-NRE client selling exposure will be allowed for security lying in DP Account and POA/DDPI authorization is given by client for payin of security.

5. Custodian Clients (Normal, NRO, FPI, Institutional):

5.1 Custodian client buy / sell exposure will be allowed against client balance maintained with custodian and balance confirmation given by custodian for client.

5.2 Custodian client selling exposure will be allowed for security lying in DP Account and POA/DDPI authorization is given by client for pay-in of security.

5.3 Custodian client Derivative exposure will be allowed to extent of 90 % of available balance or security pledged by client with custodian.

6. All margin (Intraday) positions except Derivative positions will be squared off after 3.15 PM or 15 minutes prior to the closure of the trading, whichever is later.

7. Any loss or debit arising out of the square off or non-occurrence of square off has to be borne by the client.

8. Other than the cases mentioned in point no. 7, RMS shall square off the position of the client whenever the M2M loss of a client reaches 80% of the margin available – called M2M Square off. RMS has discretion to square off position on case-to-case basis on identification of stock prospectively hitting circuit limit.

M2M Square off will work on the following positions of a client:

- All margin positions in cash segment
- All open Futures positions
- All open short/ sell positions in Options

Available margin for M2M Square off will be calculated as follows:
Ledger Balance + Pledged Security + Intra-day Funds Transferred + Value of unpledged shares sold as delivery + Premium received – Margin blocked for delivery positions – Booked losses – Premium paid –

Pending withdrawal requests.

9. Haircut: VAR margin Haircut as prescribed by Exchange on approved security and additional 20 % and above haircut and relaxation rights of the additional haircut charged lies with RMS department.

10. Cheque Bounce clients - 3 times in a Quarter (Current FY / Insufficient Funds)
Allowed exposure against 100 % advance payment only.

11. Force Sale:
11.1 Force sale is done on exceptional cases with the approval of RMS Head, Sales Head and Compliance Head.

11.2 T + 5 Process:
T + 5 – Action by RMS on T+6 (6th day) – Force Sale \ Forced Selling of stocks to clear debit valued at Rs.100 or above will be initiated by the RMS team on T+ 6.

12.1 Illiquid Trading - For trading in GSM , ASM, Z, Illiquid group and X series stock requires 100 % margin.

12.2 Force sale will be done irrespective of scrip and whether the client is making profit or loss on the transaction.

12.3 Forced sale deadlines may be advanced depending on client/ market/ funds position.

12.4 Any shortfall in margin has to be settled as specified by RMS.

12.5 RMS will close any open position to clear the Margin / MTM shortfall and such actions may be taken even on T day if the position turns adverse or has the potential of turning adverse.

Different types of margin

There are different types of margin has to maintain which is mentioned below

1. **Initial Margin:** Initial margin is the money deposited by traders to ensure performance of trades executed. Initial margin is payable on all open positions at any point of time, and is payable upfront by the client in accordance with the margin computation mechanism and/or system as may be adopted by the exchange from time to time. Initial margin includes span margin and such other additional margins that may be specified by the exchange from time to time.

2. **Exposure Margin**: A trader is entitled to withdraw any balance in the margin account in excess of the initial margin. To ensure that the balance in the margin account never becomes negative, a exposure margin, which is somewhat lower than the initial margin, is set. If the balance in the margin account falls below the exposure margin, the trader receives a margin call and is requested to deposit extra funds to bring it to the initial margin level within a very short period of time. The extra funds deposited are known as a variation margin.

3. **Additional Margin**: In case of sudden higher than expected volatility, the exchange calls for an additional margin, which is a pre-emptive move to prevent breakdown. This is imposed when the exchange fears that the markets have become too volatile and many result in some payments crisis etc.

4. **Mark-to-Market Margin (MTM):** At the end of each trading day, the margin account is adjusted to reflect the trader's gain or loss. All future contracts are settled daily reducing the credit exposure to one day's movement. Based on the settlement price, the value of all positions is marked-to-market each day after the official close. I.e. the accounts are either debited or credited based on how well the positions fared in that day's trading session. If the account falls below the margin level the trader needs to replenish the account by giving additional funds. On the other hand, if the position generates a gain, the funds can be withdrawn (those fund above the required initial margin) or can be used to fund additional trades.

5. **Pre-expiry margin:** This margin is charged as additional margin for most commodities expiring during the current/near month contract. It is charged on a cumulative basis from typically 3 to 5 days prior to the expiry date (including the expiry date). This is done to ensure that only interested parties remain in the market and speculators roll over their positions to subsequent months. (Positions held during this period will attract additional margin)

6. **Margin for Calendar Spread positions:** Calendar spread is defined as the purchase of one delivery month of a given futures contract and simultaneous sale of another delivery month of the same commodity by a client. For calendar spread positions, margins are imposed as one half of the initial margin (inclusive of the exposure margin). No benefit of calendar spread is given in the case of additional and special margins.

Review of SOP:

The Risk Management SOP forms part of RMS Policy shall be reviewed on ongoing, periodic basis and the necessary market changes as and when made by SEBI, Exchange or any other regulators or to incorporate the changes necessitated due to changes in the market condition or to strengthen the internal control or for such other reason as deemed fit by the Management and Compliance Officer to ensure that the same is updated in line with market trends, updated regulations, and practices.

Risk Management Policy
The Jainam Broking Limited

Prepared By : IT Team

Disclaimer: ***This document is intended for the internal use of The Jainam Broking Limited .***

DOCUMENT VERSION CONTROL

DATE	VERSION	Revision Description	PREPARED BY	REVIEWED BY	APPROVED BY
21st June, 2023	1.0	First Release	Ms. Nidhi Parmar	Mr. Mitesh Boghani & Mr. Raviranjan Sharma	Board of Management
15th September, 2023	2.0	Second Release	Ms. Nidhi Parmar	Mr. Mitesh Boghani & Mr. Raviranjan Sharma	Board of Management
20th March, 2024	3.0	Third Release	Ms. Krusha Kinkhabwala	Mr. Mitesh Boghani	Board of Management
19th October,2024	4.0	Forth Release	Ms. Krusha Kinkhabwala	Mr. Mitesh Boghani	Board of Management
28th April, 2025	5.0	Fifth Release	Ms. Krusha Kinkhabwala	Mr. Mitesh Boghani	Board of Management

Contents

1. **Introduction** 4
2. **Purpose** 4
3. **Scope** 5
4. **Governance and Responsibilities:** 5
5. **Risk Management Framework:** 6

1. Introduction :

Jainam Broking Limited, the primary objective of the Risk Management Policy is to implement a systematic and forward-looking approach to managing potential threats that could adversely affect our information systems, digital infrastructure, business operations, client services, and reputation.
We are committed to preserving the **confidentiality, integrity, and availability (CIA)** of our critical data and technology assets. Through this policy, we aim to establish a resilient risk management framework that allows the organization to:

- Proactively **identify emerging and existing risks** across all operational domains.
- **Assess the impact** and likelihood of these risks in a quantifiable manner.
- **Mitigate vulnerabilities** through preventive and detective controls.
- **Continuously monitor the risk environment**, including internal and external risk factors.

This objective is aligned with our broader business goals of ensuring regulatory compliance, safeguarding stakeholder interests, minimizing potential operational disruptions, and maintaining a strong security posture across the enterprise.

2. Purpose :

The purpose of this policy is to provide a standardized, enterprise-wide framework for **identifying, analyzing, treating, monitoring, and reporting risks** related to information technology and digital operations.
By implementing this policy, **Jainam Broking Limited** intends to:

- **Establish a structured methodology** for risk assessment that is repeatable, consistent, and transparent across the organization.
- **Ensure that all critical information assets and business systems** are clearly identified, classified based on their criticality, and periodically evaluated for associated risks.
- **Embed risk management practices** within our corporate governance processes, ensuring that risk considerations form part of strategic decision-making and operational planning.
- **Foster accountability and risk ownership** by empowering departmental heads, business unit managers, and asset owners to participate in the risk lifecycle actively.
- **Enable continuous improvement** by using feedback from internal audits, incident reports, regulatory inspections, and industry benchmarks to refine the risk management approach.
- Support compliance with internal controls and external obligations, while building organizational resilience against cyber threats, system failures, and third-party risks.

This policy serves as a foundation for risk-based thinking across all levels of the organization and supports our commitment to secure and responsible operations.

3. Scope

This Risk Management Policy is applicable across the entire organizational ecosystem of **Jainam Broking Limited**, including all processes, technologies, personnel, and third-party interactions. Specifically, it covers:

- **All business departments, functions, and operational units**, regardless of their size or risk exposure, ensuring consistent application of risk management principles.
- **All employees**, whether full-time, part-time, temporary, or contractual, who have access to the organization's systems, data, or facilities, and are responsible for adhering to defined risk controls.
- **All third-party entities** such as vendors, consultants, service providers, and outsourcing partners who access, process, or store company information or connect to the company's technology environment.
- **All technology infrastructure and platforms**, including:
    - On-premises hardware (servers, networking devices, storage systems),
    - Enterprise software applications and databases,
    - Network and communication channels,
    - Cloud services and hybrid deployments,
    - Internet-facing applications and internal portals.

4. Governance and Responsibilities:

➢ Board and Senior Management

- Provide direction and oversight for enterprise risk management.
- Approve the Risk Management Policy and review risk reports and escalations.

➢ Risk Management Committee / IT Steering Committee

- Monitor the overall risk profile of the organization.
- Review and approve major risk assessments, mitigation actions, and technology changes.
- Ensure effective functioning of risk management activities.

➢ Chief Information Security Officer (CISO)

- Develops and maintains the risk management framework.
- Coordinates risk assessments and ensures documentation is maintained.
- Advises management on risk exposure and mitigation strategies.

➢ Information Asset Owners

- Identify and classify their respective information assets.
- Participate in risk identification and ensure control implementation.
- Conduct timely reviews and updates for their area of responsibility.

➢ Compliance Teams

- Verify the effectiveness of risk mitigation and control implementations.
- Provide assurance on compliance with risk management practices.

5. Risk Management Framework:

➢ Asset Identification and Classification :

- **All assets must be identified by their respective Department Heads**, and an up-to-date asset inventory must be maintained. The assets can be classified into the following categories:
- **Information Assets**: These include electronic and paper-based records, such as data files, e-records, system documentation, user manuals, training materials, operational procedures for IT management, software licenses, source codes, business continuity plans, contracts, guidelines, HR records, etc. Information assets also encompass business documents such as contracts, company documentation, business results, purchase documents, invoices, license agreements, and escrow agreements.
- **Software Assets**: These include business applications, operating systems, databases, knowledge management applications, development tools, utilities, and other software components used by the organization.
- **Physical Assets**: These include servers, networking equipment, security devices, backup media, printers, biometric devices, server racks, desktops, laptops, and other hardware assets.
- **Services and Processes**: These include all outsourced services, such as hosted service providers, outsourced data center management, outsourced application support, and other organization-related outsourced activities. Services also encompass telecommunications, power, general utilities (e.g., air conditioning, alarm systems, fire prevention services, etc.). The most critical service, like a hosted managed service provider, should be assigned the highest asset value.
- **People Assets**: These refer to the organization's employees, customers, visitors, and any other personnel directly associated with the organization.
- **Designation of Asset Owner**: Every asset must have a designated owner. The asset owner's primary responsibility is to ensure the confidentiality, integrity, and availability of the asset. The asset owner will also define the access rights for the asset.
- **Annual Review and Risk Assessment**: All assets, including hardware, software, physical assets, and media, must undergo a risk assessment review by the designated asset owner at least once per year. It is essential to ensure that any unnecessary functionality (such as scripts, drivers, features, subsystems, and file systems) that is not required to fulfill job responsibilities is removed or disabled from hardware before being provided to end users.
- **Asset Classification**: All information system assets of the organization should be classified by the asset owner in collaboration with the IT Manager, based on their business value and impact on business operations.

- **Asset Value Assignment**: Asset value should be determined based on three key parameters: **Confidentiality**, **Integrity**, and **Availability**. Each of these parameters should be evaluated as **High**, **Medium**, or **Low**. The highest value among the three parameters will determine the overall asset value. For example, if Confidentiality = High, Integrity = Medium, and Availability = Medium, the asset value will be classified as **High** due to the highest confidentiality level. Critical outsourced services should always be assigned the highest asset value.

- The level of Confidentiality, Integrity and Availability should be valued in terms of business value and impact of Information System assets for continuance of business operations of the Organisation as follows,

Classification	Description
High	Assets classified as High are mission-critical to the organization. Any unavailability, unauthorized disclosure, alteration, or damage to these assets may result in a significant disruption to core business functions, severe financial loss, legal liabilities, or reputational damage. The business will not be able to continue normal operations without the timely restoration of these assets.
Medium	Assets classified as Medium are important to business continuity. While the organization may still function in their absence or if compromised, there would be a notable reduction in operational efficiency, service quality, or compliance. Such disruptions can have a moderate financial or reputational impact.
Low	Assets classified as Low have limited impact on the organization if disrupted. Their unavailability, alteration, or disclosure would only cause minimal effect on operational performance, with business activities continuing largely unaffected.

- Information shall also be classified based on its sensitivity to business operations. Asset owners should classify the information in consultation with the IT Manager. The Organisation classifies information as one of the following,

Classification	Description
Restricted	This category is applied to the most sensitive business information. Unauthorized access, modification, or disclosure of such information could cause severe financial, operational, regulatory, or reputational damage. Access to restricted information must be strictly controlled, monitored, and limited to only those with explicit authorization.

Confidential	This classification includes sensitive information that must be limited to personnel with a legitimate business need-to-know. All customer, client, and financial data processed or accessed by the organization is considered *Confidential* by default. Confidential information must be protected with appropriate access controls and encryption where applicable.
Internal Use Only	This classification applies to non-public business information intended for use only within Jainam Broking Limited. It includes documents such as internal memos, operational manuals, process charts, policy circulars, and emails. This information may be shared freely among employees but must not be disclosed outside the organization. All information not explicitly classified as *Restricted*, *Confidential*, or *Public* is considered *Internal Use Only* by default. Explicit labeling is not mandatory for this category.
Public	This classification is reserved for information that has been formally approved by senior management for release into the public domain. This includes press releases, public notices, marketing materials, and regulatory disclosures. Public information must be clearly labeled and should not contain any sensitive or confidential content. Mislabeling or accidental disclosure of internal data as public is strictly prohibited.

- Asset owner shall semi-annually review the classification given to the information or valuation of an asset based on changes in business environment.

➢ **Risk Assessment:**

- Risk Assessment shall be performed by designated owners, in consultation with the IT Manager, the following three steps as described below:
- The asset owners shall identify various risks based on the identified threats and vulnerabilities and the impacts that losses of confidentiality, integrity and availability may have on the assets.
- Threats shall be categorized as “High”, “Medium”, “Low” based on their likelihood of occurrence. The following table defines the threat levels:

Threat Level	Description
Low	The probability of this threat materializing is minimal. There is no significant historical data, incidents, or motivation that suggest it is

	likely to occur.
Medium	There is a reasonable possibility of occurrence. Similar incidents may have occurred in the past, or statistical/trend-based evidence exists. There may be potential motives for exploitation.
High	The threat is highly probable or imminent. Past incidents, current intelligence, or specific motives indicate a strong likelihood of exploitation.

- Vulnerabilities shall be rated as “High”, “Medium”, “Low” based on ease of exploit and level of protection currently present on the asset. The following table defines the vulnerability levels:

Level	Description
Low	The vulnerability is considered **unlikely to be exploited** due to its high complexity or low attractiveness to attackers. In addition, **robust protection mechanisms** are already in place, significantly reducing the associated risk.
Medium	The vulnerability is **potentially exploitable**, although **some controls or mitigations are in place** to prevent or limit damage. Exploitation may require specific conditions or moderate effort.
High	The vulnerability is **highly likely to be exploited** or is easily exploitable using publicly known techniques. There are **few or no existing controls** to prevent or detect exploitation, representing a critical security risk.

- The risk assessment process of the Organisation follows a zero-control approach for the first time for new systems/applications. In this approach, all the threats and vulnerabilities a particular asset may be exposed to are identified and appropriate controls are selected to mitigate the vulnerabilities and reduce the risk to acceptable levels.
- The risk assessment process should follow an ongoing approach for existing systems/applications. This approach takes into account all the existing controls and their effectiveness in terms of residual risks and assessment for new vulnerabilities and controls required.
- The ranking of risks is based on a qualitative and quantitative method. Risk ranking is arrived based on the following formula:

Risk Ranking = Asset value × Threat Value × Vulnerability Value

- Values for Assets, Threat and Vulnerability are scaled as 3 for High, 2 for Medium and 1 for Low.
- Threat includes the likelihood of occurrence of an incident.
- The asset values and the threat and vulnerability levels are matched in a matrix as shown below. All the identified risks for the asset should be ranked based on the risk ranking matrix given below,

	Threat Level	Low			Medium			High		
	Vulnerability Level	L	M	H	L	M	H	L	M	H
Asset Value	Low	1	2	3	2	4	6	3	6	9
	Medium	2	4	6	4	8	12	6	12	18
	High	3	6	9	6	12	18	9	18	27

➢ **Risk Acceptance Level :**

- Based on the above matrix, the risks can be ranked on a scale of 1 to 27. For example, if the asset has the value of “medium”, the threat is “high” and the vulnerability is “low”, the measure of risk in this case would be “6”. The Organisation has decided a risk value of 0 – 9 as acceptable and any risk having a value between 10 – 27 needs to be mitigated to bring down the risk level.
- The asset owner, in consultation with the IT MANAGER, should conduct a risk evaluation to determine whether risks are acceptable or require treatment. The risk evaluation should be conducted in terms of the business impact and probability of occurrence in the context of existing controls. Asset owners should document the same in a Risk Assessment report.
- Risks that are above the acceptable level qualify for the risk treatment. Controls should be determined by the asset owner and approved by the IT MANAGER. The selection of controls should take into account the business, legal, statutory and regulatory requirements.

➢ Residual Risk :

- The asset owner should measure the residual risk after implementing the controls. Residual Risk is the risk that remains even after risk treatment. This may be due to the cost of implementation is higher than the potential loss.
- If the residual risk level is above Risk Acceptance level (9) after risk treatment, the decision to accept the risk should be taken by the application owner with approval of the Head of IT.
- Whenever control cannot be identified or the cost of implementation outweighs the potential loss, a decision can be taken to accept the risk. In such a scenario, the decisions should be documented and approved by the head of IT.

➢ 5.5 Continuous Monitoring and Review :

- The asset owner should undertake reviews at regular intervals to verify the adequacy of existing controls, residual risk and acceptable level of risks. The asset owner should monitor the implemented controls, measure the control effectiveness.

- The asset owner should identify any new risks arising due to significant changes made to the assets or business processes.

➢ 5.6 Risk Assessment of outsourced processes :

- Critical business processes which have been outsourced by the Organisation shall be assessed for their risk to the Organisation. Critical processes are the ones which an organization is highly dependent on for performing important business activities and shall cause financial and reputational impact on the organization if performed erroneously.
- Any change in the scope of the business process that is outsourced to shall be reviewed by the organization's IT Steering committee.
- Appointment of new service provider to carry out the critical business process shall be done only after a signing off the valid legal agreement between two parties. Refer to IT Outsourcing policy for more details on appointing a new service provider.
- The organization's IT Steering committee shall ensure that outsourced service providers shall have a robust business continuity framework implemented and tested periodically. The periodicity of the vendor's DR test must coincide with the organization's DR test frequency. Refer to the BCP policy for further details on DR testing.

Thank You