FINQUEST FINANCIAL SOLUTIONS PRIVATE LIMITED

RISK MANAGEMENT POLICY

Finquest Financial Solutions Private Limited
CIN: U74140MH2004PTC146715
Registered Address: 602, Boston House,
6th Floor, Suren Road, Andheri (E),
Mumbai-400093
Email Id: hpatel@finquestonline.com

Version control:

Particulars	Date	Version No.
Adopted in the Board Meeting held on	02/02/2017	V. 1
Revision in the Board Meeting held on	19/04/2022	V. 2
Revision in the Board Meeting held on	02/03/2023	V. 3
Revision in the Board Meeting held on	22/07/2024	V.4

RISK MANAGEMENT POLICY

Introduction

Non-Banking Financial Companies ("NBFCs") form an integral part of the Indian financial system. Over the past few years, NBFCs have played a prominent role in the Indian financial system. They provide financial inclusion to the underserved section of the society that does not have easy access to credit. NBFCs have revolutionized the Indian lending system and have efficiently leveraged digitization to drive efficiency and provide customers with a quick and convenient financing experience. The plethora of services include vehicle financing, MSME financing, home financing, microfinance and other retail segments. NBFCs are therefore required to ensure that a proper policy framework on Risk Management Systems with the approval of the Board is formulated and put in place.

Finquest Financial Solutions Private Limited ("FFSPL/the Company") is registered with the Reserve Bank of India (RBI) is classified as a Base Layer NBFC ("NBFC-BL") under the Scale Based Regulatory Framework of RBI.

In accordance with the RBI Master Direction - Non-Banking Financial Company – Non-Systemically Important Non-Deposit taking Company (Reserve Bank) Directions, 2016 dated September 1, 2016 (as amended from time to time), {the Master Directions} the Board of Directors of the Company has adopted this Risk Management Policy ("Policy").

Risk Management is a key aspect of the "Corporate Governance Principles and Code of Ethics" which aims to improvise the governance practices across the activities if the Company. The Management of the Company as a NBFC-BL have to base their business decisions on a dynamic and integrated risk management system and process, driven by corporate strategy.

NBFCs per se are exposed / more vulnerable to several major risks in the course of their NBFC business activity including Credit Risk, Market Risk, Liquidity Risk, Operational Risk, Compliance Risk and Reputation Risk, Cyber- Security Risk. It is therefore important for the NBFCs to introduce effective Risk Management Policy which addresses, minimise and mitigate the various business risks stated earlier (the Risk Mitigation Actions).

Risk Management Policy and processes is expected to enable the Company to proactively mitigate and manage uncertainty and changes in the internal and external environment, to limit negative impacts and capitalize on opportunities.

Objective & Purpose of Risk Management Policy

Risk Management is a business facilitator by making more informed decision with balanced risk-reward paradigm. The Company shall follow a disciplined Risk Management Process and shall take business decisions, ensuring growth and balancing approach on risk reward matrix.

The main objective of the Risk Management Policy is to ensure sustainable business growth with stability and to promote a pro-active approach in reporting, evaluating and resolving and mitigating risks associated with the business of the Company. In order to achieve the key objectives, the Risk Management Policy establishes a structured and disciplined approach to Risk Management, in order to guide on decisions on risk identification, mitigation and related issues.

Following are the specific objectives of the Risk Management Policy of the Company:

1) To ensure that all the current and future material risks to which the Company is exposed / more vulnerable to are identified, assessed, quantified, appropriately mitigated, minimized and managed i.e. to ensure adequate systems for Risk Management.
2) To establish a framework for the Risk Management process of the Company and to ensure its implementation for risk mitigation.
3) To enable compliance with appropriate regulations, wherever applicable, through the adoption of best compliance and governance practices.
4) To assure business growth with financial stability.

Risk Management Framework

In principle, risk always results as a consequence of activities or as a consequence of non-activities (i.e. Act or Omission. Risk Management and Risk Monitoring are important in recognizing and controlling risks.

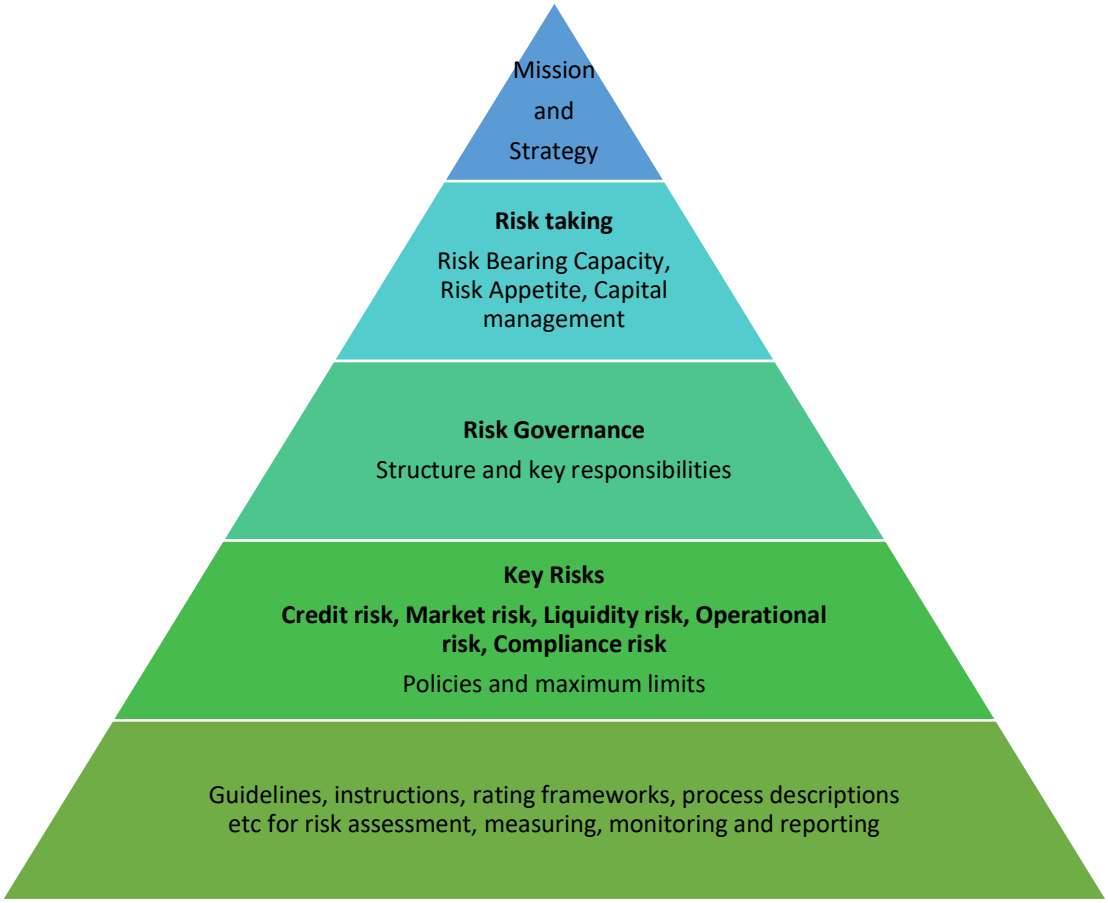
Risk Mitigation is an exercise aiming to reduce the loss or injury arising out of various risk exposures to which the Company more vulnerable.

The Company shall adopt a systematic approach to mitigate various risks associated with accomplishment of objectives, operations, revenues and regulations. The Company believes that this would result in mitigating risks proactively and would help the Company to achieve stated /desired objectives.

The Company shall consider activities at all levels of the organization and its Risk Management with focus on three key elements, viz.,

(1) **Risk Identification and Assessment:** Study of threats and vulnerability and resultant exposure to various risks.
(2) **Risk Management and Monitoring:** The probability of risk assumption is estimated with available data and information.
(3) **Risk Mitigation and minimisation:** Measures adopted to mitigate and minimise risk to which the Company is exposed to.

The **Risk Management Framework** of the Company has been stated hereunder.



Mission and Strategy

The Company is a RBI classified as a NBFC-BL under the Scale Based Regulatory Framework of RBI.

The objective of the Company is as follows:

"To achieve the financial goals of the Company by enhancing our understanding of potential investments and allocate our finances to maximize risk adjusted return and secure our financial future."

We are dedicated to steering our clients towards the right growth-oriented investment decisions, and to provide strategic support at every step to ensure that our clients achieve their desired growth and liquidity objectives.

The Company is deploying its funds across the capital structure in borrowers having an emphasis on long term returns. The Company has required experience, resources and the flexibility to provide the financial solutions quickly, and the strategic and operational expertise to help and support its investments.

Risk Taking

The Company shall set their risk appetite and guidelines for each of the following areas:

Area	Risk Appetite and Guideline
Capital adequacy and balance sheet measures	to comply with capital requirement regulations as applicable to the Company as Base Layer - NBFC and to maintain a strong financial base in continuing to conduct businesses under various economic conditions.
Liquidity risk	to maintain sufficient liquidity to survive a severe liquidity situation and to comply with the applicable regulatory requirements.
Market risk and credit risk	to manage market risk and credit risk within the businesses of the Company.
Operational risk	to understand and mitigate the impact and likelihood of operational risk events assumed in the course of conducting business.
Compliance risk	to promote proper understanding and compliance culture with the letter and spirit of all applicable laws, rules and regulations and avoid non-compliance and misconduct.

Risk Governance

Constitution of Risk Management Committee

- In accordance with the provisions of the Master Directions, the Company shall constitute the Risk Management Committee.
- The Risk Management Committee shall ensure that the risks associated with the business/functioning of the Company are identified, controlled and mitigated and shall also lay down procedures regarding managing and mitigating the risks through integrated risk management systems, strategies and mechanisms. The Risk Management Committee shall be responsible for evaluating the overall risks faced by the Company including liquidity risk and will report to the Board.

Chairman	The Chairman of the Committee shall be one of the Committee members to be appointed by the members
Composition	The Risk Management Committee shall be decided by the Board of Directors of the Company from time to time. The MD & CEO of the Company, as well as, heads of various risk verticals shall be members of the Committee.
Meetings	The Risk Management Committee will meet periodically at least once in a quarter to review the risk management policies and practices of the Company.
Quorum	Two members
Terms of Reference	As per the Board approved Risk Management Framework

Role of the Board of Directors of the Company

To ensure that risk is managed appropriately, the Board of Directors of the Company (the Board) shall undertake following:

- The Board shall be responsible for framing, implementing and monitoring the risk management plan for the company.
- The Board shall define the roles and responsibilities of the Risk Management Committee and may delegate monitoring and reviewing of the risk management plan to the Committee and such other functions as it may deem fit.
- Ensure that the appropriate systems for risk management are in place.
- The Committee shall help in bringing an independent judgment to bear on the Board's deliberations on issues of risk management and satisfy themselves that the Risk Management System of the Company is robust and defensible;
- Participate in major decisions affecting the organization's risk profile;
- Have an awareness of and continually monitor the management of strategic risks;
- Be satisfied that processes and controls are in place for managing less significant risks;
- Be satisfied that an appropriate accountability framework is working whereby any delegation of risk is documented and performance can be monitored accordingly;
- Ensure risk management is integrated into board reporting and annual reporting mechanisms;
- Convene any board-committees that are deemed necessary to ensure risk is adequately managed and resolved where possible.

Key Risks

The various types of risk associated with the business of the Company and its risk mitigation mechanisms are stated hereunder:

- **Credit Risk**
  - A risk of loss due to failure of a borrower to meet the contractual obligation of repaying debt as per the agreed terms, is commonly known as risk of default.
  - Credit risk encompasses both the loss of income resulting from inability to collect anticipated interest earnings as well as the loss of principal resulting from loan defaults.
  - The Company has put in place statistical analysis based on internal assumptions for conducting for credit risk.

✓ **Risk mitigation:**

(a) Credit bureau check:

A credit check is done for every customer through an automated system-to-system integration with the credit bureau. As part of this check, the various parameters as specified in the loan policy are looked at to verify a customer's credit worthiness and also ensure that they are not overburdened. These will be dynamic and reviewed periodically based on RBI Regulations, directives and internal norms.

(b) Customer verification

The loan application is processed only after verification of customer's address and documents provided. Every Customer is met by the company official at his/ her residence before loan is approved to confirm the correctness of details furnished.

- **Operational Risk**
  - Operational risk is the risk of possible losses, resulting from inadequate or failed internal processes, people and systems or from external events.
  - The risk can emanate from procedural lapses arising due to higher volumes of transactions; lapses in compliance with established norms; regulatory as well as internal guidelines; misplaced/ lost documents, collusion and fraud; breakdown or non-availability of core business applications.
  - Skill gap and sudden attrition of key personnel in the Company, is also an operational risk, which needs to be countered and addressed by the application of appropriate HR strategies.

✓ **Risk mitigation**:

(a) Process compliance

(i) Ensure that the designed processes are being followed including interaction with the customers during various stages of the relationship lifecycle.

(ii) Ensure all activities are carried out as per norms/ procedures as mentioned in the operational manual.

(iii) Identify any process lapses/ deviations and provide guidance to employees to ensure compliance.

(iv) Training of employees is conducted so as to avoid process violations and ensure strict compliance.

(b) Document storage and retrieval

(i) The Company recognizes the need for proper storage of documents as also their retrieval for audit and statutory requirements.

(ii) Physical storage: The Company shall maintain an established record of all the physical loan documents and shall store them in a specialized secure facility.

(iii) Scanned copies: The Company shall store scanned copies of the loan documents for easy retrieval especially for audit purposes where physical documents are not required.

(iv) The Company maintains software facility to process with system generated records, documents etc.

(c) Non-compliance reporting

(i) The Company encourages all its employees to report any non-compliance of stated processes or policies without fear.

(ii) All issues reported shall be categorized for nature and severity as financial or nonfinancial; major or minor; procedural lapse or gross violation; and breach in process or disciplinary issue.

(d) Internal audits

(i) The key objective of internal audit department is to cross check the functions and various internal controls existing in the Company, the standards viz. RBI directions, credit policies, KYC aspects etc.

(ii) Deviations will be reported for correction in a timely manner. All significant audit observations of internal audits and follow-up actions are presented to the management.

(e) Reporting structure

(i) It shall be ensured that not more than reasonable no. of borrowers are handled by one staff.

(ii) The Company shall have organisation structure including Departmental head, accounts assistant and assistant manager to monitor financial and non-financial parameters of the Company

- **Liquidity risk**

- Liquidity risk is the possibility of negative effects on the interests of stakeholders resulting from the inability to meet current cash obligations in a timely and cost-efficient manner.
- Liquidity risk arises largely due to maturity mismatch associated with assets and liabilities of the company. Liquidity risk stems from the inability of the company to fund increase in assets, manage unplanned changes in funding sources and meet financial commitments when required.
- Due to the high reliance on external sources of funds, the Company is exposed / more vulnerable to various funding and liquidity risks.
- Concentration of a single source of funds exposes the Company to an inability to raise funds in a planned and timely manner and resort to high cost emergency sources of funds. Further,

concentration of funding sources can also result in a skewed maturity profile of liabilities and resultant asset-liability mismatch.

- A high degree of leverage can severely impact the liquidity profile of the Company and lead to default in meeting its liabilities.
- The Company shall also adhere to the Asset Liability Management Policy of the Company when managing Liquidity Risk.

✓ **Risk mitigation**

(a) Short term liquidity forecasts to identify gaps and thereby take immediate corrective actions to bridge the same.

(b) The exposure profile to the lenders is regularly updated to ensure that skewness does not creep in in respect of the sources of external funds.

(c) With the major borrowings of the Company in the form of long tenor NCDs, the Company adequately plans its business to meet its repayment obligations in the event of adverse impact on business.

(d) The Company is exposed / more vulnerable to perception risk because of inherent industry characteristics. At the risk of negative carry on its funds, it is prudent to maintain some amount of excess liquidity. This enables Company to meet its repayment obligations as well give time to take necessary corrective actions to ensure an adequate funding pipeline.

(e) The Company targets adequate leverage and healthy levels of capital adequacy to safeguard itself against the impact of adverse market conditions. It also affords reasonable time to tie-up timely equity infusion.

(f) Daily cash collection and centralized (Head Office) fund management and loan disbursement through bank channels are implemented by the Company. The Company also maintains daily minimum reserve.

➢ **Portfolio concentration Risk**

- This is the risk to Company due to a very high credit exposure to a particular business segment, industry, geography, location, etc. though in the context of micro finance, it pertains predominantly to geographical concentration.

✓ **Risk mitigation**

(a) The Company intends to maintain a diversified exposure in lending to customers across various states to mitigate the risks that could arise due to political or other factors within a particular state.

(b) With this in mind, the Company has steadily diversified its presence to 02 (two) States and is planning to extend its business portfolio to other States as well.

(c) The Company follows district wise allocation of loan portfolio without any religious or community barriers.

(d) The Board of Directors has also duly placed Asset Liability Management Policy which provides detailed measures portfolio concentration risk.

➢ **Compliance Risk**

• The Company is present in an industry where the Company has to ensure compliance with regulatory and statutory requirements. Non-compliance can result in stringent actions and penalties from the regulator and/ or statutory authorities and which also poses a risk to the Company reputation.

• These risks can take the form of non-compliance with RBI regulations, non-compliance with statutory regulations, Income Tax Act, Companies Act, non-compliance with covenants laid down by lenders etc.

✓ **Risk mitigation**

The Company regularly monitors and reviews shortfalls in its compliance system and implements corrective measures to address any variations. The compliance department plays a critical role in this process by:

- Conducting periodic audits and assessments to identify potential compliance gaps.
- Ensuring that regulatory requirements and internal policies are consistently met.
- Providing guidance and training to personnel to enhance compliance awareness.
- Reporting compliance risks and recommending mitigation strategies to senior management and the Board.
- Collaborating with other departments to implement corrective actions and improve control mechanisms.

➢ **Reputation Risk**

• It is the risk to earnings and capital arising from adverse perception of the image of the Company, on the part of customers, counterparties, shareholders, investors and regulators.

• It refers to the potential adverse effects, which can arise from the Company's reputation getting tarnished due to factors such as unethical practices, political activism, regulatory actions, customer dissatisfaction and complaints leading to negative publicity.

• Presence in a regulated and socially sensitive industry can result in significant impact on Company's reputation and brand equity as perceived by multiple entities like the RBI, Central/ State/ Local authorities, banking industry and customers.

✓ **Risk mitigation**

(a) Strict adherence to Fair Practices Code: All employees are trained and instructed to follow fair practices in all their dealings.

(b) Grievance redressal mechanism: The Company has a defined grievance redressal mechanism in place and the same is communicated to all customers.

(c) Customers connect: The Company has established a tele-calling facility to pro-actively reach out to customers to ensure service quality and adherence to Company policies/ processes by the field employees.

(d) Delinquency management: The Company does not resort to any coercive recovery practices and ensures delinquency management including restructuring of loans where necessary.

- **Interest Rate Risk**

• Interest rate risk is the risk of financial loss from changes in regulatory changes and market interest rates.

• The greatest interest rate risk occurs when the cost of funds goes up faster than the Company can or is willing to adjust its lending rates.

- ✓ **Risk mitigation**

  (a) Maintain a financial model that reflects the investment and loan portfolio so as to test the Company's sensitivity to an increase or decrease in interest rates. Company's sensitivity to changes in interest rates affects short and long term profitability.

  (b) Asset and liability management functions to cost-effectively manage borrowed funds and the investment portfolio.

- **Fraud Risk Management**

  Fraud risk is a critical factor, requiring a proactive approach to detection, prevention, and mitigation. The Company has established a robust fraud risk management framework that includes:

  1. **Fraud Prevention Measures**
     - Implementation of strict Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures.
     - Strengthening internal controls to prevent unauthorized access and transactions.
     - Conducting background verification of employees, agents, and third-party vendors.
  2. **Fraud Detection Mechanisms**
     - Deployment of AI-driven monitoring tools to detect unusual transaction patterns.
     - Regular internal audits and forensic analysis to identify anomalies.
     - Encouraging a whistleblower mechanism for employees and stakeholders to report suspicious activities.
  3. **Fraud Response & Investigation**
     - Establishment of a dedicated fraud response team to investigate incidents.
     - Immediate reporting of significant fraud cases to regulatory authorities.
     - Legal action and recovery measures against fraudsters.
  4. **Continuous Monitoring & Training**
     - Regular training sessions for employees on fraud awareness and ethical conduct.
     - Periodic review of fraud risk policies to address emerging threats.
     - Leveraging technology for real-time fraud monitoring and reporting.

- **Governance risk**

- This risk is associated with inadequate governance or a poor governance structure with an organisation.
- As the Company face the challenges of management succession and the need to recruit managers that can balance social and commercial objectives, the role of Directors becomes more important to ensure the Company's continuity and focus.

✓ **Risk mitigation**

(a) The Board of Directors shall clearly communicate performance expectations and lines of accountability.
(b) Proper direction and accountability from Board of directors, to oversee effective governance mechanisms, strategic decision making, clearly communicate performance expectations and lines of accountability.

➢ **External business environment Risk**

- External business environment risk refers to the inherent risks of the Company's business activity and the external business environment. The Company's business is directly affected by external business environment such as competition, disasters, customer satisfaction etc. The Company needs to check the validity of their assumptions against reality on a periodic basis, so as to respond accordingly.
- While external business risks are out of Company's direct control, Company can still anticipate them and prepare for their impact.

✓ **Risk mitigation**

a) **Scenario Planning and Forecasting –** Develop multiple risk scenarios (e.g., economic downturns, emerging competitors, shifts in customer behavior) to enhance preparedness.
b) **Diversification of Revenue Streams –** Expand into new markets, introduce new products/services, or target different customer segments to minimize risk concentration.
c) **Continuous Market Research –** Invest in ongoing research to stay ahead of market trends, customer preferences, and competitive dynamics.
d) **Financial Hedging –** Utilize financial instruments to mitigate risks related to currency fluctuations, interest rates, and commodity prices.

➢ **Transaction Risk**

- It arises on a daily basis in the Company as transactions are processed and is particularly high as the Company handle high volume of small transactions daily. As the Company make many small, short-term loans, the degree of cross-checking is not cost-effective, so there are more opportunities for error and fraud.

- Inconsistencies between the loan management system data and accounting system data, inadequate loan tracking information, disbursement and payment received information.

✓ **Risk mitigation**

(a) The Company has implemented simple, standardized and consistent procedures for transactions throughout the business transactions. Effective internal controls are incorporated into daily procedures to reduce the chance of human error and fraud.
(b) Regular MIS reporting, monitoring, rectification and minimizing the number of times data has to be manually entered reduces the chance and frequency of human error. MIS does reflects loan tracking, e.g. disbursements, payments received, current status of outstanding balances etc.
(c) MIS collects data and transforms it into the information which can ensure decision making. MIS generates overdue information almost on a daily basis, which helps in analysing delinquency.

➢ **Human Resource Risk**

- Human resource risk in the Company arises due employee turnover, replacements, training, skill, etc. Shortage of critical skills within the Company's workforce, compliance/ regulatory issues, succession planning/ leadership, gap between current talent capabilities and business goals also accounts for human resource risk in the Company.

✓ **Risk mitigation**

(a) Ensuring that the right person is assigned to the right job and that they grow and contribute towards Company's excellence.
(b) Company properly analyses and implements methods for recruitment of personnel at various levels in the office.
(c) Company has proper appraisal systems with the participation of the employee, consistent with job content, peer comparison and individual performance for revision of compensation on a annual periodical basis which is followed regularly.
(d) A sense of belonging and commitment is inculcated in the employees and also effectively train them in spheres other than their own specialization. Activities relating to the welfare of employees are undertaken.
(e) Employees are encouraged to give suggestions and discuss any problems with superiors. Efforts are made to keep cordial relations with employees at all level.
(f) Job profiles are specified, police verification and house verification of employees are conducted, and recruitment of employees is done from various communities.
(g) Employee training, staff welfare, 360 degree appraisal and yearly increments are followed by the Company.

Risk Assessment of Borrowers

It is generally recognized that certain borrowers may be of a higher or lower risk category depending on the customer's background, our references, borrowers net worth and the ability to refund and pay interest etc. As such, the Principal Officer of the Company shall apply to each of the customers due diligence measures on a risk sensitive basis which shall be reviewed every year. The basic principal enshrined in this approach is that the concerned persons should adopt an enhanced customer due diligence process for higher risk customers. Conversely, a simplified customer due diligence process may be adopted for lower risk of categories of customers. In line with risk based approach, the type and amount of information and documents shall vary depending on the risk category of a particular borrower and should be collected from the client. Obligations of the Principal Officer - The Principal Officer of the Company is required to carry out risk assessment to identify, assess and take effective measure.

Appointment of the Principal Officer

The Company shall designate a senior employee as 'Principal Officer' (PO) who shall be located at the Registered / Head/Corporate office of the Company and shall be responsible for this Policy. The PO shall be responsible for monitoring and reporting this policy to management in case of any conflict.

Audit review and policy renewal

The risk management system and its efficiency is analysed through audit reviews and effective methods and measures are adopted to ensure modifications in the Policy on the basis of audit findings. Shortfalls in the policy are identified and are rectified by way of renewal of Policy with approval of Board of Directors.

Cyber Security Risk and Risk Mitigation actions

During the course of business of the Company the Company is using Computers, Laptops other devices, internet and other computer Networks which are vulnerable to

1. **Cybercrime** (including single person or group of persons targeting systems for financial gain or to cause disruption).
2. **Cyber-attack** (often involves politically motivated information gathering),
3. **Cyberterrorism (**intended to undermine electronic systems to cause panic or fear), and
4. Malicious persons or group of persons gaining control of computer and network systems of the Company and the Internet Service providers.

The Board of Directors has adopted a Cyber Security Policy. Furthermore, the Board has directed the IT department to ensure cyber security risk management and fulfill its responsibilities.

It is observed that following common methods are used to threaten / jeopardise cyber-security:

1. **Malware**:

   Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

   There are a number of different types of malware, including:

- **Virus:** A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.
- **Trojans:** A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.
- **Spyware:** A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.

- **Ransomware:** Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.
- **Adware:** Advertising software which can be used to spread malware, and
- **Botnets:** Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

2. **Structured Query Language (SQL injection)**

   An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a databased via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

3. **Phishing**
   Phishing is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.

4. **Man-in-the-middle attack**

   A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure WiFi network, an attacker could intercept data being passed from the victim's device and the network.

5. **Denial-of-service attack**

   A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

6. **Dridex malware**:

   Dridex is a financial trojan with a range of capabilities. Affecting victims since 2014, it infects computers though phishing emails or existing malware. Capable of stealing passwords, banking details and personal data which can be used in fraudulent transactions, it has caused massive financial losses amounting to hundreds of millions.

7. **Romance scams**:

   Cybercriminals commit using dating sites, chat rooms and apps. Perpetrators take advantage of people seeking new partners, duping victims into giving away personal data.

8. **Emotet malware**:

   Emotet is a sophisticated trojan that can steal data and also load other malware. Emotet thrives on unsophisticated password: a reminder of the importance of creating a secure password to guard against cyber threats.

9. End-user protection:

End-user protection or endpoint security is a crucial aspect of cyber security. After all, it is often an individual (the end-user) who accidentally uploads malware or another form of cyber threat to their desktop, laptop or mobile device.

Risk Mitigation Strategy / Cybersecurity Risk Management:

- ✓ The Company shall adopt following Risk Mitigation strategy to avoid and protect the computers and network system of the Company from Cyber attack and to ensure Cyber security.
- ✓ **Updation of software and operating system:** To update the latest security patches.
- ✓ **Use anti-virus software:** Security solutions like Kaspersky Total Security will detect and removes threats. Keep your software updated for the best level of protection.
- ✓ **Use strong passwords:** Ensure your passwords are not easily guessable.
- ✓ **Do not open email attachments from unknown senders:** These could be infected with malware.
- ✓ **Do not click on links in emails from unknown senders or unfamiliar websites:** This is a common way that malware is spread.
- ✓ **Avoid using unsecure WiFi networks in public places:** Unsecure networks leave you vulnerable to man-in-the-middle attacks.

Cybersecurity Risk Management

Cybersecurity risk mitigation involves the use of security policies and processes to reduce the overall risk or impact of a cybersecurity threat. In regard to cybersecurity, risk mitigation can be separated into three elements: prevention, detection, and remediation.

Cybersecurity risk mitigation involves the use of security policies and processes to reduce the overall risk or impact of a cybersecurity threat. In regard to cybersecurity, risk mitigation can be separated into three elements: prevention, detection, and remediation.

Cybersecurity risk management is a strategic approach to prioritizing threats. Organizations implement cybersecurity risk management in order to ensure the most critical threats are handled in a timely manner. This approach helps identify, analyze, evaluate, and address threats based on the potential impact each threat poses.

A risk management strategy acknowledges that organizations cannot entirely eliminate all system vulnerabilities or block all cyber-attacks. Establishing a cybersecurity risk management initiative helps organizations attend first to the most critical flaws, threat trends, and attacks. The cyber security risk management process involves following four stages:

Risk Identification: Evaluating the organization's environment to identify current or potential risks that could affect business operations

Risk Assessment: Analyzing identified risks to see how likely they are to impact the organization, and what the impact could be. A cybersecurity risk assessment is a process that helps organizations determine key business objectives and then identify the appropriate IT assets required to realize their objectives. This involves the identification of cyber-attacks that may negatively impact these IT assets. The organization is required to determine the likelihood of the occurrence of these attacks, and define the impact each attack may incur. The cybersecurity risk assessment should map out the entire threat environment and how it can impact the organization's business objectives. The result of the assessment should assist security teams and relevant stakeholders in

making informed decisions about the implementation of security measures that mitigate these risks.

Risk Control: To define methods, procedures, technologies, or other measures that can help the organization mitigate the risks.

Controls Review: Evaluating, on an ongoing basis, how effective controls are at mitigating risks, and adding or adjusting controls as needed.

A cybersecurity risk assessment is a process that helps organizations determine key business objectives and then identify the appropriate IT assets required to realize their objectives.

It involves the identification of cyber-attacks that may negatively impact these IT assets. The organization is required to determine the likelihood of the occurrence of these attacks, and define the impact each attack may incur.

A cybersecurity risk assessment should map out the entire threat environment and how it can impact the organization's business objectives.

Board of Directors meetings and review

The Board of Directors, in their meetings, shall oversee the implementation of the system and review its annual basis.