INFORMATION TECHNOLOGY AND INFORMATION SYSTEM POLICY

KUSHAL FINNOVATION CAPITAL PRIVATE LIMITED

VERSION HISTORY

Version	Effective Date	Reviewed By	Approved By	Document Changes
4.0	June 23, 2025	Department of Information Technology	Board of Directors	Revisions and Amendments in the Policy
3.0	May 29, 2024	Department of Information Technology	Board of Directors	Revisions and Amendments in the Policy
2.0	March 31, 2023	Department of Information Technology	Board of Directors	Revisions and Amendments in the Policy
1.0	December 7, 2022	Department of Information Technology	Board of Directors	Implementation of the Policy

TABLE OF CONTENTS

1. PURPOSE

This Information Technology or the Information System Policy (hereinafter referred to as "**Policy**") has been devised by Kushal Finnovation Capital Private Limited (hereinafter referred to as the "**Company**") in pursuant to the rules and regulations issued by Reserve Bank of India as amended from time to time. This Policy incorporates, consolidates IT Governance, Risk, Controls, Assurance Practices and Business Continuity/ Disaster Recovery Management. This Policy applies to all aspects of the Company's operations, including information security, data privacy, and third-party relationships.

2. APPLICABILITY

2.1 This Policy applies to all individuals working for the Company at any location and at all levels and grades, including directors, Employees (whether they are working as full time or part time Employees, contractual basis), consultants, interns, external and internal stakeholders, third party Agents, intermediaries, professional consultants and others acting on the Company's behalf and instructions (hereinafter referred to as "**Employees**"), in the course of their engagement for or on behalf of the Company or any other person associated with the Company.

2.2 All individuals are required to read, agree and comply with the Policy and acknowledge.

3. INFORMATION TECHNOLOGY AND INFORMATION SECURITY FRAMEWORK

The Company shall be responsible for maintaining effective information technology (hereinafter referred to as "**IT**") governance and mitigating all the risks associated with the risk management functions, internal control and processes.

The Chief Technology Officer (hereinafter referred to as the "**CTO**") has been designated to look after the Company's IT operations and risk management framework. The CTO is responsible for ensuring the execution of this Information Technology framework (hereinafter referred to as "**IT Framework**"), which comprises Security elements; (ii) *User Role*; (iii) *Information Security and Cyber Security*; and (iv) *Backup Data*. The CTO with it's IT team is also responsible for IT training, on periodic basis.

The framework for each information asset within the Company's scope shall be guided by appropriate security standards/ IT control frameworks. The Company shall ensure that all Employees comply with the extant information security and acceptable-use policies as applicable to them. The CTO and its Team shall review their security infrastructure and security policies annually, factoring in their own experiences and emerging threats and risks and take steps to adequately tackle cyber-attacks including phishing, spoofing attacks and mitigate their adverse effects.

4. SECURITY ASPECTS

(i) Password Policy

All Employees are in charge of safeguarding the security and confidentiality of their passwords and other sensitive information. The password credentials of the Employees must adhere to the IT Framework's password parameters (hereinafter referred to as "**Complexity Requirements**") and standards, as designed by the Company's IT team. It is evident that, the passwords must not be shared or made accessible in a way inconsistent with the IT Framework.

The Complexity Requirements for creating passwords are as follows**:**

- A strong password must be at least 8 (eight) characters, long.
- It should not contain any personal information about the Employee, including his or her real

name, username, or company name.

- It must be very unique from the passwords used previously by the Employees.
- It should not contain any word spelled completely.
- It should contain characters from the four primary categories i.e. uppercase letters, lowercase letters, numbers, and characters.
- The Employees are recommended to change their passwords every 60 (sixty) days to prevent a compromised password from being used for an extended period.
- Passwords must not be stored in a readable format on computers without access to control systems or in other areas where they could be discovered by unauthorized individuals. Passwords should never be written down and stored in a location where they could be discovered by unwanted parties.
- Immediately upon assignment of the initial password and in case of password "reset" situations, the password must be immediately changed by the Employee to ensure the confidentiality of all information.
- Under no circumstances, the Employee shall use another Employee's account or password without proper authorization.
- Under no circumstances should the Employee reveal his or her password(s) to other Employees, unless the Employee has gotten the requisite consent from the department head. In circumstances where passwords are shared in accordance with the foregoing, it is the Employee's responsibility to immediately change the password(s) upon completion of the task for which the password was shared.

(ii) Access Controls

- Access to the Company's electronic information and information systems, as well as the facilities housing them, is a privilege that may be tracked down and withdrawn without prior notice, to the Employees. In addition, any and all access are governed by the rules, regulations and the internal polices of the Company, which include but are not limited to the criteria outlined in this policy.
- Individuals or organizations with access to Company's electronic information and information systems are liable for all activity linked with the Employee's credentials. They are responsible for protecting the confidentiality, integrity, and availability of information collected, processed, transmitted, stored, or communicated by the Company, regardless of the medium on which the information resides.
- Access must be allowed according to the principle of least privilege - solely to the resources necessary by the Employee's current role and obligations.
- Requirements:

    a. The Company requires all users to have a unique ID in order to access its applications and systems.

    b. Alternate authentication procedures that do not rely on a unique ID and password must be approved formally.

    c. Remote access to the Company systems and applications must use a two-factor authentication where possible

d. System and application sessions must automatically lock after 10 (ten) minutes of inactivity.

5. INFORMATION SECURITY AND CYBER SECURITY

(iii) Information Security:

The Company's information security framework consists of the following tenets:

- **Identifying and categorizing of information assets:** The Company utilizes certain IT hardware and infrastructure assets owned and managed by its holding company under a formal intra-group arrangement. A comprehensive and regularly updated inventory of all information assets accessed, processed, or managed by the Company (whether owned or shared) is maintained.
- **Functions***:* The information security function has sufficient personnel, skill level, and tools or techniques, such as risk assessment, security architecture, vulnerability assessment, forensic assessment, etc. In addition, there is a distinct separation of duties between system management, database administration, and transaction processing.
- **Role-based access control** – Information access is determined by well-defined team. The Company has delegated authority to upgrade/change the profiles and permissions, as well as critical business parameters only to its Employees and other parties the Company may deem fit.
- **Personnel Security** – Some Employees, specifically related to IT functions may have in-depth knowledge of financial institution procedures, posing a possible risk to the integrity of systems and data. The Company has a suitable system of checks and balances in place to prevent any such harm to its systems and data. IT Team with privileged access, such as system administrators and cyber security personnel, are subject to stringent background checks and screenings.
- **Physical Security -** Physical access and damage or destruction of physical components may compromise the confidentiality, integrity, and availability of information.
- **Trails** – The Company guarantees audit trails exist for IT assets satisfying its business requirements, including regulatory and legal standards, easing audit, serving as forensic evidence when necessary, and aiding in dispute settlement, for the assets as the Company may deem fit. If an Employee attempts to access an illegal sector, for example, this inappropriate action is captured in the audit trail.
- **Social Media Risks–** The Company will use social media to promote their products and is well-equipped to deal with social media risks and threats in order to prevent account takeovers and malware distribution. The Company ensures additional measures, including encryption and secure communications, to mitigate these threats.
- **Digital Signatures** - A digital signature certificate electronically verifies the identification of an entity. The Company safeguards the validity and integrity of essential electronic documents and high-value financial transfers.
- **Regulatory Returns** – The Company has a suitable structure and format to file periodic regulatory returns with the Reserve Bank of India. The authorised representatives of the Company oversee and validate the filing of regulatory returns.
- **Patch Management and Cryptographical Controls**: The Company has a structured patch system so as to ensure and secure any security vulnerabilities and any foreseen risks. Additionally, the Company has incorporated cryptographic controls which comply towards any extant laws and regulatory instructions.

(iv) Cyber Security

- The Company takes strong measures to avoid cyber-attacks and detect cyber-intrusions swiftly in order to respond, recover, and contain the fallout. The Company takes necessary preventive and corrective measures to address a variety of cyber threats, such as denial of service, distributed denial of service (DDoS), ransom-ware / crypto ware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds, and password related fraud.
- The Company recognizes that managing cyber risk necessitates the commitment of the entire organization in order to establish a cyber-safe workplace. This calls for a substantial amount of awareness from all levels of personnel. The Company ensures that the CTO and its team have an adequate understanding of the risks' intricacies. In addition, it proactively promotes an understanding of their cyber resilience objectives among their customers, vendors, service providers, and other important stakeholders, and assures appropriate action to support their synchronized implementation and testing.

(v) Confidentiality

- The Company maintains the confidentiality of client information in the custody or possession of the service provider, in addition to preserving and protecting security (as described in detail above).
- Employees of the service provider to the Company have access to customer information on a "*need to know*" basis, i.e., only in those areas where the information is required to perform the outsourced function.
- The Company makes certain that the service provider clearly identifies and isolates the Company's customer information, documents, records, and assets in order to maintain the confidentiality of the information. There are robust controls in place at the Company to prevent the mixing of information, documents, records, and assets.
- The Company undertakes that it notifies Reserve Bank of India promptly in the case of a breach of security or disclosure of confidential customer information.

6. BUSINESS CONTINUITY PLANNING (BCP)

- The Business Continuity Plan (hereinafter referred to as "**BCP**") is an integral component of any organization's Business Continuity Management plan, which comprises policies, standards, and procedures to assure the continuation, resumption, and recovery of essential business processes. The Company's BCP is also intended to mitigate the operational, financial, legal, reputational, and other significant effects of a disaster. The CTO has authorized KFCPL's BCP Policy. The CTO with its team shall monitor the operation of BCP through periodic reports.
- The Company mandates that its service providers build and implement a rigorous framework for documenting, managing, and testing business continuity and disaster recovery procedures. The Company ensures that the service provider intermittently tests the Business Continuity and Recovery Plan and once in a while conducts joint testing and recovery exercises with the service provider.
- To mitigate the risk of an unexpected termination of the outsourcing agreement or the liquidation

of the service provider, the Company preserves an adequate degree of authority over their outsourcing and the right to intervene with necessary actions to continue their business operations in such cases without incurring prohibitive expenses and without any interruption in the Company's operations and services to customers.

- The Company ensures that service providers are able to isolating their operations from the operations of the Company and its customers. Under appropriate circumstances, the Company may withdraw from the service provider's custody all of its assets, papers, transaction records, and information given to the service provider in order to continue its business activities, or delete, destroy, or render the same unusable.

- The CTO is in charge of developing, reviewing, and monitoring BCP to ensure their continuing efficacy, which includes identifying essential business verticals, locations, and shared resources in order to provide a complete business impact study.

- The Company also has backup sites in place for its critical business systems and data centres. The Company also tests these ideas on a regular basis. The CTO presents the results, together with the gap analysis, to the Board.

7. BACK-UP OF DATA WITH PERIODIC TESTING

- A periodic backup operation is carried out to prevent information loss due to the destruction of the magnetic medium in which it is stored. The IT team is in charge of backing up the information stored on shared access servers.

- Restoration testing is performed on a regular basis because both hard discs and magnetic tapes are prone to faults. In general, daily full backups are performed for all key business applications, and a complete weekly full backup is performed, including file servers/old data stored on servers.

- The Board approves this IT Framework, but the CTO is in charge of the Company's operational functions. The CTO is also responsible for timely amending this IT Framework in accordance with its operations and/or any change in the regulations or new regulations published by the RBI in regard to this IT Framework, subject to the approval of the Board.