INFORMATION TECHNOLOGY (IT) AND INFORMATION SECURITY (IS) POLICY

Document name	IT and IS Policy
Version	v1.0
Document author	Compliance and secretarial Team
Release date	19-September-2024
Last updated on	19-September-2024
Review frequency	Annual
Approved by	Board of Directors

Regd. Off: 5th Floor, Kumbhat Complex, No. 29, Rattan Bazaar, Chennai – 600 003.

Tel: 044 – 25332173. Email : cs@kumbhatfinancialservoceslimited.com

TABLE OF CONTENTS

Regd. Off: 5th Floor, Kumbhat Complex, No. 29, Rattan Bazaar, Chennai – 600 003.

Tel: 044 – 25332173. Email : cs@kumbhatfinancialservoceslimited.com

1. Background

1.1. It is the policy of Kumbhat Financial Services Limited (collectively, "**Company**", "**we**", or "**us**") to provide a secured operating environment for its business operations and ensure that all information it manages is appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information.

1.2. This Information Technology ("**IT**") and Information Security ("**IS**") policy ("**Policy**") sets out our intention to manage information security as a part of effective governance. It helps us meet our regulatory and legal obligations, and our users' expectations, ensure business continuity, and minimise operational damage by reducing the impact of security incidents.

1.3. This Policy is prepared in line with the guidelines prescribed by the Reserve Bank of India ("**RBI**") under Section-B of the Master Direction - Information Technology Framework for the NBFC Sector dated June 8, 2017 ("**IT Framework**").

2. Scope

2.1. This Policy applies in respect of all information systems including hardware, services, facilities, processes owned by us, made available by us, or which are connected to our managed networks and servers including any personally-owned devices that are used in connection with our business.

2.2. This Policy covers all information collected, handled, stored, processed, or shared by us.

2.3. This Policy applies to any person engaged by us, whether as an employee, agent, consultant, officer, intern, business partner, vendor, contractor or service provider ("**you**"). We have the right to extend the applicability of this Policy to classes of individuals or organisations who may otherwise access, handle, or process information on our behalf, or in relation to their engagement with us.

2.4. In accordance with the IT Framework, the Company shall set up an Information Technology and Information Security Committee ("**Committee**") to assist in the implementation of an IT/IS strategy that is approved by the Company's Board of Directors and to carry out internal checks to ensure the effective implementation of this Policy. The details of the composition of the Committee and its role and functions shall be as approved by the Board of Directors.

2.5. This Policy is Confidential Information (*as defined below*). Please do not share this Policy outside the Company, unless authorised by the Committee.

Regd. Off: 5th Floor, Kumbhat Complex, No. 29, Rattan Bazaar, Chennai – 600 003.

Tel: 044 – 25332173. Email : cs@kumbhatfinancialservoceslimited.com

2.6. This Policy shall be reviewed annually and may be updated from time to time.

3. Regulatory Compliance

The Company has a responsibility to abide by and adhere to requirements, processes or procedures prescribed by law. To that extent, where certain provisions of this Policy are regulated by law, you shall be required to comply with the steps detailed in this Policy in addition to the prescribed requirements under applicable legislation.

4. Organisation and Enforcement

4.1. Policy Owner and Responsibility

a. The Committee shall be the owner of this Policy and shall be responsible for its effective implementation and for monitoring compliance. Its role shall include the following:
   i. Analysing the effect of the IT organizational design on the strategy and direction of IT and the Company's business.
   ii. Ensuring that all existing and new users are instructed about their security responsibilities.
   iii. Implementing procedures to minimise the Company's exposure to fraud, theft or disruption of its systems.
   iv. Ensuring day-to-day management and security of the systems, equipment and services, with specific technical responsibilities being allocated amongst the team and to the outsourced service providers.
   v. Spreading awareness amongst the users about this Policy and ensuring that users understand and abide by them while carrying out work on the Company's behalf.
   vi. Ensuring compliance with the Policy and taking actions where and when required to ensure compliance with this Policy
   vii. Ensuring compliance with relevant legislation, principles and relevant practices of the Company in this regard.

b. The Committee shall also be responsible for maintenance and review of this Policy and also for formulating and/or reviewing all policies, procedures, standards and processes derived from this Policy with inputs from the legal and compliance teams.

c. KFSL shall coordinate with relevant internal and external parties to resolve information security-related issues.

Regd. Off: 5th Floor, Kumbhat Complex, No. 29, Rattan Bazaar, Chennai – 600 003.

Tel: 044 – 25332173. Email : cs@kumbhatfinancialservoceslimited.com

4.2. Exceptions

We recognise that specific business needs and local situations may occasionally call for an exception to this Policy. Exception requests must be made in writing to the Head of IT. The Head of IT must approve in writing, document, and periodically update the Committee on approvals for all exceptions.

4.3. Training

The Company shall provide periodic information awareness security training opportunities and expert resources to help employees, service providers and contractors understand their obligations under this Policy and avoid creating undue risks.

5. Information Classification

5.1. Classification is used to ensure proper controls are implemented for safeguarding the confidentiality of information. However, regardless of classification, the integrity and accuracy of all classifications of information must be protected.

5.2. All our information shall be categorised based on its sensitivity and the value it poses to the Company and shall accordingly be classified as: (a) Public Information or (b) Confidential Information.

5.3. Based on the classification, you should apply appropriate levels of security and access controls.

5.4. "**Public Information**" refers to information that is made available to the general public or information that has been approved for public disclosure. This includes marketing materials, press releases, job announcements, or information that is made available on publicly accessible websites.

5.5. "**Confidential Information**" means information that is not Public Information, and which may cause harm to the Company, its customers, business partners, employees, or other entities or individuals if disclosed or used in an unauthorised manner. Harms may relate to an individual's privacy, our market position or that of our customers, business partners, or legal or regulatory liabilities. Examples include financial data, customer data, revenue forecasts, intellectual property, contracts, employee information, information otherwise designated as "confidential" or some other protected information classification made by an external party and subject to a current non-disclosure or other agreement.

Regd. Off: 5th Floor, Kumbhat Complex, No. 29, Rattan Bazaar, Chennai – 600 003.

Tel: 044 – 25332173. Email : cs@kumbhatfinancialservoceslimited.com

5.6. Internal information that is intended for unrestricted use within the Company and, in certain cases with the Company's affiliate entities, is also treated as Confidential Information and is not available for public disclosure without prior authorisation. Examples include personnel directories, internal policies and procedures, internal correspondence, draft reports, summaries, minutes of meetings, or information generally obtained from our internal networks, systems and servers.

5.7. Unless otherwise marked, you must treat all information as Confidential Information regardless of its source or form, and not available for public disclosure without prior authorisation.

5.8. You must protect Confidential Information with specific technical, administrative and physical safeguards according to the risk posed. Additionally, access to Confidential Information must be restricted on a need-to-know basis.

5.9. You are strictly prohibited from moving any Confidential Information out of our information systems, disclosing, or otherwise making it available without obtaining prior authorisation of the Committee. In the event of mandatory disclosure and/or making available Confidential Information due to an order of a government agency, legislative body, judicial or quasi-judicial authority of competent jurisdiction, such prior authorization shall be obtained from the IT Head.

5.10. In certain circumstances, the Company may treat personal data such as customer's financial data (such as account details, etc.) and other sensitive personal data as a separate category, however, such data shall always be treated as Confidential Information.

6. Data Backups

6.1. Confidential Information data shall be stored on Amazon Web Services (AWS) servers [AP-South-1 [Mumbai)].

6.2. The servers shall have adequate controls in place to recover such data within a reasonable period of time in the event of any damage to the information systems.

6.3. In order to prevent loss of information, the Company shall maintain a backup of all information. The Committee shall direct the Head of IT to perform such periodical back-ups at such intervals and in such manner as it deems necessary.

Regd. Off: 5th Floor, Kumbhat Complex, No. 29, Rattan Bazaar, Chennai – 600 003.

Tel: 044 – 25332173. Email : cs@kumbhatfinancialservoceslimited.com

7. Access Controls

7.1. Based on your business role within the Company and your assigned activities, the Company shall place limits on how you may use and interact with our information assets by controlling your physical and electronic access to information systems containing Confidential Information.

7.2. The Company shall restrict access to specific resources to trained individuals and only on a need-to-know basis. The Committee shall monitor and periodically review user accounts and access levels to confirm that there exists a legitimate business need for access to such resources.

7.3. The Company shall restrict access to areas in which information processing is carried out to only authorised individuals. This includes but is not limited to the following controls:

a. Implementing facility access controls to limit access to our computer systems and facilities in which they are housed to protect against unauthorised access such as through the use of PIN-based login credentials, chip and/or ID reader cards, biometric scanners, swipe-in/swipe-out cards.

b. Granting workstation access to only authorised individuals and ensuring that adequate processes and controls are in place to prevent unauthorised access.

c. Having procedures in place to control and validate an individual's access to our computer facilities based on their role or function, including for visitors, vendors and/or third-party service providers.

8. Information Asset Management

8.1. The Company shall install and configure its information systems based on the current technical standards and procedures.

8.2. We support preventive controls to avoid unauthorised activities or access to data, based on risk levels, and detective controls to timely discover unauthorised activities or access to information, including continuous system monitoring and event management.

8.3. This includes but is not limited to the following controls:

a. **General computer controls:** All devices shall have industry-approved security controls and appropriate core infrastructure to ensure only authorised access to data.

Regd. Off: 5th Floor, Kumbhat Complex, No. 29, Rattan Bazaar, Chennai – 600 003.

Tel: 044 – 25332173. Email : cs@kumbhatfinancialservoceslimited.com

b. **End-user identification and access management:** All end-user computers shall be configured to request user login and authentication from our domain at the time of start-up. Access to the Company's network shall be denied unless an individual has been properly authenticated.

9. Software Protection

9.1. Only licensed copies of any commercial software or in-house developed software shall be used by the Company and the employees, vendors, contractors and third-party service providers.

9.2. You must not install any externally developed software on the Company's information systems without prior approval of the Committee.

9.3. Use of unauthorised copies of commercial software is a criminal offence and shall be subject to disciplinary action.

9.4. Robust anti-virus software and firewall policy shall be ensured. You shall report any detected or suspected viruses, trojan, spyware or malware on your computer to the Committee.

10. Passwords and user credentials

10.1. You must choose strong passwords and protect all user credentials, including passwords, PINs, tokens, badges, smart cards, or other means of identification and authentication.

10.2. The password must be at least 8 (eight) characters long and shall include a combination of uppercase letters, lowercase letters, numbers, and symbols.

10.3. Password rules must be implemented to enable users to select and use strong passwords.

10.4. Passwords must be treated as Confidential Information and must not be shared with others, or saved where it could be accessed by others.

10.5. You may be required to change your password periodically according to current Company standards.

10.6. Should you have reason to believe that your password has been compromised, you must change it immediately and report the incident to the Committee.

11. Data Localisation

Regd. Off: 5th Floor, Kumbhat Complex, No. 29, Rattan Bazaar, Chennai – 600 003.

Tel: 044 – 25332173. Email : cs@kumbhatfinancialservoceslimited.com

11.1. The Company shall take measures to ensure that all information including customer-related data and Confidential information are stored and maintained in infrastructure.

11.2. If any such customer-related data or transaction data is sent to other jurisdictions for processing, the Company shall ensure that such data is deleted from the systems and servers abroad and brought back to India and stored in its servers located in India.

12. Cyber Security

12.1. The Company shall have in place adequate systems to detect any incidents of cyber security crisis at the earliest possible instance.

12.2. As soon as a cyber security breach is detected, the Company shall immediately switch off all the networks connected to the device or server that is compromised.

12.3. All servers must be secured by hardening and ensuring that an antivirus solution is installed, updated and available on all the System(s). The amount of data lost or damaged must be calculated and fresh networks and systems must be installed.

12.4. Options to recover the data and the damage done along with any required legal action must be explored from regulatory viewpoints.

12.5. The magnitude of the attack and their likely impact must be identified and such assets/ information must be blocked from any usage. The degree of theft or compromise must be analysed and recorded.

12.6. All the systems must be updated to prevent occurrences of such incidents in future.

13. IT Security

13.1. Technical security measures have been put in place in order to protect the Company's IT systems from viruses and other malicious software, and all IT systems shall be monitored for potential security breaches.

13.2. All connections to external computer networks and systems including privately owned IT equipment of all kinds must be approved by the IT Head.

Regd. Off: 5th Floor, Kumbhat Complex, No. 29, Rattan Bazaar, Chennai – 600 003.

Tel: 044 – 25332173. Email : cs@kumbhatfinancialservoceslimited.com

13.3. The IT team or any other team responsible for managing the IT systems of the Company shall ensure that all laptops/personal computers used by the Company's employees are encrypted for access to the Company's IT networks using a strong authentication method.

13.4. As a practice, digital signatures (authentication through OTP) shall be used, wherever possible, to protect the authenticity and integrity of important electronic documents.

13.5. The Company shall automate controls by introducing a computer program with logical access, segregation of duties and maker/checker controls.

14. Incident Reporting and Response

14.1. All security incidents should be immediately reported to the Committee via email on it@kumbhatfinancialserviceslimited.com.

14.2. An indicative list of such security incidents which shall require reporting is as follows:

a. Targeted attack on Company network;
b. Gaining unauthorised control/access to Company resources or IT systems;
c. Denial of Service ("DoS") and Distributed Denial of Services ("DDoS");
d. Attach to Company IT network through malicious code, viruses, worms, trojan horses, bots, spyware, malware, adware, ransomware, etc.
e. Attach on Company servers, emails or other networks;
f. Theft of Company data;
g. Data breach/leaks;
h. Attack through fake websites, mobile apps or platforms;
i. Unauthorised access to social media accounts of the Company;
j. Any other security incidents as the Committee may notify its employees.

15. Social Media and Mobile Financial Services Risks

15.1. The Company understands that it is vulnerable to social media risks in the form of account takeovers, malware distribution, unauthorised access, etc. while using social media to market its services.

15.2. The Company shall ensure that all social media accounts are password protected as per the password guidelines mentioned under this Policy. The password for social media accounts shall be shared only with authorised users and one user will be designated as the primary owner of such social media account(s).

Regd. Off: 5th Floor, Kumbhat Complex, No. 29, Rattan Bazaar, Chennai – 600 003.

Tel: 044 – 25332173. Email : cs@kumbhatfinancialservoceslimited.com

15.3. The social media accounts shall also have two-factor authentication enabled wherever available possible.

15.4. The authorised users shall not operate any social media account from public Wi-Fi or any such open networks.

16. Regulatory Returns

16.1. The Company shall ensure that it has adequate systems and processes in place to file regulatory returns to the RBI on a periodic basis.

16.2. The returns filing shall be managed and verified by officials of the Company authorised by the Board of Directors.

17. Business Continuity Planning (BCP)

17.1. The Company understands that it is vulnerable to business continuity risks arising from natural or manmade disasters.

17.2. The BCP shall be designed to minimise operational, financial, legal and reputational risks.

17.3. The Company shall require its service providers to develop and establish a robust framework for documenting, maintaining and testing their business continuity and recovery procedures.

17.4. In order to mitigate the risk of unexpected termination of the outsourcing agreement or liquidation of the service provider, the Company shall retain an appropriate level of control over its outsourcing and have the right to intervene with appropriate measures to continue its business operations in such cases without incurring prohibitive expenses and without any break in the operations of the Company and its services to the customers.

17.5. The Committee shall formulate, review and monitor the BCP of the Company and ensure its continued effectiveness including identification of critical business functions, location / offices / branches, formulating recovery strategies, resource allocation, assigning roles for recovery strategies, preparing back-up sites for critical business functions and other related functions.

17.6. The Committee shall periodically test the BCP and place the results before the Committee.

18. Review

Regd. Off: 5th Floor, Kumbhat Complex, No. 29, Rattan Bazaar, Chennai – 600 003.

Tel: 044 – 25332173. Email : cs@kumbhatfinancialservoceslimited.com

This Policy shall be reviewed on an annual basis by the Committee and approved by the Board of Directors.

Regd. Off: 5th Floor, Kumbhat Complex, No. 29, Rattan Bazaar, Chennai – 600 003.

Tel: 044 – 25332173. Email : cs@kumbhatfinancialservoceslimited.com