KFin Technologies Limited (KFintech)

Information Security Policy

Document Name	**Information Security Policy**
Document Number	**ISPL-001**
Classification	**Internal**

Document Revision History

Version	Date of Release / Revision	Prepared / Revised By	Reviewed &Approved By		Reasons for revisions
			Name	Date	
1.0	15th June 2015	CISO Team	CISO	15th June 2015	Initial version
1.1	10th July 2017	CISO Team	CISO	5th July 2017	Made changes in Responsibilities section of the document
1.1	28th June 2018	CISO Team	CISO	25th June 2018	Reviewed & No changes made
1.2	04th Sep 2018	CISO Team	CISO	03rd Sep 2018	Reviewed & CRA included into the scope
1.3	22nd Nov 2018	CISO Team	CISO	20th Nov 2018	Change in Organization name from "Karvy Computershare Private Ltd" to "Karvy Fintech Pvt Ltd"
1.3	5th July 2019	CISO Team	CISO	2nd July 2019	Reviewed, No Changes
1.4	02nd Dec 2019	CISO Team	CISO	02nd Dec 2019	Change in Organization name from "Karvy Fintech Pvt Ltd to "KFIN Technologies Private Limited"
1.5	15th June 2020	CISO Team	CISO	13th June 2020	Updated the name of CEO from V Ganesh to Sreekanth Nadella
1.5	14th June 2021	CISO Team	CISO	11th June2021	Reviewed & No changes made
1.6	15th Jan 2022	CISO Team	CISO	14th Jan 2022	Updated new KFINTECH logo
2.0	11th Apr 2022	CISO Team	CISO	8th Apr 2022	"KFin Technologies Private Limited" has been replaced with "KFin Technologies Limited (KFintech), formally known as KFin Technologies Private Limited" and "KFPL", "KCPL" is replaced with "Kfintech

Distribution

This document has been distributed to:

Version No.	Board of Directors approval and Distribution Audience
V2.0	This policy document is reviewed and approved by KFintech Board of Directors and is distributed to all Employees of KFintech, External users & Management of KFintech

Table of Contents

1.0 Objective: 5
2.0 Scope: 5
3.0 Policy: 5
4.0 Subsidiary Policies: 5
4.1 Training 6
4.2 Asset Management 7
4.3 KFintech Password Policy: 7
4.4 KFintech Email Policy: 8
4.5 KFintech BYOD Policy: 10
4.6 KFintech Internet Security Policy: 11
4.7 KFintech Employee Acceptable Usage Policy: 12
4.8 KFintech Clear Desk and Clear Screen Policy: 14
4.9 KFintech Antivirus Policy: 15
4.10 KFintech Mobile Computing Policy: 15
4.11 Mobile Phone Usage 17
4.12 Social media 17
4.13.Data Backup 18

1.0 Objective:

At KFin Technologies Limited (KFintech), formally known as KFin Technologies Private Limited, we recognize that one of the fundamental responsibilities to ensure that security of all forms of information entrusted with KFintech by its clients. This is critical for the maintenance of KFintech and its client's reputation and for complying with legal and regulatory obligations to protect all forms of information including business continuity. To do so, KFintech has put in place an information security policy that sets forth principles and requirements governing the collection, usage, retention, disclosure and disposal of information assets. This policy is based on current laws and regulations and will be updated as applicable and governed by the laws and regulations of the time.

2.0 Scope:

The scope covers KFintech information assets, people and infrastructure that creates processes and transmits all activities of Mutual Fund Registry Services, Global Fund Services, Alternate Investment Fund Services, Corporate Registry Business, Communication Services & Central Recordkeeping Agency (CRA) for National Pension System (NPS).

3.0 Policy:

KFintech Private Limited is committed to provide best in class services to its customers by securing all forms of information complying with all regulatory norms and ensuring the highest levels of confidentiality, integrity, and availability. We shall strive to protect the information, resources and facilities from unauthorized access, breach of confidentiality, corruption and destruction whether accidental or deliberate.

4.0 Subsidiary Policies:

Other Subsidiary Policies include as below:

4.1 Training

KFintech Learning and Development department makes all efforts to design, develop, and conduct in-house training programs to cater to the training requirements. These programs will be tailor-made to suit the business needs cost- effectively, wherever, and whenever if the in-house talent is not available/possible, External expertise will be sought/explored. Effectiveness of training is a critical aspect to measure, post-training. The Training Effectiveness form will be administered for the trainee followed by an evaluation.

- All the new recruits shall undergo the KFintech Induction program on the day they join the organization. This induction program includes mandatory information and cybersecurity awareness session. These sessions include topics on cybersecurity threats and vulnerabilities, Data privacy, Employee Do's and Don'ts
- Employee awareness through classroom sessions/Web-based sessions.
- Cyber Security and Information Security awareness through regular email communication
- Follow advisories of industry-standard security organizations such as CERT-IN, CERT-US, SANS, NIST, MS-ISAC on Cyber and Information security and educate the employee
- Employees must undergo mandatory on-job training where ever applicable on successful completion of the Induction program either at the office or through remote on the job training.
- Based on the business demand and requirement, associates will undergo various technical training which is based on the business need and on receiving approval from respective reporting authority and unit head.
- KFintech IT INFRA and Information security teams will provide training sessions on secure remote connectivity technologies, how to secure KFintech information when connected remotely and employee Do's and Don'ts during WFH, etc...

    ❖ **Please Refer to KFintech Human Resource Policies**

4.2 Asset Management

- KFintech assets associated with Information and Information processing are appropriately classified and identified with a unique identification number.
- Employees should not remove these unique identification numbers assigned to their information assets such as Laptops and Desktops.
- An employee is the custodian of information assets assigned to him/her.
- The employee is responsible for securing these assets and to the data that is stored in these information assets.
- Physical assets should be regarded as the property of the KFintech, and due care should be taken while using the same. It is recommended that any problems encountered while using KFintech information assets should be reported in a timely manner to the respective reporting authority or IT helpdesk team.
- Employees must notify KFintech IT Helpdesk or IT INFRA, for any damage or loss of these assets' identification numbers.

4.3 KFintech Password Policy:

- Passwords must be a minimum of 10 characters in length and constructed using a combination of alphanumeric and special characters.
- Passwords must be changed once in every 30 days.
- Passwords must not be divulged to anyone without approval.
- A password history of 8 is maintained for all the systems
- After 5 unsuccessful login attempts the account shall be locked
- Password must have at least one upper case, one lower case, a special character and a numbers in a minimum

- For desktops, the lockout gets released after 30 minutes. For production systems and devices, a request must be raised to the IT team to release the lockout.
- If the security of a password is in doubt, the password must be changed immediately.
- Users are advised not to circumvent password entry with auto logon, application remembering, embedded scripts or hard coded passwords in software.
- Passwords will never be displayed in clear text or stored in readable form in batch files in automatic login scripts, in terminal function keys, in computers without access control, or in other locations where unauthorized people might discover them.
- Default passwords, shipped with devices or software upon installation of the software or receipt of a system with pre-loaded software, must be changed for first login.
- Passwords will not be included in any automated logon process. Exceptions must be approved by immediate manager or respective Head of the department.
- In the event a staff member who has privileged access is terminated or has resigned; the password for privileged access will be removed on the same day.
- System files holding authentication data or passwords will be protected from unauthorized access.
- Computing devices are enabled with the password-protected screensaver or logging off of the device within 15 minutes of idle time.

❖ **Please Refer to KFintech Password Policy**

4.4 KFintech Email Policy:

- Email is a business communication tool and employees of KFintech are obliged to use this tool in a responsible, effective and lawful manner. KFintech employees will be provided with an official email id (<username>@kfintech.com>) based on business requirements.

- Email ID's are created on prior request from HR and or on authorization from respective reporting manager or Head of department.
- Users are authorized to send emails within KFintech group or to external clients based on the privileges provided.
- E-mail facility with privilege to send mails to external domains will be granted to users only after receiving formal approval / request from the respective Departmental Head / Branch In-Charge
- All mailboxes will have a maximum storage limit of 1GB minimum and for any changes has to be reviewed and approved by IT INFRA Head.
- Email attachment size is restricted to 20 MB, all the attachment containing sensitive information must be password protected and password must be sent in a separate email addressing to only intend recipients.
- Email filters are configured at server end to filter email attachments automatically, if found to be contained illegal or absurd contents.
- KFintech official email ID should not be used for personal purpose. All the email communications at KFintech are monitored.
- Delete any email message that you do not need to have a copy of and set your email client to automatically empty your 'deleted items' on closing.
- Web mail access is enabled to employee's only on approving by respective Unit / Department Heads.
- Domain restrictions are enforced to restrict employees sending emails to other domains out of their business.
- Employees are mandate to abide with Email Etiquettes

In addition to the above, the following activities are strictly prohibited

- An employee should not send or forward emails containing attachments infected with a virus, libelous, pornographic, defamatory, offensive, racist, or obscene remarks or content. All such suspicious emails received must be promptly notified to kfin.iteuchyd@kfintech.com
- Must not configure KFintech emails in the mobile phones without prior approval from the respective reporting authority
- Forge or attempt to forge email messages.
- Tamper with or attempt to tamper with email messages.
- Disguise or attempt to disguise your identity when sending mail.
- Send email messages using another person's email account.
- Reveal your username and password to any other person.
- Allow another person to use your account to send email messages
- Use of KFintech e-mail ID to harass, intimidate, defame or discriminate against others or to interfere with the ability of others to conduct business with KFintech.
- Send email messages that violate existing legislation, instructions, civil service guidelines, and codes of conduct.

❖ **Please Refer to KFintech Email Policy**

4.5 KFintech BYOD Policy:

- It is the responsibility of all the employees, consultants, and volunteers to maintain security of their mobile device by following industrial best practices and adhere to the Kfintech IS policies.
- Respective Reporting Manager and or Unit Head is responsible to authorise teleworking using BYOD devices and ensure that the BYOD always meet KFintech criteria and KFintech holds all

rights on the data stored in the BYOD devices and has all rights to audit the BYOD devices without prior intimation.

- Respective Unit or Department Head is responsible to ensure that the employees are aware of KFintech Information Security (IS) controls.
- IT Team is responsible to verify the electronic gadgets for the adherence to KFintech IS controls and policies prior to connecting to KFintech network.

❖ **Please Refer to KFintech BYOD Policy**

4.6 KFintech Internet Security Policy:

- Authorized use of internet
  - Internet usage shall be restricted to serve business requirements.
- Unauthorized use of Internet will include, but is not limited to:
  - Using for personal entertainment, personal business or profit, and publishing personal opinions.
  - Attempting to gain or gaining unauthorized access to any computer system of KFintech or connecting to other organization or systems of other organization.
  - Sending/receiving/viewing racial, sexually threatening, defamatory or harassing messages.
  - Sending, transmitting or distributing proprietary information, data or other confidential KFintech information.
  - Using Internet for non-business purposes and wasting computer resources like uploading and downloading large files not related to business, accessing streamline audio and/or video files, playing games on the Internet and engaging in online chat groups, again not related to business.
  - Introducing computer viruses, worms, or Trojan horses.
  - Downloading obscene written material or pornography.

- The users are not allowed to download or upload any software from/to Internet without prior approval from IT INFRA Head and CISO team. All the requests for software installations must be routed through KFintech ITSM ticketing tool at https://servicedesk.kfintech.com:8090/ .
- Browser access on end-user desktop or Laptops are restricted through CISCO Umbrella, rules are enforced as per business requirements.

❖ **Please Refer to KFintech Internet Usage Policy**

4.7 KFintech Employee Acceptable Usage Policy:

All employees, contractors and third-party users follow rules for acceptable use of information and assets associated with information processing facilities including

- All Data created on KFintech authorized systems, media or for any official purpose remains the property of KFintech and its employees must adhere to organizational policies and procedures.
- Employees are discouraged from using the corporate systems for personal use.
- KFintech systems are monitored using IPS, Endpoint DLP, Email DLP, CISCO Umbrella, Privilege Access Management (PAM), Database Activity Monitoring (DAM) etc., and all Security Incident Event Management (SIEM) alerts are monitored and analyzed by IT INFRA and internal Security Operations Center (SOC) teams.
- KFintech computing systems are to be used for processing data and information relating to KFintech businesses only and KFintech has all rights to audit the systems that create, process, store, and archive KFintech data or Information
- Users are responsible to maintain Confidentiality, Integrity and Availability of information used and/or stored on/in their desktops or laptops.
- Users shall not attempt to access any data or programs for which they are not authorized or shall access on receiving explicit consent of the owner of the data, except in special circumstances and only with approval of respective department Head, or CISO.
- Users shall not make copies of system configuration files for their own personal use or provide to other organizations/people/users for illegitimate and unauthorized use.

- Users shall not download, install, or run security programs or utilities that reveal weaknesses in the security of KFintech systems.
- It is responsibility of employee to report to their immediate reporting authority or Head of the department and infosec@kfintech.com or kfin.iteuchyd@kfintech.com email IDs for any loss of KFintech issued Assets like Laptops or Desktops or information assets storing KFintech data.
- Users are not allowed to bring any personal media /software for use on KFintech owned or issued or authorized systems. Further, users would not be allowed to take computer media out of KFintech premises without appropriate approvals from concern authorities and or CISO.
- Head of ITINFRA /CISO reserves the right to seek justification from any user for installation of any software and may suggest alternate software in the best interest of the company.
- Users must ensure that they restart their Desktops and Laptops at least once in a day and report any issues or incidents or malfunctioning of KFintech issued assets @ kfin.iteuchyd@kfintech.com email ID
- The employee must not make changes to system configurations, Install unauthorized software that reveals weaknesses in the security of KFintec systems
- KFintech reserves all rights to take appropriate action if employees found to be performing suspicious activities using KFintech or employee-owned computing systems and its internet and email services. Employee must adhere to Kfintech BYOD policy in case using their own computing devices.
- Carrying personal data storage or media devices like pen-drive, external HDD, CD writer, floppy drive, or any other storage device into office premises is strictly prohibited. In case any business requires to connect must take prior approval from respective reporting authority, handover such devices to the IT helpdesk team to perform a thorough scan of the content for any malicious codes prior to connecting to KFintech information asset.
- The employee is responsible for the security of the KFintech data and regular updating of their passwords and user accounts (system & email). Source code is restricted for usage within office premises alone and authorization is required otherwise.

❖ **Please Refer to KFintech Employee Acceptable Usage Policy**

4.8 KFintech Clear Desk and Clear Screen Policy:

- Information must be protected from unauthorized disclosure, modification or theft. A clear desk policy for Physical / hardcopies of paper assets and removable storage media and a clear screen policy will reduce the risks of unauthorized access, loss and damage during and outside normal working hours to electronic data stored locally and within KFintech infrastructure.
- KFintech issued desktops and Laptops should not be left unattended or logged on, when the person responsible is away from his / her work area or workstation.
- Always ensure that your system / screen is locked when moving away from your workplace.
- The screen saver password must be put in place. When the user leaves the desk, the screen should be enabled within 15 minutes.
- All documents that contain sensitive information should not be left open on the desk in the absence of the person responsible. If such documents are available open on the desk, they should be closed and placed in lock and key before the person leaves the desk.
- Restricted documents must be kept locked in cupboards and should be accessible only by the authorized person.
- Documents that are to be photocopied must be approved by immediate reporting authority or respective Head of the department.
- Restricted hard copies should be destroyed as per KFintech disposal policy and should not be re-used as rough paper.
- Computer media will be stored in suitable locked cabinets when not in use, especially after working hours.
- Photocopiers machines will be put in power off state and protect from unauthorized use outside normal working hours.
- Backup tape media should be kept in a lock and key under fire resistant safe when not in use.

❖ **Please Refer to KFintech Clear Desk and Clear Screen Policy**

4.9 KFintech Antivirus Policy:

- All the KFintech information assets like Desktops, Laptops, servers, and other information processing equipment are adequately protected against malware software. Symantec endpoint protection antivirus software is installed in all KFintech Desktops and Laptops and Trend Micro antivirus software is installed in Servers.
- IT INFRA and KFintech SOC team is responsible for administration and maintenance of latest version of anti-virus software, the signatures database, patches on all the desktops, laptops, and servers.
- Vendor provided patches are update automatically through antivirus server on all KFintech desktops, laptops, and Servers.
- Antivirus client is installed in KFintech issued Desktops and Laptops and automatic scans are configured and schedule on daily basis. Configuration are set to verify for every four hours and initiate the scans for the systems those are not scanned in the previous cycle. Server are configured to update the vendor released patches immediately and scans are performed on weekly basis.

    ❖ **Please Refer to KFintech Antivirus Policy**

4.10 KFintech Mobile Computing Policy:

Desktop/ Laptop Usage

- The employee should take due care of the complete system and its peripherals (mouse/monitor/keyboard/external storage media etc.) and should not swap with any computer or peripherals.
- An employee is expected to maintain the identity of computers by not tampering with the asset ID and vendor's Serial No. (E.g. Dell/ IBM/HP etc.) and inform IT, helpdesk team, in the event of these labels, are not available on their computers.

- Desktops and Laptops should be locked when unattended to protect the machine from unauthorized access.
- Objectionable wallpaper should not be used on the assigned machines.
- The employee is not allowed to bring their personal Laptops / Computers / Printers and other electronic gadgets and connect to KFintech networks.
- The employee must ensure the configuration of anti-virus software on their system assigned. Non-availability of such software must be informed to IT support or IT Infra teams.
- KFintech IT helpdesk and IT Infra team are authorized to make any changes to the systems standard configurations, install and configure the software as per business requirements.
- The system should be turned off while leaving for the day unless it is a business requirement to keep it On.
- Keep recording devices away from your workspace at home
- Use of personal email accounts for business purposes is prohibited
- Observe password requirements and do not write your password on paper
- Watch out for unauthorized overlooking (shoulder surfing)

In addition to the above, the following activities are strictly prohibited

- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account credentials or passwords to others or allowing the use of your account by others, including peers, collogues, family members, friends, and other household members.
- Using a KFintech computing asset to actively engage in procuring or transmitting material that is in violation of hostile workplace laws.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing/ intercepting data of which the employee is not an intended recipient or logging into a server or account that the employee is not explicitly authorized to access.

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's/networks session, via any means.
- Transferring KFintech and its client's information to unauthorized parties.
- Employee assigned systems are subject to random checks and they are discouraged from downloading or installing unauthorized network hardware or software or altering the KFintech standard settings.
- An employee must not download, install and run security programs that reveal the details of the security of the KFintech system like password cracking programs, etc.,
- The employee must not use KFintech systems to transfer illegal information on the Internet or to commit a crime.

❖ **Please Refer to KFintech Mobile Computing Policy**

4.11 Mobile Phone Usage

- An employee is prohibited to carry his / her smart mobile phone to the working area while working at the office. In case it is required for any business reasons or to perform his /her day-to-day activities, prior authorization or approval from respective reporting authority and the unit manager is a mandate.
- While at the office when called for any business requirement during the work from home period, an employee carrying a smart mobile phone without authorization is freeze and taken into the custody of KFintech and the organization is not liable for any employee personal data stored in such mobile devices.

4.12 Social media

- An employee should be aware that KFintech may observe content and information made available by employees through social media. Employees should use their best judgment in posting material that is neither inappropriate nor harmful to KFintech, its reputation, employees, or customers.

- Employees are not to publish, post, or release any information that is considered confidential or not public. If there are questions about what is considered confidential, employees should check with their reporting authority and /or respective authority of the KFintech Human Resources Department.
- Social media networks, blogs, and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these inquiries to the authority of the KFintech Human Resources Department and/or authorized KFintech spokespersons.
- If employees find to encounter a situation while using social media that threatens to become antagonistic, employees should disengage from the dialogue in a polite manner and seek the advice of his /or reporting authority.
- Employees should get appropriate permission before you refer to or post images of current or former employees, members, vendors, or suppliers. Additionally, employees should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks, or other intellectual property.
- Subject to applicable law, any online activity performed by an employee that violates the KFintech Code of Conduct or policies may subject to disciplinary action and further to termination of employment.

4.13.Data Backup

- All necessary software and system images are backed up regularly in order to ensure that each application and its data can be recovered in the event of systems failure, loss of service, or loss/corruption of data.
- Back-up copies of essential information and software are taken on a regular basis.
- An employee must provide details of data to be backed-up and its frequency to the IT INFRA and Database teams.
- An employee in the coordination of the respective unit head must send a request to the IT INFRA and Database teams to restore data from backup media.

- The respective unit head is responsible to validate and certify the accuracy of data restored by the IT INFRA team.

Please Refer to KFintech Backup Policy

ANNEXURE – I

KFin Technologies Limited ("KFintech"), formally known as KFin Technologies Private limited, makes every effort to honor the preferences of our clients. Kfintech regards the customer data as a key asset and ensures the protection of these information assets held by the organization in a secure manner.

Kfintech Information Security Policy
"KFin Technologies Private Limited (Kfintech) is committed to providing best in class services to its customers by securing all forms of information complying with all regulatory norms and ensuring the highest levels of confidentiality, integrity, and availability. We shall strive to protect the information, resources, and facilities from unauthorized access, breach of confidentiality, corruption, and destruction whether accidental or deliberate".

Information at KFintech exists in different forms which include physical, electronic, video, audit, etc.,. Maintaining Confidentiality, Integrity, and Availability of such information is the responsibility of our employees. To prevent from Information and Cybersecurity threats and risks, KFintech has set below guidelines on the usage of its infrastructure and information assets. Employees found to be violating these guidelines are subject to disciplinary action.

KFin Technologies Limited, formally known as Kfin Technologies Private Limited will achieve this by:

Applicability

All KFINTECH personnel and suppliers, employed under contract, who have any involvement with information assets covered by the scope of the Information Security Management Systems, are responsible for implementing this policy and shall have the support of the Management.

Responsibilities

- The chief Executive officer is the approving authority of the policy
- The steering committee of Senior Management Staff, representing relevant functions will work to
    - Evaluate the performance and effectiveness of ISMS in the recent past; and accordingly decide upon the direction of ISMS in near future
    - Decide upon the strategic alignment of ISMS objective with overall organizational objective
- The chief Information Security Officer (CISO) is responsible for the implementation of this policy through the appropriate standards and procedures.

- All personnel and contracted suppliers follow the procedures to maintain the information security policy.
- Any deliberate act to jeopardize the security of information that is the property of KFINTECH – to

their customer or suppliers will be subject to disciplinary and/or legal as appropriate.

Sreekanth Nadella
Chief Executive Officer