Cyber Security and Business Continuity Plan

Document Control	
Title	Cyber Security and Business Continuity Plan
Policy Owner	Designated Partners
Preparer and Reviewer	Compliance Officer
Approved by	Designated Partners
Version	V3
Tentative next review	On any Regulatory change or Annual, whichever is earlier
Date of circulation to relevant stakeholder after approval	N.A.

Version Summary

Version	Updates	Reviewed Date	Department	Approved by
V3	Third Policy	16.05.2026	Compliance	Designated Partners

Contents

1. INTRODUCTION 3
2. SCOPE, APPLICATION AND OBJECTIVE 3
3. ELEMENTS OF CYBER SECURITY AND IT SECURITY POLICY 3
4. DATA SECURITY 4
5. HARDWARE AND SYSTEM SECURITY 5
6. E-MAIL USAGE POLICY 6
7. INTERNET SECURITY AND USAGE 7
8. CLOUD SECURITY 10
9. INCIDENT RESPONSE 11
10. LEGAL AND CONTRACTUAL OBLIGATIONS 12
11. DATA OWNERSHIP AND LOCALIZATION 13
12. COMPLIANCE AND RISK MANAGEMENT 14
13. RELIANCE ON THIRD PARTY CLOUD SERVICE PROVIDERS 15
14. BUSINESS CONTINUITY PLANNING (BCP), DISASTER RECOVERY & CYBER RESILIENCE 15
15. VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT)/AUDIT OF THE INFORMATIONAL TECHNOLOGY INFRASTRUCTURE 18

1. Introduction

Moneysukh Advisors IFSC LLP *(hereinafter referred to as " LLP")*, is a Fund Management entity regulated by International Financial Services Centres Authority having registration No. ACB-8040 and is acting as an Investment Manager of existing fund and funds that may be launched in the future.

Pursuant to IFSCA (Fund Management) Regulations, 2022, A registered FME shall have robust cyber security and cyber resilience framework in accordance with the requirements as may be specified by the Authority from time to time and accordingly, the Company/LLP has appointed Designated Partner (*hereinafter referred to as "the fund administrator")* as a fund administrator.

The LLP has adopted the terms of the Cyber Security and Information Technology Policy of the fund administrator along with the dynamics of IT Infrastructure of the LLP to bring it in line with the regulatory requirements and to ensure that our business and our clients are constantly protected from cyber risks. LLP's security strategy is to protect its business and its Clients by continually assessing and reviewing risks as well as the cyber threat landscapes and to have strong disaster recovery system in place for the cyber incidents.

2. Scope, Application and Objective

This Policy applies to the LLP, its Designated Partners, Officers and all its employees including any of the person authorized to act on behalf of the LLP. All persons to be referred as "Concerned Persons." The Policy and the Annexures thereto are reviewed and confirmed by the Designated Partners of the LLP.

The objective of the Cyber Security and IT Policy is to highlight the key risks and to provide for the measures to be adopted to prevent any information technology threat and any cyber breach to the data and devices of the LLP or the Clients and to ensure that various other IT requirements like Log Retention, Audit, Access Controls, Email Usage Policy etc. are in place.

3. ELEMENTS OF CYBER SECURITY AND IT SECURITY POLICY

The following elements are considered to establish the Cyber Security Framework:

1. Data Security
2. Hardware and System Security
3. E-Mail Usage Policy
4. Internet Security & Usage Policy
5. Cloud Security
6. Incident Response
7. Legal And Contractual Obligations
8. Data Ownership and Localization
9. Compliance and Risk Management
10. Reliance on Third Party Cloud Service Providers
11. Business Continuity Planning (BCP), Disaster Recovery & Cyber Resilience.
12. VAPT/Audit of the Informational Technology Infrastructure

The measures to control and manage the above elements of cyber security are provided in detail in this policy hereinafter.

4. Data Security

- **Data Access Control:** The LLP uses the principle of least privilege to control access to information. Access is only granted where needed and must go through an approval process. Unique domain IDs, strong password policies, multifactor authentication, Privileged Identity Management, and central logging of events are used to ensure sensitive information is protected.
- All administrative users shall be tracked via a ticket/ request by the LLP, and the same shall be provided to the Clients on request.
- Access to systems or interfaces to be provided to the Client's data only if the Client has given explicit time-limited or special permission for that access.
- Data of each Client shall be isolated and inaccessible to any other tenants and no access of data will be provide to any external party without the consent of the Client except for audit and regulatory requirements.
- **Document and files usage control**: Information and records are now mostly kept electronically. It is therefore important that Concerned Persons are aware of the legal consequences of this medium. All electronic documentation is recognised for legal purposes, like paper-based documentation. This includes internal records as well as external communications. Internal records such as Group records, departmental reports, working records must be accurately completed and kept up to date. Any abuse will be treated similarly to the falsification of paper records and will be dealt with under the disciplinary process.
- **Measures against Phishing attacks:** Majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence the LLP issues standards for avoidance of clicking on links and attachments in email to establish an essential pillar of defence. Required Anti-Virus Scan Software is adequately installed on the systems and devices of the LLP to scan the external emails and attachments.
- **Data Authenticity Controls**: All external communications with clients, associates and suppliers must be considered for the relevance of content and accuracy and potential to commit LLP's business transactions or exposure to liability. Therefore, employees/ partners should clearly evaluate such communications before they are sent. In addition, attachments received from external sources may be subject to copyright and should not be forwarded unless permission is expressly stated.
- It is LLP's policy to have a **disclaimer** attached to every email communication. This must be set up on every account to include on each employee's digital signature and to appear on each e-mail sent.
- **Data Encryption:** Data-at-rest encryption to be done with strong encryption algorithms. Data object encryption, file level encryption or tokenization in addition to the encryption provided at the platform level shall be used. Data-in-motion including the data within the cloud shall be encrypted. Session encryption or data object encryption in addition to the encryption provided at the platform shall be used wherever any sensitive data is in transit.
- Data-in-use i.e., wherever data that is being used or processed in the cloud, confidential computing solutions shall be implemented.

- "Bring Your Own Key" (BYOK) approach shall be adopted, which ensures that the LLP retains the control and management of cryptographic keys that would be uploaded to the cloud to perform data encryption.
- The LLP and its Client's data must only be accessed through approved channels and no data is permitted to be stored or processed on devices or outside of approved application containers. It is each user's responsibility to ensure that their user ID is never shared or left visible for another user to see.
- **Backup and recovery measures:** All the data available with the LLP on will basis should be adequately backed up on everyday basis on clouds or physical servers located in jurisdiction of the Clients or India in case of the LLP.
- The backup shall be logically segregated amongst production/dev/UAT environment to ensure that the malware infection in such systems does not percolate to backup environment. Backup devices shall also have secured access for designated persons of the LLP only. LLP should ensure that production environment is kept properly segregated.
- The LLP shall ensure that the minimum retention requirements for data (including logs) as prescribed by regulators are met and that the required data, logs, etc. are archived, even if the Client moves out of the cloud/ changes.

5. Hardware and System Security

The principle of Defence-in-Depth is used for the Hardware and System Security. Multiple layers of security are in place to protect against IT threats. **Security patches are deployed on a regular basis and system scanning is conducted** of the infrastructure to ensure critical systems meet all current standards. The principal of **no data on the endpoints is enforced** with mobile device management. All devices can be remotely wiped in a scenario where they become lost or stolen. Continuous vulnerability assessments and independent penetration testing is performed to identify potential weaknesses.

A Hardware Security Module is a device that is used for management of Keys, as well as for implementing various functions like encryption, decryption, authentication, etc. The purpose of this policy is to highlight the rules expected of all users in respect of the use of any LLP's or Third-party systems used by the LLP to access or use the internet via LLP's property or technology.

Each user is responsible for all activities carried out under their user ID and on LLP's provided equipment. It is each user's responsibility to ensure that their devices are never shared or left anywhere or open on desk for unauthorized person to use. All suspected malicious activity must be reported to Information Security or the Service desk contact@moneysukhifsc.com

All the Devices shall be configured with appropriate security controls, up to date software versions, and configuration of standard apps, such as browsers, security tools, up to date Anti-Virus, before they can access LLP's Services.

Windows PCs, Linux, and Apple PCs must support current citrix technology and be running Windows 10 or above. Linux based systems including Apple should be running the latest available version and be fully patched.

To prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the Company devices. Devices must be encrypted with strong encryption along with access to Mobile Device Management (MDM) App or Software to connect to the LLP services. Operating System and Software must be current and up to date [patched] to connect to LLP's services. Anti-Virus /Endpoint Protection is required to be installed and maintained with to date signatures to connect to Company's services. The Group's strong password policy is: Passwords must be at least 8 characters and a combination of upper-and lower-case letters, numbers, and symbols. The device must have a screen lock enabled and lock itself with a password or PIN if it's idle for five minutes. Smartphones and tablets that are not compatible with the MDM and MFA software or cannot employ the required controls are not supported and will not be allowed.

The Company/LLP will reserve the right to remove access to the applications and containers on a device through remote means. The Company/ LLP also reserves the right to disconnect devices or disable services without notification.

The Company / LLP allows service users the ability to use personal devices and non corporate systems including smartphones and tablets of at work for their convenience. The Company/LLP reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

Smartphones including iPhone, Android, Blackberry and Windows phones are allowed where the current MDM Software requirements are met along with current configuration requirements. Tablets including iPad and Android are allowed where the current MDM Software requirements are met along with current configuration requirements.
The Data related to the LLP may be remotely wiped if:
1) the device is lost,

2) the employee terminates his or her employment,

3) IT detects a data or policy breach, a virus or similar threat to the security of the LLP's data and technology infrastructure.

Lost or stolen devices must be reported to the LLP within 24 hours.

The employee assumes full liability for risks including, but not limited to, the partial or complete loss of personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

The employee assumes full liability for risks including, but not limited to, the partial or complete loss of personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

6. E-MAIL USAGE POLICY

- LLP's electronic mail systems are to be used only for business purposes.

- Users must not use an electronic mail account assigned to another individual to either send or receive messages. If there is a need to read another's mail (due to absence/vacation etc.) requests must be made to Service desk [mail id] and approval sought, auto-forwarding is not permitted.

- Unacceptable practices such as snooping, hacking, transmitting illegal items or nuisance items such as chain letters, are subject to disciplinary action including possible dismissal.

- The use of Messaging systems must be approved, transfer of LLP's data using unauthorised systems is considered a data breach and subject to disciplinary action including possible dismissal. Microsoft Teams is linked to each employee's primary and Outlook account and is classified as an extension of employee's Outlook profile, communications, and audio/video calls. The use of Teams messaging should be conducted whilst following the email policy.

- Each employee must use the standardised e-mail signature structure and fonts outlined by Group Marketing and HR. All emails to clients should be re-read before being sent and should be polite, professional, and signed off fully with 'Regards, name' or' Thanks, name'. The shortcuts taken with internal Group LLP emails must not be taken with emails to clients.

- All employees are reminded to set their Out of office notifications when on leave (including Local holidays as we are global business email queries will keep coming from other countries). Shared or Group mailboxes are the duty of each employee having access to a specific mailbox to check and when necessary, forward the email/query to the appropriate person.

- Only 'open-projects' should be kept in 'in-box'. Messages that arrive should be responded to immediately and deleted if possible.

- A reply should be sent indicating when a full response can be given if it cannot be given immediately. It then remains in the 'inbox' until responded to in the timeframe sent originally. No e-mails should go unreplied to for more than 24 hours. No projects should take more than 48 hours to reply to unless agreed with the client. All e-mails older than 3 months will be automatically archived and will be available in the archiving and journaling solution.

7. Internet Security and Usage

LLP recognises the use of the internet as an essential part of our working life. However, access to the internet is provided primarily for business use, therefore all employees are urged to use common sense and good judgement when using Group's information and communication systems. Employees may make use of these systems where it does not interfere with their job performance or breach any policies or procedures. Inappropriate internet use could result in the following, hence the importance of this policy:

- Financial or reputational damage to [LLP Name]
- Legal implications for Group employees or others
- Upset for other employees, customers or third parties

- Excessive use for non business related reasons could lead to reduced employee's productivity

All the LLP's computer equipment, software, and facilities, wheresoever used, are the property of the Group and / or outsourced partners, including all documents, materials and files created or modified while using Organisation's computer equipment.

Please note the following whilst using the internet:
The LLP's internet access is provided for the conduct of the LLP's or group's business.

While accessing the Internet, users must not engage in any activity which is illegal, offensive, disruptive, or likely to have negative repercussions for LLP. Content blocking and monitoring software is in place.

Organisation's internet systems must not be used to download or distribute copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorisation from the owner of the relevant information or materials.

Organisation acknowledges that users may occasionally need to use their internet systems for personal use; limited personal use can only be permitted provided that such use fully complies with requirements of this Policy and any other requirements specified by Organisation

To protect its legitimate business interests, Organisation reserves the right to monitor, and given reasonable grounds for investigation to intercept, access and disclose user activities including any web-based content such as, pictures or documents, created, received, stored, or sent over the internet at any time without notice.

By using LLP's internet systems users are deemed to have consented to the monitoring, interception, access, and disclosure described in this Policy.
This policy applies to all parties, including but not limited to employees, contractors, consultants, and temps etc., who access the Internet through Group computers, computing, or networking resources. The Group network, computers, servers, and other equipment utilised to connect employee to the Internet are the property of the Group and are to be used to serve the business needs and purposes of the Group. Proper conduct is expected of all users on the Internet, as it is in all public forums. Failure to comply with this policy may subject employees and related persons to disciplinary action, including possible dismissal.

Accessing the Internet for any illegal conduct, personal financial gain, private business activities, unethical purposes, creation of personal web pages, or any other improper reason is prohibited within the Group. Viewing, transmitting, or storing of pornographic, indecent, or otherwise offensive material is also prohibited. The Group reserves the right to monitor, access, and review, restrict or terminate the use of the Internet.

The Group IT Department must approve, in advance, the use of new and existing Internet connections to establish new distribution channels.

The Employee and concerned person are personally responsible for all activities originating from the use of their account and / or system. This includes responsibility for all messages and / or files that originate or wilfully accept via the Internet; users are not authorised to accept / download commands, programs, or software.

If any sensitive Group information, passwords, or other system access control mechanisms are lost, stolen, or disclosed, employee must notify the Manager and the IT Security or Service desk immediately.

Terms of LLP's Internet Access:

Any usage of LLP's internet access for personal use is on the basis that personal use will be treated in the same way as business use and may be monitored similarly.

BUSINESS USE: The LLP provides internet access to enable users to conduct LLP's business more efficiently and effectively. The following rules apply:

- To ensure that anti-virus protection is kept up to date users must comply with IT departmental instructions.
- Users are prohibited from accessing, transmitting, or downloading any material which may be deemed obscene, pornographic, threatening, or of a racial, sexual, or harassing nature.

- Users are prohibited from tampering, bypassing controls, removing any website blocking and monitoring software, or using any method of bypassing any IT policies

PERSONAL USE: Always follow all rules set out in this Policy. Ensure that any personal use of the system:

- is appropriate during lunch hour; however, employees are advised that excessive VDU usage can be detrimental and encouraged to move away from their desks during this time to rest their eyes. (see below for a description of what is inappropriate)
- Does not interfere with work responsibilities
- Does not have a negative impact on the LLP or group in any way
- Does not introduce potentially threatening software to LLP's systems or no user is authorised to download any software into the LLP's environment on Citrix or onto their local PC without preapproval from the Head of IT or IT Service Desk.
- Personal e-mail accounts are not to be used for business purposes under any circumstances unless approved by the Head of IT or IT Service Desk for BCP purposes.
- Use of personal removable media and storage is strictly prohibited.

INNAPROPRIATE USE:

Usage of Organisation's internet systems should not involve users in any activity that is illegal, offensive, or likely to have negative repercussions for Group. Users must not use, retain, distribute, or disseminate any images, text, materials, or software that:

- Are or might be indecent or obscene, or might be offensive or abusive in that their content, is or can be a personal attack, rude, sexist, racist, pornographic, or generally distasteful or in any way contravene LLP's Dignity at Work policy.
- Any usage of Organisation's internet access for personal use is on the basis that personal use will be treated in the same way as business use and may be monitored similarly.

- Encourages or promote activities which make unproductive use of work time or other resources.
- Encourages or promote activities which would, if conducted, be illegal or contrary to any Group policy, including the Dignity at Work policy
- Involves activities outside the scope of user's responsibilities.
- Might be defamatory or otherwise incur a liability on the part of Group
- Adversely impacts on the image of LLP or the Group
- Interferes with the intellectual property rights of third parties; no sites known to contain inappropriate material may be visited at any time.

MONITORING INTERNET ACCESS:
Organisation's internet access is subject to review to determine whether there have been any breaches of legal requirements or Organisation's policies and standards. Use of the internet may be monitored to ensure compliance with these policies. Please be aware that a record is maintained of the site's users visit.

Disclosure and Use of Information

The contents of activity logs may be disclosed within Organisation in certain circumstances. Such disclosure shall be limited to those who have a reasonable need for access to the information. These logs are only typically released to:

- support compliance with laws and regulations.
- ensure the security of our systems and data, typically by preventing access to questionable sites which may attempt to download malicious code.
- aid investigations into internet abuse.

LLP will attempt to honour any user's reasonable objection to the disclosure to a third party of information, based on the claim that the contents are personal or private in nature, unless such disclosure is required to serve a legitimate business purpose and/or to comply with a legal obligation and/or to comply with the requirements of any regulatory or supervisory authority.

8. Cloud Security

The LLP shall check public accessibility of all cloud instances in use. Make sure that no server/bucket is inadvertently leaking data due to inappropriate configurations. To Ensure proper security of cloud access tokens the tokens should not be exposed publicly in website source code, any configuration files etc.

The LLP has implemented appropriate security measures for testing, staging and backup environments hosted on cloud. The production environment is kept properly segregated from these. LLP shall Disable/remove older or testing environments if their usage is no longer required. The LLP shall employ hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments.
Security controls such as IPS, Firewall, WAF, Anti DDOS, etc. are in place and additional controls such as IPSEC VPN shall be adopted, wherever necessary, to secure such interfaces.

The LLP has ensured that the data security controls in the nature of Anti-Virus, Data Leak Prevention (DLP) solution etc. are installed and configured on the cloud deployments for effective data security. The LLP shall also evaluate the baseline security controls provided by the Third Party Cloud Service Providers (CSPs) and may demand additional controls (from CSP) if required.

The LLP shall adopt the micro segmentation principle on cloud infrastructure. Only the essential communication channels between computing resources shall be allowed and the rest of the communication channels shall be blocked.
The LLP shall also consider the option of utilizing Cloud Access Security Broker (CASB)/ Secure Access Service Edge (SASE)/ similar frameworks or tools for effective monitoring of network, enforcement of policies etc. The Llp shall ensure that a backup and recovery policy is in place to address the backup requirement of cloud deployments. The backup and recovery processes shall be checked at least twice in a year to ensure the adequacy of the backups.
The backup shall be logically segregated from production/dev/UAT environment to ensure that the malware infection in such systems does not percolate to backup environment. Wherever CSP's backup services are utilized, adequate care should be taken with encryption solution and Key management.

The LLP has deployed web and email filters on the network. Configured the devices to scan for known bad domains, sources, and addresses, block these before receiving and downloading messages. Scanning of all emails has been enabled majorly with attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.

To block the malicious domains/IPs after diligently verifying them without impacting the operations. CSIRT-Fin/CERT-In advisories which are published periodically should be referred for latest malicious domains/IPs, C&C DNS and links.

Restrict execution of "powershell" and "wscript" in enterprise environment, if not required. Ensure installation and use of the latest version of PowerShell, with enhanced logging enabled, script block logging and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.

The Organisation utilizes host based firewall to prevent Remote Procedure Call (RPC) and Server Message Block (SMB) communication among endpoints whenever possible. This limits lateral movement as well as other attack activities. Practice of whitelisting of ports based on business usage at Firewall level has been implemented rather than blacklisting of certain ports. Traffic on all other ports which has not been whitelisted should be blocked by default.

9. Incident Response

The LLP has a full incident response plan in place for all incident types. In the event of an incident there is a dedicated IT Personnel that will address the issue and expedite a resolution. Breach Notification shall be provided by the LLP to the Client or in case of LLP by the dedicated IT Personnel of the LLP to the management or the board of the LLP of any cyber security incident (for example data breach, ransomware, etc.).

Following actions may be taken to respond to the incidents:

1. Reporting to the Client, the Designated partners of the LLP and Regulators wherever applicable. The reporting shall also be done as per the norms/ guidelines/ circulars issued by regulators (wherever applicable) as per the contractual agreement signed between the LLP and Client. The LLP shall provide all related forensic data, reports and event logs as required by regulators or any other government agency. The incident shall be dealt as per the Security Incident Management Policy of the Client along with the relevant guidelines/ directions issued by the regulator if any.

2. Unauthorized access or breach of this policy conditions or any event of malicious attack on the data or system shall be tracked to the source to identify the loss or damage caused and the quantum and quality of the data leaked or inappropriate. All such files and data or the system that has been compromised will be subjected to detailed scrutiny to identify the reason of such incident and measures will be taken to higher security checks and protections of the device or system to prevent any further incident. Deleting of data or rights, default setting storage, device lock or such mitigation measures may be taken to control the impact of cyber incident.

3. The continuous monitoring shall be done in an integrated manner and the services/application/ infrastructure deployed in cloud and it should be treated as an extension of the Client's on-premises network. Additionally, only logs, meta-data should be shipped to shared SOC of the Client and the LLP shall ensure that PII/sensitive data should not be shipped to the SOC.
4. Data Back-Up and Storage Servers shall be restored and recovered to working conditions as immediately as possible removing the impact of the Cyber incident.

5. Strong log retention policy has been implemented as per applicable regulations. Monitoring of all logs of events and incidents to identify unusual patterns and behaviours should be done. LLP is subjected to audit that all logs are being collected.

10. Legal And Contractual Obligations

1. A clear and enforceable service provider engagement agreement by whatever named called should be in place to protect Client's interests, risk management needs, and ability to comply with supervisory expectations.

2. The contractual/agreement terms between Client and the LLP shall include the provisions for third party cloud service providers details and their terms of engagement in brief so as to ensure the similar cyber security and IT Security as provided by the LLP. The agreement may include provisions for audit and information access rights to the Client as well as the regulator for the purpose of performing due diligence and carrying out supervisory reviews.

3. The agreement should also provide Client the right to intervene with appropriate measures to meet legal and regulatory obligations.

4. The LLP shall be responsible for conducting VAPT of the services/components managed by the CSP.

5. The Client may take into consideration the report/certificate of the audit of the CSP. However, wherever required, CSP has to conduct additional audits fulfil all the requirements provided in various applicable circulars/ regulations issued by SEBI, and the same shall be ensured by the RE.

6. The Client shall ensure that appropriate clauses/ terms (including SLA clauses) are added in the agreement (signed between RE and CSP) to enforce the above-mentioned audit/ VAPT requirements.

7. Contract/Agreement should have adequate provisions regarding the termination of contract with the LLP, and appropriate exit strategies to ensure smooth exit without hindering any legal, regulatory or technical obligations of the Client.
8. As part of exit strategy, a clear expunging clause shall be defined in agreement, which shall state that whenever the Client intends to expunge the data, the LLP shall securely and permanently erase the Client's data in disks, backup devices, logs, etc. and no data shall remain in recoverable form. However, it is the responsibility of the LLP to ensure that the minimum retention requirements for data (including logs) as prescribed by the regulator of India or the host country government are met and that the required data, logs, etc. are archived, even if the Client moves out of the cloud/ changes CSPs.

9. The LLP shall ensure that their data (including but not limited to logs, business data, etc.) is stored in an easily accessible, legible and usable manner (during utilization of cloud services and after exit from the cloud) and it shall be provided to SEBI/ any other government agency whenever required.

10. The Contract or Agreement shall include the terms and clauses as required under applicable regulations and laws of India or the host Country.

11. Data Ownership and Localization

The LLP is only a data processing unit for the Client, and it does not owns or controls the data of the Client. In order to ensure that the Client and regulatory right to access LLP's data as well as the regulator's rights of search and seizure are not affected by adoption of cloud services, the storage/ processing of data (DC, DR, near DR etc.) including logs and any other data/ information pertaining to Client in any form in cloud shall be done as per the following conditions:

1. The data should reside/be processed within the legal boundaries of India in case of Indian Clients.

2. However, for the investors whose country of incorporation is outside India, the LLP or the CSP engaged by the LLP shall keep the original data/ transactions/ logs, available and easily accessible in legible and usable form, within the legal boundaries of India.

12. Compliance and Risk Management

The LLP has developed this Policy basis LLP's and it's requirements in general. Key Risk Indicators and performance metrics are reported to internal stakeholders and Clients on a regular basis.

i. **Compliance**: The LLP model/strategy for cloud computing and information technology infrastructure in place. The model/ strategy includes: Details of cloud adoption such as cloud service models, deployment models etc.: The administrator uses Advent Geneva named software for Fund Accounting Services and similarly it uses the and World-Investor Software for storage of information of the investors of the Funds Administered and store the basic data of investors to maintain the investors registry of the Funds. The above are all deployed on a Private Cloud which are considered on premise deployment. There are other PaaS and SaaS software used for internal data and processing and storage like Microsoft 365 and other cloud-based software. For the servicing of Clients these software are the key components and their usage by the employees and concerned persons for the processing of information is the key implementation and operational part of the Client Servicing functions.

ii. **Cloud Risk Management**: There is a paradigm shift in the manner of how cloud technology and is built and managed in comparison with traditional on– premise infrastructure. Therefore, a comprehensive risk management should be undertaken by the LLP under this Policy to continually identify, monitor, and mitigate the risks posed by cloud computing.

The risk assessment shall include (but not limited to) standards like identifying threat sources and events, identifying vulnerabilities and pre-disposing conditions, control analysis, magnitude of impact, etc.

iii. **Compliance and Legal Aspects**: The policies, processes, etc. in place to ensure compliance with the applicable legal and regulatory requirements (including but not limited to guidelines, circulars, advisories, etc.) for deployments in cloud, issued by SEBI/ Government of India/ respective state government.

Assessment, at least on an annual basis, to review the financial and operational condition of the CSP in order to assess its ability to continue to meet the various requirements such as legal, business, compliance, etc. and highlighting any deterioration or breach in performance standards, confidentiality and security, and in business continuity preparedness to the board in a timely manner.

iv. **Risk associated with People:**

- Role of Human Resource:

i. Identification of potential skill gaps which emerge as a result of transition to cloud computing.

ii. Capacity building within organization to build adequate skill sets to manage cloud deployments effectively.

- Role of IT team: The IT team shall be responsible for managing day to day operations and assisting senior management in achieving the objectives of cloud deployments.

v. **Country Risk**

The engagement with a CSP having country of incorporation/registration outside of India, exposes the LLP or its Clients to country risk. To manage such risk, wherever applicable, the LLP shall closely monitor the CSP's country's government policies and its political, social, economic and legal conditions on a

continuous basis, and establish sound procedures for mitigating the country risk. This includes, inter alia, having appropriate contingency and exit strategies. In principle, arrangements shall only be entered into with parties operating in jurisdictions generally upholding confidentiality clauses and agreements. The governing law of the arrangement shall also be clearly specified.

Compliance with the provisions of IT Act, India and other applicable legal requirements and standards to protect the Client's (RE) data has been ensured by the LLP. However, the LLP has no liability to ensure the Compliance requirements of the Client. The LLP shall assist client in fulfilling all of their applicable regulatory requirements required to be fulfilled by the LLP as a service provider.

vi. **Third Party Risk Assessment**: All third-party service providers and vendors are assessed for compliance with Llp's policies and procedures whilst top tier management is also assessed against the applicable regulatory framework on an annual basis for an indication of their security risk and posture.

Users failing to comply with the requirements of this Policy, and/or otherwise misuse and/or abuse Company's internet access may be liable to disciplinary action up to and including dismissal. The Llp shall treat any breach of this policy in a serious manner. Users may be personally liable for any consequences of any conduct and/or action(s) deemed to be illegal. All employees are expected to immediately report any breaches of this Policy, to the respective Manager, either in person or in writing.

Additionally, the Company shall also assess the performance of the CSP, adequacy of the risk management practices adopted by the CSP, compliance with laws/regulations etc.

vii. **Awareness Training:** Upon hire and annually all staff must complete annual security awareness training, along with further focused security training on topical subjects like phishing or payment fraud. In addition, internal phishing campaigns and attack simulations are run on a scheduled basis.

13. Reliance On Third Party Cloud Service Providers

- All third-party service providers and vendors are assessed for compliance with this Policy and procedures whilst top tier management are also assessed against this framework on an annual basis for an indication of their security risk and posture.
- The requirements to be fulfilled by the Company for being appointed as the service provider will apply as such to other third parties more specifically to the Cloud Service Providers engaged by the Company.
- In addition to above if any regulatory requirement is applicable to the Cloud Service Providers (CSPs) engaged by the Company the Company shall ensure that such regulatory requirements are compiled by the CSP at the time of appointment and at all times post appointment.

14. Business Continuity Planning (BCP), Disaster Recovery & Cyber Resilience

- Local Back up of all the cloud data shall be maintained on daily basis by the Company on local server.
- Anti-Virus and Firewalls to be installed and be updated and running at all points of time.
- All the risk assessment and risk mitigation measures under this policy shall be ensured at all times.

- Business continuity management starts with planning how to maintain critical functions (e.g., IT, sales and support) during and after a disruption.
- A business continuity plan (BCP) comprises the following elements

1. **Threat Analysis**

   The identification of potential disruptions, along with potential damage they can cause to affected resources. Examples include:

Threat	Potential impact
Power outage	Inability to access servers
Natural disaster	Critical infrastructure damage
Illness	Widespread employee absences
Cyberattack	Data theft and network downtime
Vendor error	Inability to execute integrated business functions

2. **Role assignment**

   To ensure that there is well-defined chain of command and substitute plan to deal with absence of staff in a crisis scenario the employees are cross-trained on their responsibilities so as to be able to fill in for one another. Internal departments (e.g., Operations, IT, Fund Accounting) are broken down into teams based on their skills and responsibilities. Team leaders assigns roles and duties to individuals according to the organization's threat analysis ensuring that each task has more than one back up person with complete knowledge of the working of the department.

3. **Communications:**

   A communications strategy details how information is disseminated immediately following and during a disruptive event, as well as after it has been resolved.
   The strategy of the organization is as follows:

- Methods of communication – In case of emergency phone calls to internal team members may be done however a follow up email of the discussions and decisions taken shall be done by the IT employee for the purpose of records and for regulatory purposes.
- Established points of contact responsible for communicating with employees: In case of matters related to employee absence the HR team to be contacted. Email communication is the most preferable means of communication however in case mails are not accessible or any major issue the incident to be raised by team and team leads to be reported through phone within 15 minutes of non-functioning of the systems or the power failure. The Manager of teams shall be reported by team lead and the Manager in turn will take immediate action of arranging power backup and or measures for system recovery with system vendor ad the IT team member by sending requisite mails and making necessary calls. The maximum time to be taken for recovery of systems or power is within two hours of the time notifying the same to the manager.
- Means of contacting employee family members, media, government regulators, etc.

4. **Backups**

   From electrical power to communications and data, every critical business component must have an adequate backup plan that includes:

- The data backups are be stored in different locations. This prevents the destruction of both the original and backup copies at the same time. If necessary, offline copies should be kept as well.
- Backup power sources, such as generators, inverters and UPS that are provisioned to deal with power outages.
- Backup communications (e.g., mobile phones and text messaging to replace land lines) and backup services (e.g., cloud email services to replace on-premise servers).

5. Load balancing business continuity

- Load balancing maintains business continuity by distributing incoming requests across multiple backend servers in the data center. This provides redundancy in the event of a server failure, ensuring continuous application uptime.

- In contrast to the reactive measures used in failover and disaster recovery (described below) load balancing is a preventative measure. Health monitoring tracks server availability, ensuring accurate load distribution at all times --including during disruptive events.

In accordance with our policy, during disaster recovery testing or in real-time scenarios, dealers may execute trades for locations that are non-functional.

Disaster recovery plan (DCP) – the second line of defense.

- Even the most carefully thought out business continuity plan is never completely fool proof. Despite the best efforts, some disasters simply cannot be mitigated. A disaster recovery plan (DCP) is a second line of defense that enables the Company to bounce back from the worst disruptions with minimal damage.
- As the name implies, a disaster recovery plan deals with the restoration of operations after a major disruption. It's defined by two factors: RTO and RPO.
- **Recovery time objective (RTO) –** The acceptable downtime for critical functions and components, i.e., the maximum time it should take to restore services. A different RTO should be assigned to each of the business components according to their importance (e.g., ten minutes for network servers, an hour for phone systems).
- The Critical Functions like Fund Accounting and Fund Operations will have RTO one hour (1) hour for network and servers and operations systems.
- Other functions or Client On-Boarding Screening and Data Management can have a two (2) hour to restore the operations of the system.
- Mails and mail recovery time will be one (1) hour to restore the mailing downtime except for matters where the service provider notifies any other timeline which in any case will not exceed three hours. In case where more than three hours are required the mailing facility will be shifted to alternate servers.
- **Recovery point objective (RPO) –** The point to which the state of operations must be restored following a disruption. In relation to backup data, this is the oldest age and level of staleness it can have. The network servers updated hourly should have a maximum RPO of 59 minutes to avoid data loss.
- Deciding on specific RTOs and RPOs helps clearly show the technical solutions needed to achieve the recovery goals. In most cases the decision is going to boil down to choosing the right failover solution.

  Choosing the right failover solutions:

- Failover is the switching between primary and backup systems in the event of failure, outage or downtime. It's the key component of our disaster recovery and business continuity plans.

- A failover system should address both RTO and RPO goals by keeping backup infrastructure and data at the ready. Ideally, the failover solution should seamlessly kick in to insulate end users from any service degradation.
- When choosing a solution, the two most important aspects to consider are its technological prowess and its service level agreement (SLA). The latter is often a reflection of the former.
- For an IT organization charged with the business continuity of a website or web application, there are three failover options:

  Hardware solutions – A separate set of servers, set up and maintained internally, are kept on-premise to come online in the event of failure. However, note that keeping such servers at the same location makes them potentially susceptible to being taken down by the same disaster/disturbance. Accordingly, the same shall be maintained at a separate location as may be decided by the management.

  DNS services – DNS services are often used in conjunction with hardware solutions to redirect traffic to a backup server(s) at an external data center. A downside of this setup includes TTL-related delays that can prevent seamless disaster recovery. Additionally, managing both DNS and internal data center hardware failover solutions is time consuming and complicated.

  On-edge services – On-edge failover is a managed solution operating from off- prem (e.g., from the CDN layer). Such solutions are more affordable and, most importantly, have no TTL reliance, resulting in near-instant failover that allows to meet the most aggressive RTO goals.

15. Vulnerability Assessment and Penetration Testing (VAPT)/Audit of the Informational Technology Infrastructure

The VAPT activity undertaken by the Company/LLP should cover the infrastructure and applications/services hosted or managed by the Company on cloud. The VAPT tactics, tools and procedures should be fine-tuned to test and assess the cloud native risks and vulnerabilities. VAPT should also be conducted before commissioning of any new system. Additionally, the VAPT activity shall be conducted as per the requirements (including scope, classification, duration for closure of vulnerabilities, etc.) provided in applicable circulars/ regulations issued by regulators.