Business Continuity Plan

Version 1

Document Control	
Title	**Business Continuity Plan**
Policy Owner	Compliance Department
Preparer and Reviewer	Compliance Officer
Approved by	Designated Partners
Version	V1
Tentative next review	On any Regulatory change or Annual, whichever is earlier

Version Summary

Version	**Policy**	**Reviewed Date**	**Department**	**Approved by**
V1	Business Continuity Plan	25.04.2025	Compliance	Designated Partners

Contents

1. TITLE/OBJECTIVE ____ 3
2. REGULATORY BACKGROUND ____ 3
3. APPLICABILITY ____ 3
4. IMPLEMENTATION / PROCESS ____ 3
   - 4.1 Critical Business Function; ____ 3
   - 4.2 List of Important Documents record ____ 4
   - 4.3 Risk Scenarios & Responses ____ 4
   - 4.4 Data backup and recovery ____ 5
   - 4.5 Client Communication and Vendor Co-ordination ____ 5
5. POLICY REVIEW ____ 5
6. RESPONSIBILITY ____ 5
7. POWER TO REMOVE DIFFICULTIES ____ 6
8. EFFECTIVE DATE ____ 6

1. Title/Objective

The objective of this Business Continuity Plan is to ensure that a registered Fund Management Entity (FME) has comprehensive procedures in place to address emergencies or significant business disruptions. It aims to maintain operational resilience and minimize the impact of disruptions on the FME's operations. The goal is to protect client interests, maintain compliance with regulatory requirements, and minimize operational downtime.

2. Regulatory Background

This Business Continuity Plan requirement is outlined in Regulation 121 of International Financial Services Centre Authority (Fund Management) Regulations, 2025 for registered FMEs. It mandates the establishment and maintenance of a plan to address emergencies and disruptions, ensuring the FME's ability to continue essential operations.

3. Applicability

This Business Continuity Plan applies to registered FMEs, and it covers procedures and protocols for handling emergencies or significant business disruptions**.** It encompasses various scenarios that may impact operations, such as natural disasters, technology failures, or other unforeseen events.

4. Implementation / Process

This plan establishes procedures and processes to maintain operational continuity for businesses based on three types of disruptions that could occur individually or in any combination:

- Loss of access to parts of or the entire facility (e.g., following a fire, sudden storm, or flooding);
- Loss of services due to a reduction in workforce (e.g., during pandemic Covid);
- Loss of services due to equipment or systems failure (e.g., information technology (IT) systems failure, electrical grid failure)

4.1 Critical Business Function;

Following are Critical business function to identify and make business continuity plan.

Function	**Recovery Time Objective (RTO)**	**Alternate Process**
Investment Decision-Making	1 Business Day	Temporarily halted until system access restored
Trade Execution	1 Business Day	Manual execution via broker assistance
NAV Calculation/Reporting	2 Business days	Coordination with fund administrator
Client Communications and Vendor co-ordination	Same Day	Alternate email/phone systems
Regulatory Filings	Within prescribed timeline	Extensions requested if necessary

4.2 List of Important Documents record

Important record as per IFSCA (FME) Regulation are as below;

- a copy of profit and loss account for each accounting period;
- a copy of the auditor‘s report on the accounts for each accounting period;
- a statement of net worth for each quarter;
- documents relating to compliance with AML and CFT guidelines;
- documents relating to account opening of each client and any power of attorney or signature authority forms of the clients;
- relevant records and documents relating to its activities under these regulations; and
- such other books of accounts, records and documents as may be specified by the Authority from time to time.
- The FME shall be required to maintain following records describing:
- the assets under each scheme;
- valuation policies and practices;
- investment strategies;
- particulars of investors and their contribution;
- rationale for investments made.

4.3 Risk Scenarios & Responses

a. Technology or System failure

In the event of a technology or system failure, such as a malfunction in the portfolio management system or connectivity issues affecting access to investment platforms, the Investment Manager has established protocols to ensure minimal disruption. The team uses secure, cloud-based platforms with automatic daily backups and system redundancy to mitigate such risks. In case of a disruption, employees will access systems via secure connections from remote locations. Essential functions such as trade execution and client reporting can be continued through manual processes or direct coordination with service providers and brokers until full system restoration is achieved.

b. Office Inaccessibility

Whenever primary office premises become inaccessible due to a natural disaster, public emergency, or government-imposed lockdown, the team will transition to a remote working environment. All employees are equipped with necessary hardware and secure internet access to perform their duties from home. Communication among team members and with clients will be maintained through encrypted email services, video conferencing tools, and dedicated mobile channels. Since core applications and files are cloud-hosted, access to critical data and systems remains uninterrupted.

c. Key Personnel Unavailability

In the unlikely event of the unavailability of key personnel, such as due to illness, accident, or other emergencies, the Investment Manager has ensured that roles and responsibilities are clearly documented and accessible to all team members. This documentation enables another employee or an authorized external consultant to temporarily assume the required functions. For example, if the Principal Officer is unavailable, the Compliance Officer or a pre-designated senior advisor may step in to ensure continuity of critical operations and regulatory responsibilities

d. Cybersecurity Incident

All cybersecurity functions are centrally managed by the parent entity in Mumbai (i.e. Trust Investment Advisors Private Limited). In the event of a cyber-breach or data compromise, the IT team will immediately take charge of isolating affected systems, restoring data from secure backups, and investigating the incident. Robust preventive measures—including endpoint protection, system updates, and employee awareness are maintained at a group level to ensure security across locations.

4.4 Data backup and recovery

The Investment Manager relies on secure, cloud-based systems such as One Drive (i.e. Secure drive provided by Microsoft) for data storage and accessibility. All critical business and client data including client records, fund documentation, investment reports, and compliance files are backed up periodically with secure version history maintained to enable quick restoration if needed. These backups are encrypted and stored in geographically redundant locations to ensure data integrity and availability in the event of a system failure or cyber incident. Regular monitoring and periodic testing are conducted to verify the effectiveness of the backup and recovery process**.**

4.5 Client Communication and Vendor Co-ordination

In the event of any significant disruption affecting client assets or reporting, the Investment Manager ensures timely communication with clients, primarily through email and mobile contact, and secondarily via website updates or SMS alerts. Clients are informed within 24 hours of any material impact. Additionally, key third-party service provider including the fund administrator, custodian, auditor, and legal counsel are integrated into the Business Continuity Plan. Regular coordination is maintained with these vendors to ensure alignment of contingency measures and seamless operational support during disruptions.

5. Policy Review

The FME will conduct a comprehensive annual review of its business continuity plan to assess its adequacy and effectiveness in addressing emergencies and significant business disruptions.

6. Responsibility

The Senior management or Designated official will be responsible for implementation of Policy.

7. Power to Remove Difficulties

In the event of any difficulties or ambiguities arising during the implementation of this plan, the Designated Partners are empowered to provide necessary clarifications or make amendments as deemed necessary, ensuring the smooth and effective enforcement of the code.

8. Effective Date

This policy shall be effective from immediately upon approval by the Designated Partners of LLP.