BUSINESS CONTINUITY MANAGEMENT (BCM) POLICY

Entity: Ternary Fund Management Pte. Ltd. ("The Company") **Applicable Products:**

1. **IMP Emerging Equity Trends (UCITS)**
2. **All other UCITS strategies managed by the Company Version:** 1.1
3. **Effective Date:** 14/01/2026

1. Objective and Scope

The objective of this Business Continuity Management (BCM) Policy is to ensure that Ternary Fund Management (the "Manager") can continue to perform its Critical Business Services (CBS) and fulfill its fiduciary duties to the UCITS Fund and its investors in the event of a significant operational disruption.

This policy applies to all employees, systems, and third-party service providers integral to the management of the Fund. Given the Company's cloud-native infrastructure, this BCP focuses on **operational resilience** and **location independence** rather than physical site redundancy.

2. Regulatory Framework

This policy is established in accordance with:

- **MAS Guidelines on Business Continuity Management (June 2022):** Requiring identification of Critical Business Services, setting Service Recovery Time Objectives (SRTO), and dependency mapping.
- **UCITS Directive (2009/65/EC) & ESMA Guidelines:** Requiring adequate internal control mechanisms and resilient systems to mitigate operational risk.

3. Business Continuity Strategy: Cloud-First Resilience

The Company adopts a **Decentralized Operational Model**. All core systems required for portfolio management, risk monitoring, and trade execution are hosted on cloud-based infrastructure (SaaS/IaaS).

Policy Statement:

*"In the event of the inaccessibility of the Company's primary office, the primary Business Continuity Strategy is **Remote Work Area Recovery**. All staff are authorized and equipped to execute Critical Business Services from secure remote locations (including home offices) using company-issued devices or approved BYOD protocols via secure cloud access."*

3.1 Core System Redundancy

Function	System/Platform	Resilience Strategy
Portfolio Management (PMS)	[INFIN]	SaaS-based; accessible via internet with 2FA.
Email & Files	[Google Workspace / Microsoft Azure]	Cloud-hosted with geo-redundancy by provider.
Trade Execution	[FTP, Excel]	Web-based access or mobile app backup.
Fund Admin/Transfer Agency	[Credit Agricole – Indosuez - OLIS]	Web-portal access (External Dependency).

4. Critical Business Services (CBS) & Recovery Objectives

In alignment with MAS Guidelines, the Manager has identified the following Critical Business Services. The **Service Recovery Time Objective (SRTO)** indicates the maximum acceptable downtime.

Critical Business Service	SRTO	Recovery Priority
Portfolio Management & Trading	4 Hours	**High** (Market Risk Impact)
NAV Calculation & Pricing	24 Hours	**Medium** (Regulatory Impact)
Cash Management / Collateral	4 Hours	**High** (Liquidity Impact)
Investor Communication	24 Hours	**Low** (Reputational Impact)

5. Crisis Management Structure

A Crisis Management Team (CMT) is established to declare a disaster and trigger the BCP.

- **Gold Team (Decision Makers):** CIO, Portfolio Manager (Authorized to declare BCP activation).
- **Silver Team (Execution):** Head of Trading, Head of Operations (Execute recovery procedures).

Activation Criteria: The BCP is activated immediately upon confirmation of:

1. Physical inaccessibility of the office (Fire, Pandemic, Civil Unrest).
2. Cybersecurity incident rendering local networks unsafe.
3. Loss of key personnel.

6. Incident Response Scenarios

Scenario A: Loss of Physical Access (Office Unavailability)

- **Response:** Immediate transition to Remote Work strategy.
- **Action:** Staff relocate to home/remote locations. Confirm internet connectivity. Log in to Cloud Systems via VPN/2FA.
- **Dependencies:** Residential internet availability; Cloud Provider uptime (AWS/Azure).

Scenario B: Cloud Service Provider Failure (e.g., Bloomberg/Microsoft Down)

- **Response:** Dependency Failover.
- **Action:**
    - *Trading:* Use backup brokers (excel execution).
    - *Data:* Access offline backups of critical positions/NAV (saved daily at INFIN in France).
    - **Note:** As a UCITS manager, if a system failure prevents accurate NAV calculation, the Manager may suspend dealing in consultation with the Fund Administrator and Depositary.

Scenario C: Cyber Attack / Ransomware

- **Response:** Isolation and Restoration.
- **Action:** Disconnect affected devices from the cloud network. Trigger incident response plan with IT Support. Restore data from immutable cloud backups (Snapshot recovery).

7. Third-Party Dependency Management

The Manager acknowledges that Critical Business Services (e.g., Fund Administration, Custody) are outsourced.

- **Oversight:** The Manager shall review the BCP of key service providers (Fund Administrator, Prime Brokers) annually to ensure they can meet the Fund's SRTOs.
- **Contact List:** Digital copy of the **Critical Contact List** (Depositary, Administrator, Legal, MAS, Regulator) is maintained by the CIO.

8. Testing and Audit

- **Annual Testing:** The Company will conduct a BCP test at least once every 12 months.
- **Remote Work Test:** Given the cloud model, a mandatory "Full Remote Working Day" for all staff will serve as the functional BCP test.
- **Audit:** Internal or external auditors will review the BCP testing logs and policy effectiveness every year.

Approved by the Board of Directors

Date: _____

Signature: _____