Contingency Operations Playbook (COP)

Business Continuity & Disaster Recovery Procedures

> **CONFIDENTIALITY NOTICE**
>
> This document contains detailed operational continuity procedures and system architecture. Unauthorized access could compromise business resilience capabilities.

1. Objective

To ensure uninterrupted delivery of essential banking functions during adverse events through tested operational redundancies.

2. Business Continuity Plan (BCP)

- **Primary Site: Bangkok HQ**
- **Secondary Site: Singapore**
- **Disaster Recovery Data Center: Frankfurt**
- **Recovery Time Objective (RTO): 15 minutes**
- **Recovery Point Objective (RPO): 5 minutes**

3. Continuity Activation

- Triggered automatically by the COO or CMC
- All critical systems fail over to alternate data centers
- Staff relocated to designated BCP sites or remote operations network
- Customer notification via SMS, email, and website banner within 2 hours

4. Operational Priorities

Priority	Function	Objective
1	Payments & Core Banking	Maintain financial stability
2	Treasury Operations	Preserve liquidity and FX exposure
3	Risk & Compliance	Continue AML and reporting functions
4	Customer Service	Maintain client communication

5. Testing & Drills

- Semi-annual simulation exercises involving all departments
- Annual audit by independent BCP assessor
- Post-test evaluations and continuous updates
- Tabletop exercises quarterly for executive leadership
- Unannounced drills twice annually to test readiness

6. Vendor & Partner Continuity

- All third-party vendors must maintain ISO 22301-certified continuity programs
- SLAs include mandatory disaster recovery clauses
- Annual vendor BCP audits and certification reviews
- Backup vendors identified for all critical services

7. Documentation & Review

All crisis and BCP documentation updated annually or post-incident. Reviewed by the Board Risk & Audit Committee. Version control maintained with full audit trail of all changes.

Emergency Contact Protocol

All CMC members maintain 24/7 availability via redundant communication channels: primary mobile, backup mobile, satellite phone, and encrypted messaging app. Contact tree tested monthly.