Business Continuity Plan Summary

Version 2.0 - January 2025

Classification: INTERNAL

1. Purpose and Scope

This Business Continuity Plan (BCP) outlines the procedures to maintain essential business functions during and after a disruptive event. Events covered include: natural disasters, cyber attacks, pandemic, loss of key personnel, supplier failure, and infrastructure failure.

The BCP covers all business units and functions. Critical business functions have been identified through a Business Impact Analysis (BIA) and are listed in Appendix A. Each critical function has a documented Maximum Tolerable Downtime (MTD) and recovery procedures.

The BCP is maintained by the Business Continuity Manager and reviewed by the Crisis Management Team quarterly. Full plan testing (tabletop exercise or live test) is conducted annually.

2. Crisis Management Team

The Crisis Management Team (CMT) consists of: Chief Executive (Chair), Chief Operating Officer, Chief Information Security Officer, Head of Communications, Head of HR, Head of Facilities, and the Business Continuity Manager (Secretary).

The CMT is activated when a disruptive event exceeds the capacity of normal operational management. Activation is triggered by the COO or, in their absence, the most senior available member of the CMT.

The CMT operates from the primary Crisis Management Room (Building A, Room G-01). If the primary location is unavailable, the secondary location (Building B, Room 2-15) is used. If neither is available, the CMT convenes virtually using the emergency Teams channel.

CMT decisions are documented in real-time by the Secretary using the Crisis Log template. Post-incident, the Crisis Log forms the basis of the post-incident review report.

3. Communication Procedures

Internal communication during a crisis is managed through the Mass Notification System (MNS). All employees must ensure their contact details (mobile phone, personal email) are up to date in the HRIS.

The MNS sends simultaneous notifications via SMS, email, and push notification. Test messages are sent quarterly to verify system functionality and contact data accuracy.

External communication during a crisis is managed exclusively by the Head of Communications. No other employee is authorised to make statements to media, regulators, or external stakeholders without explicit approval from the CMT.

Customer and partner notifications follow the Communication Protocol (BCP-003), which specifies templates, approval chains, and timing requirements for different incident categories.

Social media monitoring is intensified during crisis events. The Communications team monitors all major platforms and responds to queries/misinformation in accordance with the approved messaging framework.

4. IT Disaster Recovery

IT disaster recovery procedures are documented separately in the IT DR Plan (ITDR-001). The following provides a summary of key recovery objectives.

Recovery priorities are categorised as: Tier 1 -- restore within 4 hours (email, authentication, VPN, core business applications), Tier 2 -- restore within 24 hours (HRIS, financial systems, document management), Tier 3 -- restore within 72 hours (development environments, training systems, analytics platforms).

All Tier 1 systems operate in active-active or active-passive high-availability configurations across two geographically separated data centres. Tier 2 and 3 systems are recovered from daily backups.

Backup strategy: Tier 1 systems -- continuous replication with 15-minute RPO; Tier 2 systems -- 4-hourly snapshots with 4-hour RPO; Tier 3 systems -- daily backups with 24-hour RPO.

DR failover testing is conducted semi-annually. Each test involves a full failover of at least two Tier 1 systems to the secondary data centre, with success criteria including: successful failover within RTO, data integrity verification, and user acceptance testing.

Cyber-specific recovery procedures include: network isolation of affected segments, forensic preservation of evidence, clean restoration from known-good backups, and progressive reconnection with continuous monitoring.

5. Business Recovery Procedures

Each department maintains a Department Recovery Plan (DRP) that details how critical functions will be maintained during a disruption. DRPs must be reviewed and updated at least annually.

Work relocation options include: remote working (for disruptions affecting office premises), relocation to the backup office site (Building C, available at 24 hours notice with capacity for 150 staff), and buddy arrangements with named partner organisations.

Staff welfare during a crisis is coordinated by HR. This includes: regular communication updates, access to the Employee Assistance Programme (EAP), flexible working arrangements, and additional leave provisions where appropriate.

Supply chain continuity is managed by the Procurement team. Critical suppliers have been identified through the BIA and are subject to annual business continuity assessments. Alternative suppliers are pre-qualified for all single-source dependencies.

Financial provisions for crisis response, including emergency expenditure authorisation limits, are documented in the Finance appendix to this plan. The CFO has delegated authority for emergency spending up to 500,000 GBP without board approval.

6. Plan Testing and Maintenance

The BCP testing programme includes: quarterly tabletop exercises (scenario-based discussions), annual simulation exercises (partial activation of recovery procedures), and biennial full-scale tests (complete plan activation).

Testing results are documented in the Test Report template (BCP-005), including: scenario description, participants, actions taken, issues identified, and improvement recommendations.

Identified improvements are tracked in the BCP Improvement Register and assigned to responsible owners with target completion dates. Progress is reported to the CMT quarterly.

All employees must be aware of their roles and responsibilities under the BCP. Annual business continuity awareness is included in the mandatory security awareness training programme.

Department heads are responsible for maintaining their DRP, participating in testing exercises, and ensuring their teams are trained in recovery procedures. DRP compliance is included in the annual departmental audit.