Business Continuity and Disaster Recovery Policy

Introduction

This policy applies equally across all Supreme Group businesses (hereafter, “the Company”).

1. Scope

The Company is committed to maintaining the continuity of its business operations and ensuring the safety and wellbeing of its employees in the face of potential disruptions. This Business Continuity and Disaster Recovery (BCP/DR) Policy outlines our approach to managing both localised and widespread crises, considering our remote operations and flexible working conditions.

This policy applies to all Company employees. It covers both localised disruptions affecting individual employees or teams, and widespread crises that may impact our entire organisation or multiple regions simultaneously.

2. Objectives

- Ensure the safety and wellbeing of all Company personnel
- Maintain critical business functions during and after a disruptive event
- Protect the Company’s data, assets, and reputation
- Comply with legal, regulatory, and contractual obligations
- Minimise financial losses and business disruptions

3. Risk Assessment and Business Impact Analysis

3.1 The Company will conduct an annual strategic risk assessment to identify potential threats to business continuity, including but not limited to:

- Cybersecurity incidents
- Natural disasters affecting employees' locations
- Infrastructure failures (internet, power, etc.)
- Pandemics or widespread health crises
- Any other not unreasonably foreseeable event or events.

3.2 A business impact analysis will be performed to identify:

- Critical business functions and their recovery time objectives
- Key personnel and their backups
- Essential tools and technologies
- Critical third-party dependencies

4. Business Continuity Strategies

4.1 Remote Work Infrastructure

- Ensure all employees have necessary equipment for remote working
- Maintain redundant cloud-based systems for critical applications

- Provide appropriately secure access for connections to company resources

4.2 Communication

- Establish a crisis communication plan with clear roles and responsibilities
- Maintain up-to-date employee contact information
- Utilise multiple communication channels (email, messaging apps, telephone)

4.3 Data Backup and Recovery

- Implement automated, regular backups of all critical data to cloud storage
- Ensure data is encrypted both in transit and at rest
- Conduct periodic tests of data restoration processes

4.4 Third-Party Risk Management

- Regularly assess the BCP/DR capabilities of critical vendors and partners
- Maintain a list of alternative suppliers for essential services

4.5 Financial Resilience

- Maintain adequate cash reserves or credit lines to manage potential disruptions
- Develop strategies for rapid cost reduction if needed

5. Incident Response Procedures

5.1 Incident Classification

- Level 1: Minor incident affecting an individual or small team
- Level 2: Moderate disruption affecting a significant portion of the organisation
- Level 3: Major crisis affecting the entire organisation or multiple regions

5.2 Incident Response Team

- Establish a cross-functional incident response team with clearly defined roles
- Conduct periodic training and simulations for the response team

5.3 Response and Recovery Steps

5.3.1 Incident detection and reporting
5.3.2 Assessment and classification
5.3.3 Activation of appropriate response plans
5.3.4 Communication to stakeholders
5.3.5 Implementation of continuity strategies
5.3.6 Monitoring and adjustment of response
5.3.7 Recovery and return to normal operations
5.3.8 Post-incident review and lessons learnt

6. Specific Scenario Plans (note, this is a non-exhaustive list)

6.1 Cybersecurity Incident

- Implement immediate containment measures
- Engage cybersecurity experts for incident investigation and resolution
- Notify affected parties as required by law

6.2 Natural Disaster Affecting Employee Locations

- Account for all employees in the affected area
- Provide support for relocation or alternative work arrangements if necessary
- Redistribute workload to unaffected team members

6.3 Widespread Health Crisis (e.g., Pandemic)

- Implement additional health and safety measures for any in-person activities
- Provide mental health support and resources to employees
- Adjust policies to accommodate increased caregiving responsibilities

7. Testing and Maintenance

7.1 Conduct annual tabletop exercises to test the BCP/DR plan

7.2 Perform quarterly tests of critical systems and recovery procedures

7.3 Review and update (as appropriate) the BCP/DR policy annually or after any major organisational changes

8. Roles and Responsibilities

8.1 Executive Leadership

- Overall responsibility for BCP/DR policy approval and resource allocation

8.2 BCP/DR Coordinator

- Maintain and update the BCP/DR policy and procedures
- Coordinate testing, training, and awareness programmes

8.3 Department Heads

- Ensure BCP/DR measures are implemented within their departments
- Identify critical functions and personnel within their areas

8.4 All Employees

- Familiarise themselves with the BCP/DR policy and their roles in it
- Report any potential threats or incidents promptly

9. Policy Review and Approval

This policy will be reviewed annually and updated as necessary. All changes must be approved by the Company's executive leadership.

Document Classification		External	
Document Number	Issue Number	Last Review Date	Next Review Date
SG-003	SG-HR-003	Jan-2026	Jan-2027