

Business Continuity Policy

1. Purpose

This policy establishes the principles, structure, and responsibilities for maintaining and implementing an effective Business Continuity Plan (BCP) across all areas of the organisation. The aim is to ensure the continuity of critical operations during and after disruptive events, protect stakeholders, safeguard assets, and maintain regulatory compliance.

2. Scope

This policy applies to all business units, services, personnel, technologies, and third-party dependencies across all divisions and locations, including:

- Cleanroom Projects (All Cleanrooms, Rapid Cleanrooms, Mobile & Prefabricated Cleanrooms)
- Cleanroom Hardware
- Service and Decontamination Teams
- Technology Infrastructure and Data Assets
- Critical Suppliers and Partners

3. Governance & Oversight

Executive Responsibility

Senior management holds ultimate accountability for business continuity. This includes ensuring:

- Adequate resourcing and funding of the BCP.
- Leadership direction and ongoing engagement.
- Compliance with applicable legal and regulatory requirements.

Business Continuity Steering Committee

A cross-functional committee comprising representatives from each key business unit and, where appropriate, differentiated by company. Responsibilities include:

- Overseeing implementation and effectiveness of the BCP.
- Approving updates and changes.
- Driving continuous improvement.

Business Continuity Manager

A designated individual responsible for:

- Day-to-day management of the BCP.
- Coordinating training and awareness.

- Maintaining documentation and plan updates.

4. Risk Assessment & Business Impact Analysis (BIA)

Risk Identification

The organisation will conduct regular assessments to identify and monitor potential threats, including:

- Cybersecurity incidents
- Supply chain interruptions
- Equipment or system failures
- Health emergencies (e.g., pandemics)
- Natural disasters
- Malicious activities
- Regulatory changes

Business Impact Analysis (BIA)

BIA will be conducted to:

- Identify critical functions and interdependencies.
- Determine Recovery Time Objectives (RTOs) and acceptable downtime for each function.
- Prioritise services based on operational, client, and regulatory impact.

5. Continuity & Recovery Strategies

Service-Specific Plans

Each business area must maintain continuity strategies tailored to their function:

- **All Cleanrooms:** Backup suppliers and alternate sourcing strategies.
- **Rapid Cleanrooms:** Inventory of standardised components and rapid build protocols.
- **Mobile & Prefabricated Cleanrooms:** Off-site manufacturing agreements.
- **Cleanroom Hardware:** Critical component stocking and fast-track supplier arrangements.
- **Service Teams:** Emergency personnel rosters and access to tools and systems.
- **Decontamination Teams:** Certified professionals and equipment for rapid response.

Data & Technology Recovery

- Critical data must be backed up both onsite and offsite.
- Technology recovery strategies must ensure rapid restoration of systems and records.

6. Emergency Response & Communication Plan

Immediate Response

Upon detecting a disruptive event:

- The BCP is activated.
- Stakeholders are notified.
- Incident management teams are deployed per service area.
- Evacuation and employee safety procedures are followed as needed.

Communication Protocols

- **Internal:** Clear communication of roles, updates, and operational changes to all employees.
- **External:** Transparent client updates regarding impacts and service alternatives.
- **Stakeholders:** Regular updates to directors, regulators, and key partners.

7. Critical Resources & Personnel Management

Key Personnel

Identify essential roles and ensure training in emergency response and continuity procedures.

Personnel Availability

Enable flexible working arrangements (e.g., remote work) and cross-training to reduce dependency on single individuals.

Resource Prioritisation

Allocate critical materials, financial resources, and personnel to the most essential functions during disruptions.

8. Recovery & Restoration

Recovery Objectives

Each function will have defined:

- **RTO (Recovery Time Objective):** Maximum tolerable downtime.
- **RPO (Recovery Point Objective):** Maximum data loss threshold.

Restoration Process

- Documented restoration procedures for each business line.
- Prioritise restoration based on regulatory, client, and health/safety impacts.

9. Training, Testing & Drills

Training Programs

Ongoing training for all staff on the BCP, with role-specific responsibilities highlighted.

Tabletop Exercises

Simulated scenarios to evaluate team responses and refine plans.

System Testing

Regular testing of:

- Backup systems
- Cleanroom operational continuity measures
- Critical IT infrastructure

10. Maintenance & Review

Annual Review

The BCP must be reviewed:

- Annually, at a minimum.
- Following any significant operational or structural change.
- After any actual disruptive event.

Audit & Compliance

Periodic internal and/or third-party audits will verify:

- Compliance with regulatory requirements.
- Alignment with held or targeted industry standards (e.g., ISO 22301, ISO 9001, GMP).

11. Continuous Improvement

Feedback Mechanisms

Collect and integrate feedback from:

- Employees

- Clients
- Partners and vendors

Post-Incident Reviews

Thorough review after each disruption to:

- Identify lessons learned
- Improve policies and procedures
- Update documentation accordingly

12. Enforcement & Non-Compliance

Failure to adhere to this policy may result in disciplinary action and increased operational risk. All employees and contractors are expected to understand and comply with their responsibilities as outlined.

Signed: 

Date: 01/09/25

Name: Raymond Wheeler

Position: Founder

