BUSSINESS CONTINUITY PLAN

TABLE OF CONTENTS

Clause 1: Scope and Applicability

1.1 This Business Continuity Plan ("BCP" or "the Plan") applies to all operations of Urathon Europe Ltd (“the company”) including staff, contractors, suppliers, technology platforms, and external partners, across its UK and international footprint.

1.2 The Plan is mandatory for all departments and applies to disruptions affecting the supply of critical products and services, particularly in regulated sectors such as healthcare, medical devices, and NHS contracts.

1.3 This Plan aligns with the principles of the **ISO 22301:2019** Business Continuity Management standard and the UK **Civil Contingencies Act 2004**.

Clause 2: Definitions

2.1 **Business Continuity**: The ability of the organisation to maintain essential functions during and after a crisis or disruption.

2.2 **Disaster Recovery**: IT- and data-specific procedures for restoring critical digital infrastructure.

2.3 **Critical Operations**: Business activities whose interruption may compromise patient safety, data integrity, legal compliance, or stakeholder confidence.

Clause 3: Risk Assessment and Business Impact Analysis

3.1 Annual risk assessments shall be undertaken to identify threats such as cyberattacks, system failures, pandemics, extreme weather events, and supplier insolvency.

3.2 Business Impact Analysis (BIA) will determine Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for all mission-critical functions.

3.3 Risks shall be mapped by severity and likelihood, with scenario planning for high-impact events (e.g. data breach, product recall, supply failure).

3.4 The Board’s Risk Committee will oversee and update the Risk Register quarterly.

Clause 4: Data Protection and IT Infrastructure Recovery

4.1 All digital infrastructure must comply with **UK GDPR** and **Data Protection Act 2018**, including regular encrypted backups and dual-location redundancy.

4.2 IT systems shall be restored within 24–72 hours post-incident, depending on impact classification.

4.3 Biannual stress testing of systems will verify cybersecurity resilience and disaster recovery capabilities.

4.4 All incidents must be reported under the Company's Data Breach Response Plan and, where applicable, to the **ICO** within 72 hours.

Clause 5: Supply Chain Resilience

5.1 Supplier continuity plans are mandatory, particularly for high-risk products like CGMs and wheelchairs.

5.2 Contracts must contain robust **Force Majeure**, audit access, and recovery provisions.

5.3 A 90-day minimum inventory buffer shall be maintained for critical stock-keeping units (SKUs).

Clause 6: Power and Infrastructure

6.1 Key sites must be equipped with uninterruptible power supplies (UPS) and tested backup generators.

6.2 All facilities must meet standards for fire safety, HVAC, telecommunications redundancy, and accessibility (per **Equality Act 2010** and **BS 8300**).

Clause 7: Communication Plan

7.1 A pre-defined communication protocol shall be activated during a disruption, including stakeholder trees, external messaging templates, and crisis hotlines.

7.2 All communication systems must be backed up and diversified (email, SMS, VOIP) to ensure delivery continuity.

7.3 Senior management must receive crisis communication training annually.

Clause 8: Training and Awareness

8.1 Mandatory BCP training will be delivered to all staff annually, with scenario-specific simulation exercises conducted at least once per year.

8.2 Role-specific responsibilities shall be communicated and documented with signed acknowledgment.

8.3 Records of training completion will be retained for audit and regulatory review.

Clause 9: Insurance Coverage

9.1 The Company must maintain adequate policies for:

- Business Interruption
- Product Liability
- Cyber Risk
- Public Liability
- Employer's Liability (as per the **Employers' Liability (Compulsory Insurance) Act 1969**)

9.2 Insurance levels and coverage terms will be reviewed annually in collaboration with legal and finance.

Clause 10: Testing and Review

10.1 The BCP shall be tested via tabletop exercises, red team simulations, and technical failover testing at least once annually.

10.2 Findings from post-mortem evaluations must result in corrective actions.

10.3 The Plan shall be updated immediately following material changes in law, services, or company structure.

Clause 11: Specialized Equipment (Wheelchairs)

11.1 Business continuity protocols shall ensure uninterrupted production and distribution of mobility equipment, including spare parts and service support.

11.2 Contingency plans must prioritise wheelchair users whose independence or health may be compromised by delays.

Clause 12: Custom Orders

12.1 Custom medical device orders shall be logged in secure systems and prioritised during business disruption.

12.2 Clients shall be notified of any delays within 48 hours, and documentation shall remain available in **UK GDPR**-compliant cloud repositories.

Clause 13: Regulatory Compliance

13.1 All operations must comply with applicable laws, including:

- **UK Medical Devices Regulations 2002 (as amended post-Brexit)**
- **MHRA vigilance requirements**
- **NHS contract continuity clauses**
- **Health and Social Care Act 2012**

13.2 Any deviation from service-level agreements (SLAs) due to disruption must be escalated to compliance officers immediately.

13.3 Regulated disruptions (e.g. affecting patient care) must be reported to MHRA/NHS as required.

Clause 14: CGM-Specific Continuity Measures

14.1 CGM supply and calibration services must be prioritised due to their impact on real-time diabetes care and patient safety.

14.2 Data management related to CGMs must comply with **UK GDPR** and **Medical Device Data Systems (MDDS)**guidance.

14.3 Any issue impacting CGM availability, integrity, or usage must be escalated within 24 hours and flagged to patient services and regulatory authorities.

Clause 15: People, Processes, Premises, and Providers

15.1 The Company must ensure continuity across four core pillars:

- **People**: Emergency staffing rotas and role redundancy
- **Processes**: Priority SOPs and remote-access workflows
- **Premises**: Safe facilities with alternate site agreements
- **Providers**: Prequalified backup vendors

15.2 Secure, VPN-enabled remote access must be available to critical staff.

15.3 Contracts with alternate facility providers (e.g., hot sites) must be in place and reviewed annually.

15.4 Emergency contacts and shift rosters will be updated monthly.

Clause 16: ISO 22301 Alignment

16.1 This Plan is written in accordance with the **ISO 22301:2019 Business Continuity Management System**, suitable for audit and certification.

16.2 All procedures follow the **Plan–Do–Check–Act** model and are subject to continuous improvement and internal audit.

Appendix A: Emergency Preparedness and Response

1. Purpose and Scope

1.1 This Emergency Preparedness and Response Policy ("the Policy") establishes the procedures and responsibilities for managing unforeseen disruptive events that may impact Urathon Europe Ltd ("the company")'s ability to deliver critical goods and services.
1.2 The Policy applies to all Company operations, including manufacturing, warehousing, logistics, digital infrastructure, and customer services, both in the UK and internationally.
1.3 This Policy is aligned with the Civil Contingencies Act 2004, ISO 22301:2019, and relevant sector-specific guidance issued by the UK Health Security Agency (UKHSA) and the NHS Emergency Preparedness, Resilience and Response (EPRR) Framework.

2. Definitions

2.1 Emergency: Any incident that threatens life, disrupts operations, or poses significant risk to safety, health, environment, or service continuity.
2.2 Critical Infrastructure: Essential systems such as IT, utilities, healthcare devices, and communications platforms required for service delivery.
2.3 Resilience Measures: Pre-planned interventions to prevent, absorb, and recover from disruptive events.

3. Risk Categories Covered

3.1 This Policy covers, at a minimum, emergency planning for the following categories:

- Power outages, utility failures, and energy disruption
- Natural disasters, including storms, floods, fires, and severe weather
- Health emergencies, such as pandemics, infectious disease outbreaks, and biological incidents
- Terror threats or civil unrest, where applicable
- IT infrastructure failures or cyberattacks

4. Emergency Planning Measures

4.1 The Company maintains and regularly updates emergency response protocols for each risk category. These include:

- Backup power generators and uninterruptible power supplies (UPS)
- Designated alternate sites for critical operations
- Remote working capabilities for essential staff
- Crisis communication plans (internal and public facing)
- Evacuation and safety protocols for all premises
- Medical-grade PPE, sanitisation protocols, and pandemic checklists

4.2 Emergency scenarios are modelled through the Company's Business Impact Analysis (BIA) and incorporated into the overarching Business Continuity Plan (BCP).

5. Responsibilities and Coordination

5.1 The Emergency Response Lead shall activate response protocols, coordinate across departments, and liaise with emergency services, regulators, and NHS partners where necessary.

5.2 Department Heads must ensure staff are trained in emergency procedures and familiar with evacuation plans, contact trees, and shelter-in-place protocols.

5.3 Suppliers and subcontractors must maintain equivalent emergency response capabilities, as contractually required under continuity and Force Majeure clauses.

6. Regulatory Compliance and Public Sector Alignment

6.1 The Company's preparedness aligns with:

- Civil Contingencies Act 2004 (Category 2 responder responsibilities)
- NHS EPRR Framework
- Health and Safety at Work Act 1974
- Equality Act 2010, including accessible evacuation for persons with disabilities

6.2 Disruptions that impact regulated product delivery (e.g., CGM devices or mobility aids) will be reported to the MHRA, NHS Trusts, or local authority commissioners as required.

7. Testing, Training, and Continuous Improvement

7.1 Emergency drills (e.g., fire, power loss, cyber breach) shall be conducted biannually, with lessons learned integrated into revised procedures.

7.2 All staff must undergo annual training on emergency response relevant to their roles.

7.3 The Policy is reviewed annually or after any material incident to incorporate updated best practices, legal obligations, and lessons learned.