BUSINESS CONTINUITY PLAN

Version 1.5 | Effective Date: January 20, 2025 | Classification: CONFIDENTIAL

DOCUMENT CONTROL

Version	Date	Author	Approved By	Changes
1.0	Jan 15, 2023	David Miller	Executive Committee	Initial version
1.1	Jun 10, 2023	David Miller	Executive Committee	Updated recovery priorities
1.2	Nov 30, 2023	Lisa Chen	Executive Committee	Added pandemic response section
1.3	Apr 15, 2024	David Miller	Executive Committee	Updated contact information
1.4	Sep 22, 2024	Lisa Chen	Executive Committee	Enhanced cloud recovery procedures
1.5	Jan 20, 2025	David Miller	Executive Committee	Annual review and updates

1. INTRODUCTION

1.1 Purpose

This Business Continuity Plan (BCP) provides the framework for TNO to prepare for, respond to, and recover from disasters and business disruptions. It outlines the procedures, responsibilities, and resources needed to maintain essential business functions during and after a disruptive event.

1.2 Scope

This plan applies to all TNO facilities, systems, and operations. It covers a wide range of potential disruptions, from localized technical failures to large-scale natural disasters or global pandemics.

1.3 Objectives

1. Protect human life and safety
2. Minimize financial and operational impact of disruptions
3. Maintain essential business functions during disruptions

4. Ensure timely recovery of normal operations

5. Meet regulatory and contractual obligations

6. Protect TNO's reputation and stakeholder confidence

2. BUSINESS IMPACT ANALYSIS

2.1 Critical Business Functions

The following business functions have been identified as critical to TNO's operations:

| Function | Department | Maximum Tolerable Downtime | Recovery Time Objective | Recovery Point Objective |

|---|---|---|---|---|

| Security Operations Center | Information Security | 0 hours (continuous) | < 15 minutes | < 5 minutes |

| Core Production Systems | Operations | 2 hours | 1 hour | < 15 minutes |

| Customer-facing Portals | IT | 4 hours | 2 hours | < 30 minutes |

| Communication Systems | IT | 4 hours | 2 hours | < 30 minutes |

| Payment Processing | Finance | 8 hours | 4 hours | < 1 hour |

| Human Resources Systems | HR | 24 hours | 12 hours | < 4 hours |

| Email and Collaboration | IT | 8 hours | 4 hours | < 1 hour |

| Market Data Services | Research | 8 hours | 4 hours | < 2 hours |

| Document Management | IT | 24 hours | 12 hours | < 4 hours |

2.2 Critical Resources

The following resources are required to support critical business functions:

1. **Personnel**: Key staff required to perform critical functions

2. **Technology**: IT systems, applications, and infrastructure

3. **Facilities**: Physical locations and work environments

4. **Information**: Critical data and documentation

5. **Suppliers**: External service providers and vendors

2.3 Threat Assessment

Threat Type	Likelihood	Impact	Risk Level
Cyberattack/Ransomware	High	Critical	High
Power Outage	Medium	High	Medium
Natural Disaster	Low	Critical	Medium
Pandemic/Health Crisis	Medium	Critical	Medium
IT System Failure	Medium	High	Medium
Supply Chain Disruption	Medium	High	Medium
Telecommunications Failure	Medium	High	Medium
Fire	Low	Critical	Medium
Civil Unrest	Low	Medium	Low
Terrorist Attack	Low	Critical	Medium

3. RECOVERY STRATEGY

3.1 Personnel Recovery

1. Employee safety and welfare protocols
2. Remote work capabilities and policies
3. Cross-training program for critical roles
4. Emergency staffing arrangements
5. Crisis counseling and support services

3.2 Technology Recovery

In the event of a disaster, the following recovery procedures shall be implemented:

1. Activate redundant systems and failover mechanisms
2. Restore from backups following established procedures
3. Deploy emergency virtual infrastructure if primary and secondary sites are unavailable
4. Implement manual workarounds for critical processes while systems are being restored
5. Escalate to cloud-based disaster recovery environment if necessary

3.3 Facility Recovery

1. Primary site evacuation procedures
2. Alternate work location activation
3. Remote work implementation for non-essential personnel
4. Temporary facility procurement process
5. Facility restoration coordination

4. RECOVERY PRIORITIES AND PROCEDURES

4.1 Recovery Priority Order

Critical systems shall be restored according to the following priority order:

1. Security and access control systems
2. Network infrastructure and connectivity
3. Core production applications
4. Customer-facing services
5. Communication systems
6. Data storage and management systems
7. Financial systems
8. Collaboration tools
9. Support systems

4.2 Recovery Time Frames

| Phase | Timeframe | Activities |

|-------|-----------|------------|

| Emergency Response | 0-2 hours | Initial assessment, life safety, crisis communication, immediate containment |

| Stabilization | 2-24 hours | Damage assessment, temporary measures, critical function restoration |

| Initial Recovery | 1-3 days | Essential function restoration, alternative processing, customer communication |

| Full Recovery | 3-30 days | Complete system recovery, return to normal operations, after-action review |

4.3 Data Backup and Recovery

1. Full system backups are conducted daily

2. Transaction logs are backed up hourly

3. Backups are stored both on-site and off-site

4. Cloud-based backup retention: 30 days rolling

5. Quarterly backup restoration tests are conducted

6. Backup encryption and integrity verification procedures

5. CRISIS MANAGEMENT

5.1 Crisis Management Team

| Role | Primary | Alternate | Responsibilities |

|------|---------|-----------|------------------|

| Crisis Director | CEO | COO | Overall direction and decision-making |

| Operations Lead | COO | Operations Director | Coordination of operational response |

| Technical Lead | CIO | IT Director | IT systems recovery |

| Communications Lead | Communications Director | Marketing Manager | Internal and external communications |

| HR Lead | HR Director | HR Manager | Staff welfare and communications |

| Legal/Compliance Lead | General Counsel | Compliance Officer | Legal and regulatory matters |

| Finance Lead | CFO | Finance Director | Financial impact assessment and management |

| Facilities Lead | Facilities Manager | Security Manager | Physical location management |

5.2 Crisis Command Center

Primary Location: Headquarters Conference Room A

Secondary Location: Regional Office Executive Suite

Virtual Command Center: Microsoft Teams Crisis Management Channel

5.3 Communication Plan

1. Initial notification procedures
2. Regular status update schedule
3. Customer communication templates
4. Regulatory notification requirements
5. Media response protocols
6. Internal staff communications

6. BUSINESS CONTINUITY PROCEDURES

6.1 Plan Activation

1. Incident detection and assessment criteria
2. Activation authority and process
3. Notification and escalation procedures
4. Initial response actions
5. Plan activation documentation

6.2 Emergency Response

1. Life safety procedures
2. Evacuation and assembly points
3. Emergency services coordination
4. Damage containment measures
5. Initial assessment reporting

6.3 Department-Specific Procedures

Each critical department maintains detailed recovery procedures in their departmental appendices to this plan.

7. TESTING AND MAINTENANCE

Regular testing of the business continuity plan shall be conducted annually:

1. Plan review: Quarterly
2. Tabletop exercises: Semi-annually
3. Functional drills: Annually
4. Full-scale simulation: Annually
5. Technical recovery testing: Quarterly
6. Supplier continuity verification: Annually

7.1 Testing Schedule

Test Type	Frequency	Last Test	Next Test	Responsibility
Plan Review	Quarterly	Dec 2024	Mar 2025	BC Coordinator
Tabletop Exercise	Semi-annual	Nov 2024	May 2025	Crisis Management Team
Technical Recovery	Quarterly	Jan 2025	Apr 2025	IT Department
Call Tree Verification	Quarterly	Jan 2025	Apr 2025	Department Managers
Full-Scale Simulation	Annual	Sep 2024	Sep 2025	BC Committee

7.2 Plan Maintenance

1. Annual plan review and update process
2. Change management procedures
3. Version control and distribution
4. Training requirements for new personnel
5. Post-incident review and improvement process

8. ROLES AND RESPONSIBILITIES

8.1 Executive Management

1. Approve and support the business continuity program
2. Provide necessary resources
3. Participate in crisis management
4. Review and approve major recovery decisions

8.2 Business Continuity Coordinator

1. Maintain and update the business continuity plan
2. Coordinate testing and exercises
3. Train employees on their roles and responsibilities
4. Lead post-incident reviews
5. Report on program status to executive management

8.3 Department Managers

1. Develop and maintain department recovery procedures
2. Identify critical functions and resources
3. Ensure staff awareness and preparedness

4. Participate in testing and exercises

5. Lead department recovery efforts during activation

8.4 All Employees

1. Be familiar with the business continuity plan

2. Understand individual roles during disruptions

3. Participate in training and exercises

4. Follow procedures during plan activation

5. Provide feedback for plan improvement

9. APPENDICES

9.1 Contact Lists

Critical contact information is maintained in Appendix A.

9.2 Vendor and Supplier Information

Key vendor and supplier contact information and recovery expectations are documented in Appendix B.

9.3 Equipment and Resource Inventories

Comprehensive inventories of critical equipment and resources are maintained in Appendix C.

9.4 System Recovery Procedures

Detailed technical recovery procedures are documented in Appendix D.

9.5 Alternate Site Information

Information about alternate work locations is maintained in Appendix E.

9.6 Forms and Checklists

Standardized forms and checklists for use during plan activation are included in Appendix F.

APPROVED BY:

Richard Spencer, Chief Executive Officer

Date: January 20, 2025