BUSINESS CONTINUITY AND DISASTER RECOVERY POLICY

Effective Year: 2026

1. Introduction

This Business Continuity and Disaster Recovery Policy establishes the framework for maintaining critical MDOI services during disruptions and restoring operations following incidents that threaten the availability, integrity, or functionality of the MDOI infrastructure.

2. Purpose of the Policy

The purpose of this policy is to ensure that the MDOI Foundation can continue providing essential services, including identifier registration, metadata management, identifier resolution, dashboard access, API services, and digital preservation functions during emergencies, disasters, technical failures, or security incidents.

3. Scope

This policy applies to all MDOI systems, infrastructure, applications, databases, metadata repositories, identifier services, cloud resources, backups, communication systems, personnel, service providers, and operational processes supporting the MDOI ecosystem.

4. Business Continuity Principles

MDOI shall maintain preparedness, resilience, redundancy, responsiveness, recovery capability, continuous improvement, and stakeholder communication as the core principles guiding continuity and recovery planning.

5. Critical Services Identification

The following services are considered critical and shall receive priority during recovery operations:

- Identifier Resolution Services
- Metadata Registry Services

- Identifier Registration Services
- User Authentication and Access Control
- Dashboard Platform Operations
- API Services and Integrations
- Notification and Communication Systems
- Backup and Preservation Infrastructure

6. Risk Assessment

The Foundation shall periodically assess risks that may disrupt operations, including cyberattacks, hardware failures, software failures, data corruption, network outages, cloud service disruptions, power failures, natural disasters, human error, insider threats, and third-party service interruptions.

7. Business Continuity Planning

MDOI shall maintain documented continuity procedures that define how critical services will continue operating during disruptions. Plans shall include service prioritisation, alternative operating procedures, emergency communication mechanisms, recovery responsibilities, and escalation processes.

8. Disaster Recovery Planning

Disaster recovery procedures shall define how systems, databases, applications, metadata repositories, identifier records, and operational services are restored following a disruptive incident. Recovery procedures shall be documented, tested, and periodically updated.

9. Backup Management

MDOI shall maintain secure and reliable backups of critical databases, metadata records, identifier registries, configuration files, audit logs, user accounts, and operational records. Backups shall be performed at appropriate intervals and stored in secure locations.

10. Data Recovery Objectives

Recovery efforts shall aim to minimise data loss and service interruption. Recovery objectives may include:

- Recovery Time Objective (RTO): The target time to restore critical services.

- Recovery Point Objective (RPO): The maximum acceptable amount of data loss measured by time.

The Foundation shall define and periodically review these objectives based on operational requirements.

11. Redundancy and Resilience

Where feasible, MDOI shall implement redundancy mechanisms such as replicated databases, backup servers, cloud failover services, alternative communication channels, and distributed storage systems to improve resilience and service continuity.

12. Incident Response Integration

Business continuity and disaster recovery activities shall align with the MDOI Information Security Policy and Incident Response Procedures. Security incidents that affect service availability shall trigger coordinated response and recovery actions.

13. Roles and Responsibilities

The Foundation shall assign responsibilities for continuity and recovery activities. Responsibilities may include incident coordination, technical recovery, communication management, infrastructure restoration, security assessment, stakeholder engagement, and post-incident review.

14. Emergency Communication

During major incidents, MDOI shall provide timely communication to users, members, organisations, partners, and stakeholders regarding service disruptions, estimated recovery timelines, system status, and available support channels.

15. Third-Party Dependencies

Where critical services depend on cloud providers, hosting services, payment processors, communication platforms, or other external providers, MDOI shall evaluate dependency risks and maintain contingency plans where practical.

16. Testing and Exercises

The Foundation shall periodically test business continuity and disaster recovery procedures through simulations, tabletop exercises, backup restoration tests, failover testing, and operational reviews to validate preparedness and identify improvement opportunities.

17. Preservation of Metadata and Identifiers

The Foundation shall prioritise the preservation of metadata records, identifier assignments, resolution history, audit logs, and digital preservation records. Continuity measures shall support long-term persistence and reliability of identifiers even during extended disruptions.

18. Recovery Prioritisation

Recovery efforts shall prioritise services based on operational importance. Identifier resolution, metadata access, and core infrastructure services shall generally receive priority over non-critical functions.

19. Post-Incident Review

Following significant incidents, MDOI shall conduct a post-incident assessment to identify root causes, evaluate response effectiveness, document lessons learned, and improve continuity and recovery procedures.

20. Training and Awareness

Relevant personnel shall receive appropriate training regarding continuity responsibilities, disaster recovery procedures, emergency communication practices, and incident response coordination.

21. Compliance

This policy supports compliance with applicable information security, data protection, digital preservation, governance, and operational resilience requirements. Users and service providers must cooperate with continuity and recovery efforts where applicable.

22. Enforcement

Failure to comply with continuity and recovery responsibilities may result in corrective action, access restrictions, contract review, suspension of privileges, or other measures necessary to protect the reliability of the MDOI infrastructure.

23. Policy Review and Updates

This policy shall be reviewed periodically and updated to reflect technological developments, emerging threats, operational changes, lessons learned from incidents, and best practices in business continuity management.

24. Conclusion

This Business Continuity and Disaster Recovery Policy strengthens the resilience of the MDOI ecosystem by ensuring preparedness, rapid recovery, operational continuity, and long-term protection of identifiers, metadata, and digital knowledge infrastructure.

Through effective planning and recovery measures, MDOI remains committed to reliable and uninterrupted service delivery.