MIROSLAV TADEJ CONSULTING

Business Continuity & Disaster Recovery Plan

Maintaining and recovering critical services after disruption

Aligned with ISO/IEC 27001:2022 (A.5.29, A.5.30, A.8.13, A.8.14) and recognised business-continuity practice

Document control

Document title	Business Continuity & Disaster Recovery Plan
Document owner	Miroslav Tadej, Principal Consultant
Organisation	Miroslav Tadej Consulting
Version	1.0
Status	Approved
Classification	Public — issued for tender and client assurance
Effective date	13/06/2026
Next review date	12/06/2027
Approved by	Miroslav Tadej, Principal Consultant

Contents

1. Purpose and objectives

This Business Continuity & Disaster Recovery Plan ("the Plan") sets out how Miroslav Tadej Consulting ("the Consultancy") maintains its critical services and recovers its systems and information following a disruptive event. Its objectives are to protect the interests of clients, to limit the impact of disruption, and to restore normal service as quickly and safely as possible.

The Plan recognises that the Consultancy operates as a specialist, principal-led practice, and so addresses the specific continuity risks that arise from that model — including key-person availability and reliance on third-party cloud providers — with proportionate, practical arrangements.

2. Scope

The Plan covers the people, information, systems, suppliers, and facilities the Consultancy depends on to deliver its services, including:

- the Consultancy's own operations — client communications, project delivery, and business administration;
- client systems hosted or maintained by the Consultancy, where continuity is a contractual responsibility;
- the source code, data, credentials, and documentation needed to deliver and recover services; and
- the third-party providers on which the Consultancy and its clients rely — cloud hosting, source-code hosting, payment processing, email, and monitoring.

3. Roles and responsibilities

The Principal Consultant is responsible for invoking, leading, and coordinating the response to any disruption, for client communication, and for maintaining and testing this Plan. To mitigate the key-person risk inherent in a sole-practitioner model, the Consultancy maintains:

- **Documentation:** clear, current documentation so that a competent third party could understand and recover each client system;
- **Standby support:** a trusted contractor or associate who can be called upon to assist or act in the event of the Principal Consultant's unavailability; and
- **Access continuity:** secured, accessible records of critical credentials and recovery information held in a password manager and, where appropriate, made available to clients for their own systems.

4. Business impact analysis

The Consultancy has assessed the relative criticality of its activities and the maximum tolerable period of disruption for each. This analysis drives the recovery priorities and objectives in section 5.

Activity	Criticality	Maximum tolerable disruption
Client production systems (hosted/maintained)	Critical	Hours — governed by client SLA
Security incident response for clients	Critical	Immediate — as incidents arise
Active project delivery	High	1–2 business days
Client communications	High	1 business day
Business administration & billing	Moderate	Several business days
Marketing & website	Low	1–2 weeks

5. Recovery objectives

The Consultancy defines its recovery objectives using two standard measures:

- **Recovery Time Objective (RTO):** the target time to restore a service after disruption.
- **Recovery Point Objective (RPO):** the maximum acceptable amount of data loss, measured as the period since the last usable backup.

Indicative objectives are set out below. For client systems, the applicable objectives are those agreed in the relevant contract or service-level agreement, which take precedence where they are more demanding.

System / service	Target RTO	Target RPO
Client production application	4–24 hours (per SLA)	≤ 24 hours
Client database	4–24 hours (per SLA)	≤ 24 hours
Source code & repositories	≤ 4 hours	≤ 1 hour (hosted & mirrored)
Consultancy email & comms	≤ 4 hours	Near-zero (cloud-hosted)
Business records & documentation	≤ 1 business day	≤ 24 hours

6. Data backup and recovery strategy

Reliable, tested backups are the foundation of recovery. The Consultancy applies the following approach:

- **3-2-1 principle:** critical data is backed up following the 3-2-1 principle — at least three copies, on two types of media or location, with at least one held off-site or in a separate cloud region.
- **Automated backups:** production databases use automated backups with point-in-time recovery provided by managed database services, so data can be restored to a moment before an incident.
- **Source code:** source code is held in hosted repositories and mirrored, so loss of any single copy does not lose the work.
- **Encryption:** backups are encrypted in transit and at rest, and access to them is restricted.
- **Restore testing:** restores are tested periodically to confirm that backups are usable and that recovery objectives can be met — a backup is only as good as the last successful restore.

7. Disruption scenarios and response

The Plan addresses the disruption scenarios most relevant to the Consultancy. For each, the response aims to contain the impact, communicate with affected clients, and restore service within the recovery objectives.

7.1 Cloud or hosting provider outage

If a hosting or cloud provider suffers an outage, the Consultancy monitors the provider's status, keeps affected clients informed, and — for prolonged outages — restores affected systems from backup into an alternative region or provider. Provider selection favours those with strong resilience and multi-region capability.

7.2 Data loss or corruption

If data is lost, corrupted, or affected by a faulty change, the Consultancy restores from the most recent clean backup using point-in-time recovery, validates integrity, and identifies and corrects the root cause before returning to normal operation.

7.3 Cyber-attack or ransomware

A security-driven disruption is handled jointly under this Plan and the incident-management process in the Information Security and Data Protection policies: the affected systems are isolated and contained, clean backups are used to rebuild rather than paying any ransom, affected parties and — where personal data is involved — the Data Protection Commission are notified within the required timeframes, and lessons are captured afterwards.

7.4 Loss, theft, or failure of a working device

Working devices are protected by full-disk encryption so that loss or theft does not expose data. Because work and credentials are held in cloud services and a password manager rather than solely on local devices, the Consultancy can resume work on a replacement device quickly, with minimal data loss.

7.5 Key-person unavailability

If the Principal Consultant becomes unavailable, the Consultancy relies on its current documentation and standby support arrangements so that critical client systems can continue to be supported. Clients with critical systems are made aware of the continuity arrangements relevant to them, including access to their own credentials and recovery information.

7.6 Supplier or service failure

If a critical third-party service fails or is withdrawn, the Consultancy assesses alternatives, migrates affected functions where necessary, and keeps clients informed. Dependence on any single provider is kept to what is reasonable, and data portability is considered when selecting suppliers.

8. Communication during disruption

Clear communication limits the impact of any disruption. During an incident the Consultancy will, as a priority, inform affected clients of the nature of the disruption, the expected impact, and the steps being taken, and will provide regular updates until service is restored. Contact details for clients and key suppliers are kept current and accessible independently of the systems that may be affected. Where a disruption involves a personal data breach, communication follows the requirements of the Data Protection Policy.

9. Testing, maintenance, and improvement

A plan that is never tested cannot be relied upon. The Consultancy:

1. tests backup restoration periodically to confirm data can be recovered within the recovery objectives;
2. reviews and walks through the disruption scenarios at least annually to confirm the response remains practical;
3. updates the Plan whenever services, systems, suppliers, or client commitments change materially; and
4. records the outcome of tests and real incidents, and feeds improvements back into the Plan and the risk register.

10. Related documents

- Information Security Policy
- Data Protection Policy
- GDPR Compliance Statement
- Secure Development Policy
- Quality Management Statement

11. Approval

This Business Continuity & Disaster Recovery Plan is approved and issued by the Principal Consultant of Miroslav Tadej Consulting and takes effect from the effective date recorded in the document-control table above.

Name & role	Signature	Date
Miroslav Tadej Principal Consultant	Miroslav Tadej	13/06/2026

Miroslav Tadej Consulting · Dublin, Ireland · Business Continuity & DR Plan v1.0