Information Continuity Policy

Classified: External

Organisation Issue No: 1

Organisation Issue Date: 28/7/2025

Document Owner: Information Security Manager

1. Purpose

This policy establishes IDDQD Limited's commitment to maintaining information continuity during adverse events, ensuring the availability, integrity, and confidentiality of critical information assets. It provides the framework for developing, implementing, and maintaining information continuity capabilities across the organisation.

2. Scope

This policy applies to all IDDQD employees, contractors, and third parties with access to company information. It encompasses all information assets regardless of format, whether electronic, physical, or verbal. The policy covers all information processing facilities and systems, as well as all locations where IDDQD information is processed, stored, or transmitted.

3. Policy Statements

3.1 Information Continuity Management

IDDQD shall establish and maintain information continuity processes that are fully integrated with the organisation's business continuity management framework. The organisation will identify and prioritise critical information assets and systems based on comprehensive business impact analysis. Recovery objectives will be defined in alignment with business requirements and the organisation's risk appetite. Throughout any continuity event, IDDQD will ensure that information security controls remain effective and appropriate to the circumstances.

3.2 Planning and Preparedness

The organisation shall develop and maintain comprehensive information continuity plans that address various disruption scenarios. Clear roles, responsibilities, and authorities for continuity management will be defined and communicated to all relevant parties. The organisation will establish specific recovery time objectives (RTO) and recovery point objectives (RPO) for all critical systems. Current inventories of information assets and their dependencies will be maintained to ensure rapid and effective response during disruptions.

3.3 Priority Levels

Information security incidents shall be categorised into priority levels to ensure appropriate response and resource allocation. Priority 1 (P1) incidents are those where an outage would have immediate impact on customer operations. Priority 2 (P2) incidents are those where an outage would have immediate impact on IDDQD's ability to continue business operations. Priority 3 (P3) incidents are those where an outage lasting greater than 72 hours would impact IDDQD's ability to continue business. Priority 4 (P4) incidents involve non-critical systems where neither customers nor IDDQD operations are affected.

3.4 Recovery Objectives

The organisation establishes specific recovery objectives for each service category to ensure timely restoration of critical services:

Service Category	Time until BCP Activates	Recovery Time Objective	Recovery Point Objective
Priority 1 (P1)	1 hour	1 hours	1 hour
Priority 2 (P2)	3 hours	3 hours	1 hour
Priority 3 (P3)	24 hours	72 hours	1 hour
Priority 4 (P4)	N/A	N/A	N/A

3.5 Risk-Based Approach

Information continuity planning shall be based on systematic risk assessment that considers all threats to information availability. The organisation will identify and address single points of failure in critical information processing chains. Dependencies on third parties and supply chains will be carefully considered and managed. Plans will include specific provisions for maintaining appropriate security levels during degraded operations.

To mitigate risks of service disruption, critical systems shall be designed with appropriate redundancy and failover capabilities. Critical systems shall be distributed across multiple geographic locations to ensure resilience against localised failures. Automated failover mechanisms shall be implemented to minimise service interruption and ensure rapid recovery without manual intervention. The organisation will maintain sufficient redundancy in infrastructure, applications, and data to meet defined recovery objectives. All failover procedures shall be regularly tested to ensure they function correctly when needed.

3.6 Response and Recovery

The organisation shall establish clear escalation procedures and activation criteria for continuity plans to ensure timely and appropriate response. Emergency response teams will be defined with appropriate authority and resources to make critical decisions during incidents. Alternative communication channels and contact methods will be maintained to ensure continuity of communications. All restoration activities will ensure the secure recovery of information systems and data, maintaining confidentiality and integrity throughout the process.

3.7 Testing and Improvement

IDDQD shall regularly test information continuity arrangements through planned exercises and simulations to verify their effectiveness. Plans will be reviewed and updated based on test results and lessons learned from both exercises and actual incidents. The organisation will incorporate changes in business operations, technology landscape, and emerging threats into continuity planning. Evidence of all testing and improvement activities will be maintained for audit and review purposes.

4. Compliance

4.1 Standards and Regulations

This policy supports compliance with ISO 27001:2022 control A.5.30 (ICT readiness for business continuity), all applicable legal and regulatory requirements, and contractual obligations regarding service availability.

4.2 Related Policies

This policy should be read in conjunction with the Information Security Policy, Risk Management Policy, Backup and Restore Policy, Network Security Policies and Procedures, and Computing Device Security Policy.

5. Responsibilities

5.1 Management

Senior management shall provide adequate resources for information continuity management and ensure these resources are appropriately allocated. They will review and approve continuity strategies and plans, ensuring their alignment with business objectives.

Management will ensure full integration between information continuity and overall business continuity management. They will champion a culture of resilience and preparedness throughout the organisation.

5.2 Information Security Committee

The Committee shall oversee the development and maintenance of continuity capabilities across the organisation. They will coordinate testing and improvement activities to ensure plans remain current and effective. During incidents, the Committee will act as the emergency response team, making critical decisions and coordinating response efforts. Regular reports on continuity readiness will be provided to senior management.

5.3 All Staff

All personnel shall understand their specific roles in information continuity and how they contribute to organisational resilience. They will actively participate in training and awareness activities to maintain competency. Staff members are expected to report potential continuity risks or issues as they identify them. During continuity events, all personnel will follow established procedures and support recovery efforts as directed.

6. Implementation

6.1 Documentation

Supporting documentation for this policy includes the Information Continuity Plan containing detailed procedures, Business Impact Analysis results that inform priority decisions, risk assessments and treatment plans addressing continuity threats, testing schedules and reports demonstrating plan effectiveness, and contact lists and escalation procedures for emergency response.

6.2 Training and Awareness

The organisation shall ensure regular training on continuity procedures is provided to all relevant personnel. Awareness programmes will ensure all staff understand their individual responsibilities. Simulation exercises will be conducted for key personnel to maintain readiness. Documentation of competency requirements will be maintained to ensure appropriate skill levels.

7. Monitoring and Review

This policy shall be reviewed annually or after significant changes to ensure continued relevance and effectiveness. Updates will be made based on emerging threats and business changes. The effectiveness of the policy will be assessed through defined metrics and indicators. The policy and its implementation will be subject to internal audit and management review processes.

8. Exceptions

Any exceptions to this policy must be formally documented with clear business justification. All exceptions will be risk assessed and require approval by the Information Security Committee. Exceptions will be time-bound with defined compensating controls to manage residual risks. All exceptions will be regularly reviewed to ensure continued validity and necessity.

9. Enforcement

Non-compliance with this policy may result in disciplinary action in accordance with company procedures. Access privileges and authorities may be reviewed and potentially revoked for serious breaches. Additional training requirements may be mandated for personnel who fail to comply with policy requirements. Where appropriate, legal action may be taken for violations that result in significant harm to the organisation.

10. Definitions

Information Continuity refers to the capability to continue, resume, or recover critical information processing within acceptable timeframes following disruption.

Recovery Time Objective (RTO) is the maximum acceptable time for restoring functionality after a disruption.

Recovery Point Objective (RPO) is the maximum acceptable data loss measured in time, representing the point to which data must be recovered.

Business Impact Analysis is the process of determining the criticality of business activities and their associated resource requirements.

This policy has been approved by senior management and is effective immediately.

IDDQD Limited