Business Continuity and Disaster Recovery (BCP/DR) Policy

Approved by	Signature	Effective Date
Security Team	Official Security Team Approved	03/11/2025

1. Purpose

This policy establishes the framework and guidelines to ensure that DanfeCorp is prepared to continue operations in the event of a disaster or significant disruption. It outlines the processes for minimizing downtime, protecting critical data, and ensuring prompt recovery of systems and business functions.

2. Scope

This policy applies to all business processes, systems, applications, networks, data, and personnel at DanfeCorp. It covers:

- Protection of critical business functions.
- Establishment of recovery strategies and procedures.
- Definition of roles and responsibilities during disruptions or disasters.
- Procedures for testing and maintaining continuity and recovery plans.

3. Objectives

The comprehensive objectives of DanfeCorp's Business Continuity and Disaster Recovery program are designed to create a resilient organization capable of maintaining essential operations under adverse conditions while protecting its assets and stakeholders. Our primary objective is to minimize operational downtime by efficiently restoring mission-critical systems and processes following an incident, ensuring that business functions can resume within established recovery time parameters that align with organizational priorities. Data protection forms another crucial objective, as we commit to preserving data integrity and ensuring availability with minimal data loss through robust backup strategies, redundant storage solutions, and clearly defined recovery point objectives that balance business needs with technical capabilities. Throughout any disruptive event, maintaining timely and clear communication with internal stakeholders, customers, and external parties is essential for effective coordination, expectation management, and reputation preservation. Our BCP/DR strategies are also designed to ensure alignment with all regulatory and contractual obligations applicable to our industry and operational jurisdictions, demonstrating our commitment to compliance and due diligence. Underpinning all these objectives is our dedication to continuous improvement, whereby we regularly update and test our plans to enhance organizational readiness, address emerging risks, and incorporate lessons learned from exercises and real-world incidents, creating an evolving framework that strengthens our resilience posture over time.

4. Business Continuity Planning

4.1 Business Impact Analysis (BIA)

- **Identification of Critical Functions:** Conduct a BIA to identify and prioritize critical business functions, processes, and systems.
- **Risk Assessment:** Regularly assess potential threats—including natural disasters, cyberattacks, and system failures—to identify risks and vulnerabilities.
- **Recovery Time Objectives (RTO):** Establish the maximum acceptable downtime for each critical function.
- **Recovery Point Objectives (RPO):** Define the maximum acceptable data loss for each system or process, ensuring backup procedures meet organizational needs.

4.2 Business Continuity Strategy

Strategy Component	**Implementation Approach**	**Key Considerations**
Preventative Measures	Implement measures to reduce the likelihood and impact of disruptions	Regular backups, redundant infrastructure, robust security controls
Alternative Work Locations	Maintain secondary facilities or remote work capabilities	Ensuring continuity if the primary location becomes unavailable
Supplier and Vendor Continuity	Assess continuity plans of key vendors and suppliers	Ensuring critical service delivery during disruptions

4.3 Plan Development and Documentation

- **Business Continuity Plan (BCP):** Develop a formal, documented BCP for each critical business function and system. The plan outlines procedures for various types of disruptions.
- **Roles and Responsibilities:** Clearly assign roles and responsibilities for business continuity efforts, including escalation procedures, decision-making authority, and contact information for key stakeholders.

5. Disaster Recovery (DR) Planning

5.1 Disaster Recovery Strategy

DanfeCorp's disaster recovery strategy encompasses a comprehensive set of technical and procedural measures designed to ensure rapid recovery of IT systems and data following a disruptive incident. The foundation of this strategy is our robust data backup system, which implements and maintains secure, encrypted backups of all critical data stored in geographically diverse locations to mitigate regional disaster risks. These backups undergo regular recovery testing to verify their reliability and integrity, ensuring they can be successfully restored when needed. Complementing our backup approach, we employ system redundancy by configuring key systems and applications for high availability using failover mechanisms, load balancing technologies, and strategically deployed cloud-based infrastructure that can automatically assume processing responsibilities if primary systems fail. When appropriate to our operational requirements, we leverage cloud-based solutions that enable us to quickly scale resources during recovery operations and provide inherent geographic redundancy without the need for maintaining multiple physical facilities. As an additional layer of protection, we have established dedicated disaster recovery sites—either through internal resources or partnerships with specialized third-party providers—that stand ready to facilitate rapid recovery operations if our primary operating locations become compromised or inaccessible. This multi-faceted strategy provides DanfeCorp with resilient recovery capabilities designed to meet or exceed the recovery time and point objectives established through our business impact analysis process.

5.2 Disaster Recovery Procedures

- **Incident Detection and Response:** Initiate disaster recovery procedures upon detection of a disruptive incident based on predefined recovery protocols.
- **Activation of the DR Plan:** Activate the disaster recovery plan when a disaster is confirmed, following the priorities established by the BIA.
- **System Restoration:** Restore systems and applications according to their criticality and the defined RTO and RPO.
- **Post-Recovery Assessment:** Conduct a post-recovery assessment to evaluate recovery effectiveness, document lessons learned, and update the plan accordingly.

6. Testing and Maintenance

6.1 Plan Testing

- **Regular Testing:** Test the BCP/DR plan annually to verify the effectiveness of recovery strategies. Simulate various disaster scenarios, including system outages, data breaches, and physical disruptions.
- **Tabletop Exercises:** Conduct tabletop exercises to practice decision-making, communication, and coordination among key personnel.
- **Test Reporting:** Prepare detailed reports after each test to evaluate the plan's performance and identify areas for improvement.

6.2 Plan Maintenance

- **Review and Update:** Review and update the BCP/DR plan annually or when significant changes occur in business processes, technology, or external conditions.
- **Continuous Improvement:** Incorporate feedback from tests, real-world incidents, and personnel experiences to ensure the plan remains current and effective.

7. Roles and Responsibilities

Role	Responsibilities
Executive Management	Provide resources and support for BCP/DR initiatives to ensure alignment with business objectives and participate in critical decision-making during disastersOversee resource allocation and stakeholder communication
Business Continuity Coordinator	Oversee development, implementation, testing, and maintenance of BCP/DR planEnsure all employees are trained on their roles during disastersConduct regular awareness campaigns
IT and Security Teams	Manage technical aspects of disaster recoveryPerform data restoration, system reconfiguration, and security assuranceOversee regular backups and ensure backup data security
Employees and Contractors	Remain aware of individual responsibilities under the BCP/DR plan and participate in required training and exercises

8. Communication

- **Internal Communication:** Establish clear communication channels for internal stakeholders, detailing incident reporting, remote access procedures, and recovery actions.
- **External Communication:** Provide updates to customers, vendors, and other external parties regarding the status of recovery efforts and any service impacts.

9. Compliance and Legal Considerations

- **Regulatory Compliance:** Ensure that the BCP/DR plan meets all relevant regulatory requirements and contractual obligations.
- **Legal Documentation:** Have the policy reviewed by legal counsel to confirm compliance with industry standards and legal requirements related to disaster recovery and business continuity.

10. Policy Review and Updates

This policy will be reviewed and updated annually or in response to significant changes in the business environment, technology, or external regulations. All updates will be documented and communicated to relevant stakeholders.

This policy document supersedes all previous business continuity and disaster recovery guidelines and becomes effective as of the date specified above.