Elevaite365

Business Continuity and Disaster Recovery Policy

Version 1.0

PURPOSE

This document outlines the planning, building, operation, and maintenance of continuity and recovery requirements across all levels and departments within Elevaite365 (hereby referred to as organization). It aims to minimize downtime, protect critical operations, and facilitate swift recovery from disruptive events.

SCOPE

This policy covers all employees, contractors, and third-party entities within the organization who interact with or support critical processes, data, or systems. It encompasses the organization's technology infrastructure (on-premises or cloud), physical facilities, and any external resources essential for business operations. It is effective across all locations and departments under the organization's operational control.

DEFINITIONS

Following is an explanation of various terms used within this document

- **Business Continuity Plan (BCP):** Documented procedures to ensure essential functions continue during or after a disruption.
- **Disaster Recovery Procedure (DRP):** Technical steps to restore IT systems, applications, and data to meet defined recovery objectives.
- **Business Impact Analysis (BIA):** Process identifying critical functions, dependencies, and potential impact of disruptions, thereby determining recovery priorities.
- **Maximum Allowable Outage (MAO**): The longest duration of a business function can be unavailable before causing an unacceptable impact.
- **Recovery Time Objective (RTO):** Target time to restore a function, service, or system post-disruption.
- **Recovery Point Objective (RPO):** Maximum acceptable data loss interval, indicating how far back in time data can be recovered.
- **Critical Function**: Any process or activity whose failure or unavailability would lead to a significant impact on the organization's operations, finances, reputation, or compliance.
- **Downtime**: When a system, application, or business function is unavailable, whether planned or unplanned.
- **Failover**: Automatically or manually switching operations from a primary to a backup system when a failure or disruption is detected.
- **Recovery Priority**: The order or ranking of systems, services, or functions to be restored based on their criticality to business operations.

RESPONSIBILITIES

1. **DevOps and IT Team**:
    a. Hold the primary responsibility for implementing and maintaining the measures described in this policy.
    b. Coordinate with other departments to ensure all systems, processes, and documentation align with business continuity and disaster recovery objectives.
2. **Escalation Matrix**:
    a. This procedure must be followed in the event of any critical issue or incident that cannot be resolved at the current level.
    b. Outlines specific contacts, timeframes, and escalation paths to ensure timely resolution and minimize downtime.

3. **Emergency Services Table**:
    a. To be referred to in any emergency, providing a quick reference for immediate contacts, resources, and procedures required to stabilize the situation.

POLICY

Business Continuity Principles

1. **Outcome-Focused:** Business continuity management strategies address the impact of disruptions rather than focusing solely on their underlying cause.
2. **Scalability and Adaptability:** Continuity plans must be flexible to accommodate various disruption scales and adapt to organizational changes.
3. **Local Decision-Making:** Continuity planning, response, and recovery activities enable on-the-ground teams to make timely decisions.
4. **Collaboration:** Effective business continuity management fosters cooperation among all involved parties, both internal and external.
5. **Continuous Improvement:** A culture of ongoing refinement underpins the organization's approach to business continuity.

Incident Management Integration

1. **Disruptive Event Linkage:** Incident management processes must recognize and align **disruptive events** with business continuity plans.
2. **Risk-Based Exclusions:**
    a. **Low-Risk Disruptions:** Events deemed low-risk may be omitted from continuity strategies.
    b. **Cost-Prohibitive Scenarios:** Where continuity solutions are prohibitively expensive or restrictive, an exclusion may be granted with the Leadership Team and, if applicable, customer approval.

Critical Function Coverage

1. **Business Impact Analysis (BIA):** Each continuity plan must account for the continuity and recovery of critical business functions identified through a formal BIA.
2. **Risk-Based Identification:** Potential disruptive events are identified using a risk-based approach; only those posing significant impact receive formal continuity strategies.
3. **Recovery Objectives:**
    a. **Maximum Acceptable Outage (MAO):- 24 Hours**
    b. **Recovery Time Objective (RTO):- 24 Hours**
    c. **Recovery Point Objective:- 24 Hours**

These metrics guide the design of backup, failover, and restoration measures for each critical function.

Roles, Responsibilities, and Governance

1. **Plan Content:** Each business continuity plan (BCP) shall define responsibilities, authorities, and communication flows to initiate and maintain operations during and after a disruption.
2. **Stakeholder Training:** All relevant personnel must receive adequate training for their roles within continuity operations.
3. **Plan Testing and Review:** Business continuity arrangements and recovery procedures must be exercised, reviewed, and tested at least once a year using one or more of the following methods:

a. Tabletop review

b. Simulated exercise

c. Partial test

d. Complete test

4. **Testing Evidence and Improvements:** All records and evidence from BCP/DRP tests must be retained, analyzed, and leveraged to enhance the organization's business continuity management.

5. **BCP Training Frequency:** Business continuity training occurs at least annually or whenever the plan undergoes significant changes.

Business Continuity and Disaster Recovery on Cloud

1. **Key BC/DR Aspects in Cloud Environments:**

    a. **SaaS Continuity and Recovery:** Ensure tools and techniques can keep services running if deployment issues or partial cloud outages occur.

        i. **SaaS Application Outages:** Prepare for and effectively manage disruptions in hosted applications.

            A. **Platform Portability:** Evaluate the feasibility of migrating between platforms when required.

2. **Shared Responsibility Model:**

    a. **The organization's Role is to** maintain the resilience of provided SaaS services and leverage zonal redundancy for platforms and applications hosted on IaaS.

    b. **Provider's Role:** Provide reliable computing, networking, and storage infrastructure.

3. **Annual Cloud Testing:**

    a. **BCP & DR Exercises:** Conduct cloud-based BC/DR testing at least annually; produce a report detailing findings, gaps, and improvements.

    b. **Data Restoration Testing:** Verify multi-region or multizone data restoration to ensure zonal resiliency.

Appendix - 1

Information Security Guidelines for Work from Home

Securing Wi-Fi and Network Connections

1. Use secure, encrypted Wi-Fi (e.g., WPA2 or WPA3). Check for older routers or improperly configured networks to prevent unauthorized access.
2. Confirm you are connecting to the correct SSID and avoid using open or public networks for sensitive work.

Antivirus and Software Updates

1. Maintain updated antivirus on all work devices and verify that scans are performed regularly.
2. Keep operating systems, privacy tools, browser add-ons, and all security patches current.

Backup Strategy

1. Develop and follow a routine backup plan for critical files.
2. Store backups securely—preferably on encrypted drives or approved cloud repositories.

Physical Security and Screen Locks

1. Lock your screen whenever you step away, especially if you share the space with others.
2. Avoid working in public areas or co-working spaces where unauthorized individuals might view or intercept your work.

Secure Connections to Work Environment

1. Always use VPN or other secure remote access solutions approved by the organization.
2. Ensure authentication and session encryption (e.g., SSL/TLS) are enabled whenever transmitting confidential data.

Electronic Signatures and Approval Workflows

1. Use electronic signatures or virtual approval mechanisms only through authorized channels.
2. Communicate each instance of such approvals to the appropriate manager or project lead.

Incident Reporting

1. Familiarize yourself with the Incident Management Policy to report potential security breaches or suspicious activity.
2. Contact the IT team via their specified email or helpdesk system for IT-related issues.

Data Handling and Minimizing Downloads

1. Avoid downloading production environment data (from your company or clients) unless necessary.

2. If you must download such data, inform your manager and delete the files once the task is complete to reduce the risk of data exposure.

Reference to Organizational Policies

For further guidance on acceptable use, data classification, and additional security standards, refer to the Intranet or the Information Security Policies page.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Aug 29 2025	Initial Release	Borhan	Linh	Borhan