SynrgiseLearn

Business Continuity Plan

Document Reference	**[Insert Reference]**
Version	1.0
Effective Date	January 03, 2025
Prepared By	Xenothan Hojem
Confidentiality Level	Confidential

Document Control Information

Version History	**Date**	**Author**	**Change Description**
Version 1.0	January 03, 2025	Xenothan Hojem	Initial Document

Organization Information:

Department	**Contact Information**
Executive	info@synrgise.com

Table of Contents

1. Objectives of the Plan

The objectives of this plan are to:

- Maintain the continuity of essential business processes with defined **Key Performance Indicators (KPIs)** such as Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
- Minimize operational disruption through a structured response plan with clearly defined escalation thresholds.
- Establish a recovery framework to restore operations efficiently, reducing downtime and financial loss.
- Ensure the safety of employees and protection of critical assets by implementing robust security measures outlined in the Synrgise Information Security Policy.
- Comply with legal and regulatory requirements such as **ISO 27001**, and conduct bi-annual compliance audits.

2. Roles and Responsibilities: Crisis Management Team (CMT)

A well-defined CMT ensures effective response to business disruptions.

2.1 IT Recovery Team

Name	Title	Roles and Responsibilities	Role in Plan
Xenothan Hojem	IT Manager	Oversee IT systems recovery	Plan Owner
Carlos Herrera	Database Analyst	Ensure data integrity	Data Specialist
Kevin Wallet / Xenothan Hojem	Server Technician	Restore server infrastructure	Server Specialist

Escalation Procedures:

- **Primary Contact:** IT Manager (Immediate response within 15 minutes)
- **Backup Contact:** Head of Operations
- **Communication Methods:** Slack, Email, SMS Alerts

2.2 Business Recovery Team

Name	Title	Roles and Responsibilities	Role in Plan
Chris Asals	Business Manager	Lead non-IT recovery efforts	Plan Owner
Chris Asals / Christine Taylor	HR Lead	Manage employee communications	HR
Philippe De Costa	Finance Lead	Ensure financial process continuity	Finance Specialist

Employee Awareness and Training: All CMT members must undergo quarterly business continuity training.

3. Business Impact Analysis

This analysis identifies potential disruption effects and mitigation strategies.

Department Function	Likelihood of Disruption	Business Impact	Risk Level	Mitigation Strategy
IT Infrastructure	Likely	High	Significant	Implement redundant backups, including off-site replication, automated failover systems, and periodic recovery testing to ensure data integrity.
Finance	Moderate	Major	Medium	Transition to cloud-based systems with multi-region failover, encrypted transactions, and continuous monitoring for financial integrity.
Operations	Rare	Severe	Low	Establish redundant sites with predefined operational workflows, ensuring minimal downtime and seamless operational handovers.

All business units must complete an impact assessment questionnaire every six months.

4. Response Plan

4.1 Unavailability of Site

Impacted Area	Action Plan	Responsible Role	Time to Execute
Office	Notify all staff, activate remote work plan via VPN, set up temporary communication channels (e.g., Microsoft Teams, Slack), and ensure access to critical applications. Conduct regular status updates every 2 hours.	Business Continuity Manager	1 hour
Data Center	Initiate switch to secondary data center, validate system integrity, confirm failover success, and monitor critical system performance. Regular updates provided every 30 minutes.	IT Manager	2 hours
Communications	Deploy alternative telecommunication solutions, including mobile hotspots and cloud-based communication platforms. Notify stakeholders and ensure contact lists are up to date.	Communications Lead	Immediate

4.2 Unavailability of Systems

Impacted System	Action Plan	Responsible Role	Recovery Time
Email Servers	Activate backup email system, notify staff of interim solutions, and monitor mail queues to prevent backlogs. Conduct periodic testing to confirm accessibility.	IT Manager	1 hour
CRM System	Switch to cloud-based CRM backup instance, validate data synchronization, and inform users of any functionality limitations. Provide a guide for manual operations if needed.	CRM Administrator	3 hours
File Storage	Restore from offsite backups, verify data integrity, and conduct a sample test to ensure files are accessible. Communicate restoration progress every hour.	IT Support Lead	4 hours

4.3 Unavailability of People

Key Role	Interim Arrangement	Responsible Activation	Recovery Time
IT Manager	Delegate tasks to IT Support Lead, reassign high-priority incidents, and ensure continuity of critical operations. Communicate role changes internally.	Head of Operations	1 hour
Finance Lead	Engage external accounting firm for temporary support, document financial operations, and ensure payroll continuity.	CFO	2 hours
HR Manager	HR Assistant to manage internal communications, track employee welfare, and liaise with department leads to minimize impact.	Head of HR	Immediate

5. Business Continuity Procedures

5.1 Fire or Physical Disaster

- **Immediate Actions:**
  - Ensure the fire alarm is triggered, and all personnel evacuate the premises following emergency exit routes.
  - Contact emergency services and notify the Crisis Management Team (CMT).
  - Assemble at designated muster points and conduct a headcount.
- **Secondary Actions:**
  - Assess the extent of damage and potential hazards with assistance from emergency responders.
  - Secure backup sites and arrange for temporary office space.
  - Retrieve data from offsite backups and initiate temporary operational workflows.
  - Communicate restoration timelines to stakeholders via multiple channels (email, SMS, company website).
  - Conduct a post-incident review and update continuity plans accordingly.

5.2 Cybersecurity Breach

- **Immediate Actions:**
  - Detect and contain the breach by isolating affected systems from the network.
  - Notify the Information Security Team and external cybersecurity consultants if necessary.
  - Perform forensic analysis to determine the scope and entry point of the breach.
- **Secondary Actions:**
  - Reset compromised credentials and enforce multi-factor authentication across affected systems.
  - Communicate breach details and recovery plans to internal teams and regulatory bodies.
  - Conduct user awareness training to prevent future incidents.
  - Implement enhanced monitoring tools to detect suspicious activity.
  - Perform a security audit and strengthen identified vulnerabilities.

5.3 Natural Disasters

- **Immediate Actions:**
  - Monitor local authorities for alerts and advisories.
  - Initiate emergency response protocols, including moving critical operations to safer locations.
  - Ensure staff safety and enable remote working where feasible.
- **Secondary Actions:**
  - Assess damage and liaise with property insurers for claims processing.
  - Relocate essential equipment and operations to backup sites.
  - Communicate status updates to employees, customers, and partners.
  - Activate support services for affected employees, such as counseling and transportation assistance.
  - Review disaster response effectiveness and update training programs accordingly.

6. Related Policies

- Synrgise Information Security Policy (Section 9: Business Continuity)
- Synrgise Information Security Policy - Data Backup
- Synrgise Information Security Policy - Incident Management
- Synrgise Information Security Policy - Access Control

7. Review and Maintenance

The Business Continuity Plan (BCP) requires ongoing review and maintenance to ensure its effectiveness and alignment with evolving business operations and potential risks. The following procedures outline the review and maintenance framework:

7.1 Annual Full-Scale Reviews

- Conduct a comprehensive review of the entire BCP to validate its relevance and effectiveness.
- Include all departments in the review process to ensure their specific continuity requirements are met.
- Update risk assessments and business impact analyses based on new threats, operational changes, and lessons learned from past incidents.
- Ensure compliance with regulatory standards, such as ISO 27001 and GDPR, by engaging external auditors if necessary.
- Submit a formal report detailing findings, recommendations, and action plans for the next review cycle.

7.2 Bi-Annual Testing of Business Continuity Drills

- Execute scenario-based drills twice a year, simulating different types of disruptions such as cyber incidents, natural disasters, and operational failures.
- Evaluate response times, decision-making processes, and staff preparedness during each drill.
- Document test results, identifying areas for improvement and required training.
- Incorporate lessons learned into the BCP and ensure corrective actions are implemented.

7.3 Monthly Automated Audits for Critical Services

- Implement automated tools to continuously monitor the health and availability of critical business systems.
- Audit backup integrity, failover capabilities, and system performance logs.
- Generate monthly reports highlighting potential vulnerabilities and maintenance needs.
- Assign responsibilities for resolving detected issues and track progress through an internal ticketing system.

7.4 Post-Incident Analysis and Documentation

- Conduct a structured review following each incident to assess the effectiveness of the response and recovery processes.
- Involve key stakeholders in a debriefing session to gather insights and feedback.
- Document findings in an incident report, detailing root causes, response timelines, impact assessments, and recommended improvements.
- Update the BCP based on lessons learned to enhance resilience and reduce future risks.
- Maintain a repository of past incidents and response evaluations to track trends and recurring issues.