Disaster Recovery Plan

Business Supplies Inc. (BSI)

Effective Date: October 3, 2024
Version: 1.1

Prepared by: CloudStrategik Consulting
Anderson@cloudstrategik.com

Confidentiality Statement

This document contains proprietary and confidential information of CloudStrategik Consulting and Business Supplies Inc. The information contained herein is disclosed to the recipient in confidence for the sole purpose of internal use. No part of this document may be disclosed, reproduced, or distributed without the prior written consent of CloudStrategik Consulting and Business Supplies Inc.

Contents

1 Introduction

1.1 Purpose

The purpose of this Disaster Recovery Plan (DRP) is to provide a structured approach for recovering Business Supplies Inc.'s (BSI) critical IT systems and data in the event of a major disaster or disruption. This plan aims to minimize downtime, data loss, and the overall impact on business operations.

1.2 Scope

This plan covers all critical IT systems, infrastructure, and data necessary for BSI's core business functions. It outlines procedures for various disaster scenarios, including but not limited to natural disasters, cyber-attacks, and infrastructure failures.

2 Disaster Recovery Team

2.1 Team Structure

- Disaster Recovery Coordinator
- IT Infrastructure Lead
- Applications Lead
- Data Recovery Specialist
- Network Specialist
- Communications Coordinator

2.2 Roles and Responsibilities

- **Disaster Recovery Coordinator:** Overall management of the recovery process
- **IT Infrastructure Lead:** Coordination of hardware and infrastructure recovery
- **Applications Lead:** Oversight of application and software recovery
- **Data Recovery Specialist:** Management of data backup and restoration
- **Network Specialist:** Restoration of network connectivity and services
- **Communications Coordinator:** Internal and external communication management

3 Risk Assessment and Business Impact Analysis

3.1 Potential Disasters

- Natural disasters (e.g., earthquakes, floods, fires)
- Cyber-attacks (e.g., ransomware, DDoS attacks)
- Infrastructure failures (e.g., power outages, hardware failures)
- Human-caused incidents (e.g., accidental data deletion, sabotage)

3.2 Critical Business Functions

1. Order processing and fulfillment
2. Inventory management
3. Financial operations
4. Customer service
5. Human resources management

3.3 Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)

System/Function	**RTO**	**RPO**
ERP System	4 hours	15 minutes
Email Server	2 hours	1 hour
File Servers	6 hours	1 hour
Customer Portal	4 hours	30 minutes
HR Management System	12 hours	4 hours

4 Disaster Recovery Strategies

4.1 Data Backup and Replication

- Implement a 3-2-1 backup strategy (3 copies, 2 different media, 1 off-site)
- Use real-time replication for critical systems
- Perform daily incremental and weekly full backups
- Store backup media in a secure, off-site location

4.2 Alternative Site

- Maintain a hot site for immediate failover of critical systems
- Establish a contract with a disaster recovery service provider for additional resources

4.3 Cloud-Based Recovery

- Utilize cloud services for backup storage and recovery
- Implement cloud-based disaster recovery solutions for key applications

4.4 Virtualization

- Use virtualization technologies to enable quick recovery and flexibility
- Maintain updated virtual machine images for rapid deployment

5 Disaster Recovery Procedures

5.1 Disaster Declaration

1. Assess the situation and determine if a disaster should be declared
2. Notify the Disaster Recovery Coordinator
3. Activate the Disaster Recovery Team
4. Inform executive management

5.2 Initial Response

1. Ensure personnel safety
2. Assess damage to IT infrastructure and systems
3. Activate alternative site if necessary
4. Establish communication channels for the recovery team

5.3 Recovery Execution

5.3.1 Infrastructure Recovery

1. Restore power and environmental controls
2. Set up network connectivity at the recovery site
3. Deploy necessary hardware (servers, storage, networking equipment)

5.3.2 Data Recovery

1. Retrieve backup media or access cloud-based backups
2. Verify backup integrity
3. Restore data according to predefined priorities

5.3.3 Application Recovery

1. Restore application servers and databases
2. Verify application functionality
3. Reconfigure applications for the recovery environment if necessary

5.3.4 Network Services Recovery

1. Restore internet connectivity
2. Configure firewalls and security appliances
3. Reestablish VPN connections

5.4 Testing and Verification

1. Conduct functionality tests for all recovered systems
2. Verify data integrity and consistency
3. Test network connectivity and performance
4. Validate integration between systems

5.5 Business Resumption

1. Notify users that systems are operational
2. Provide instructions for accessing recovered systems
3. Monitor system performance and address any issues
4. Gradually transition users back to the recovered environment

6 Communication Plan

6.1 Internal Communication

- Use predefined communication channels (e.g., emergency notification system)
- Provide regular updates to employees on recovery progress
- Establish a helpdesk for employee inquiries during the recovery process

6.2 External Communication

- Notify key customers and vendors of the situation
- Provide updates on service restoration timelines
- Coordinate with public relations team for media communications if necessary

7 Plan Testing and Maintenance

7.1 Testing Schedule

- Conduct full-scale disaster recovery tests annually
- Perform tabletop exercises quarterly
- Test individual recovery procedures on a rotating monthly basis

7.2 Plan Updates

- Review and update the plan annually
- Update the plan after any major system changes or organizational restructuring
- Incorporate lessons learned from tests and actual incidents

8 Appendices

8.1 Appendix A: Emergency Contact List Template

Name	**Role**	**Phone Number**	**Email**
[Full Name]	Disaster Recovery Coordinator	[Phone]	[Email]
[Full Name]	IT Infrastructure Lead	[Phone]	[Email]
[Full Name]	Applications Lead	[Phone]	[Email]
[Full Name]	Data Recovery Specialist	[Phone]	[Email]
[Full Name]	Network Specialist	[Phone]	[Email]
[Full Name]	Communications Coordinator	[Phone]	[Email]
[Full Name]	CEO	[Phone]	[Email]
[Full Name]	CIO	[Phone]	[Email]

8.2 Appendix B: Vendor Contact Information Template

Vendor Name	Service Provided	Contact Person	Phone Number	Email
[Vendor Name]	Cloud Services	[Contact Name]	[Phone]	[Email]
[Vendor Name]	Data Center	[Contact Name]	[Phone]	[Email]
[Vendor Name]	Network Provider	[Contact Name]	[Phone]	[Email]
[Vendor Name]	Hardware Supplier	[Contact Name]	[Phone]	[Email]
[Vendor Name]	Security Services	[Contact Name]	[Phone]	[Email]

8.3 Appendix C: System Recovery Priority List

System	RTO	RPO	Recovery Steps
ERP System	4 hours	15 minutes	1. Restore from latest backup 2. Verify data integrity 3. Test system functionality 4. Notify users
Email Server	2 hours	1 hour	1. Activate failover server 2. Restore recent emails 3. Test email flow 4. Update DNS if necessary
File Servers	6 hours	1 hour	1. Restore from backup 2. Verify file integrity 3. Test access permissions 4. Notify users
Customer Portal	4 hours	30 minutes	1. Restore web servers 2. Restore database 3. Test functionality 4. Update DNS if necessary
HR Management System	12 hours	4 hours	1. Restore application server 2. Restore database 3. Verify data integrity 4. Test functionality
Network Infrastructure	2 hours	N/A	1. Restore core switches and routers 2. Configure VLANs 3. Test connectivity 4. Enable external access

8.4 Appendix D: Disaster Recovery Checklist

1. **Immediate Response**

    Ensure personnel safety

    Assess the extent of the disaster

    Notify Disaster Recovery Coordinator

    Activate Disaster Recovery Team

    Declare disaster if criteria are met

    Notify executive management

2. **Activation of Recovery Site**

   Activate alternative site contract if necessary

   Dispatch team to recovery site

   Verify power and environmental controls at recovery site

   Establish secure communication channels

3. **Network Recovery**

   Set up core network infrastructure

   Configure and test internet connectivity

   Establish VPN connections

   Configure firewalls and security appliances

4. **Server and Data Recovery**

   Retrieve backup media or access cloud backups

   Verify integrity of backups

   Restore servers according to priority list

   Restore data to appropriate servers

   Verify data integrity and consistency

5. **Application Recovery**

   Restore application servers

   Restore databases

   Configure applications for recovery environment

   Test application functionality

   Verify integration between systems

6. **Testing and Verification**

   Conduct end-to-end testing of critical systems

   Verify network performance

   Test external connectivity and access

   Validate security controls

7. **Business Resumption**

   Notify users of system availability

   Provide access instructions to users

   Monitor system performance

   Address any issues reported by users

8. **Communication**

Update employees on recovery progress

Notify key customers and vendors

Coordinate with PR team for external communications

Establish helpdesk for user support

9. **Documentation**

Log all recovery activities

Document any issues encountered and resolutions

Record time taken for each recovery step

Prepare post-incident report

10. **Post-Recovery Actions**

Assess damage to primary site

Plan for transition back to primary site (if applicable)

Conduct post-incident review

Update Disaster Recovery Plan based on lessons learned

9 Document Revision History

Version	Date	Description of Changes	Author
1.0	10/03/2024	Initial document creation	A. Anthony
1.1	10/04/2024	Added detailed appendices	A. Anthony

10 Approval

This document has been reviewed and approved by:

Name: **Signature:**

Title: **Date:**

Name: **Signature:**

Title: **Date:**

11 Disclaimer

This Disaster Recovery Plan provides guidelines for recovering IT systems and data in the event of a major disaster. While it aims to address various scenarios, unforeseen circumstances may arise that are not explicitly covered. The Disaster Recovery Team should use their best judgment in conjunction with this plan when responding to specific incidents.

12 Contact Information

For any questions or clarifications regarding this Disaster Recovery Plan, please contact:

Name:	Anderson Anthony
Title:	Disaster Recovery Coordinator
Email:	Anderson@cloudstrategik.com
Phone:	+1 (555) 123-4567