

Halcyon Super Holdings B.V.

IT Disaster Recovery Plan
Version 1.2.1

Revision History

REVISION	DATE	NAME	DESCRIPTION
V1.0	9 August 2018	Head of Infrastructure	First Version
V1.1	5 June 2019	Head of Infrastructure	Minor updates to Appendix A – Technology Disaster Recovery Plan headings for clarity
V1.1.0	22 June 2020	Head of Infrastructure	Reviewed for currency
V1.1.1	9 June 2021	Head of Infrastructure	Reviewed for currency
V1.1.2	25 June 2022	Head of Infrastructure	Reviewed for currency
V1.1.3	2 June 2023	Head of Infrastructure	Reviewed for currency
V1.1.4	5 June 2024	Head of Infrastructure	Reviewed for currency
V1.2	16 June 2025	Head of Infrastructure	Updated to latest information: – Business IT vendors
V1.2.1	12 June 2026	Head of Infrastructure	Reviewed for currency

Table of Contents

Information Technology Statement of Intent	4
Policy Statement	4
Objectives	4
Key Personnel Contact Info	5
Notification Calling Tree	6
External Contacts	7
1 Plan Overview	8
1.1 Plan Updating	8
1.2 Plan Documentation Storage	8
1.3 Backup Strategy	8
1.4 Risk Management	10
2 Emergency Response	11
2.1 Alert, escalation and plan invocation	11
2.1.1 Plan Triggering Events	11
2.1.2 Assembly Points	11
2.1.3 Activation of Emergency Response Team	11
2.2 Disaster Recovery Team	11
2.3 Emergency Alert, Escalation and DRP Activation	11
2.3.1 Emergency Alert	12
2.3.2 DR Procedures for Management	12
2.3.3 Contact with Employees	12
2.3.4 Backup Staff	12
2.3.5 Recorded Messages / Updates	12
2.3.7 Alternate Recovery Facilities	13
2.3.8 Personnel and Family Notification	13
3 Media	14
3.1 Media Contact	14
3.2 Media Strategies	14
3.3 Media Team	14
3.4 Rules for Dealing with Media	14
4 Financial and Legal Issues	14
4.1 Financial Assessment	14
4.2 Financial Requirements	14
4.3 Legal Actions	14
5 DRP Exercising	15
Appendix A – Technology Disaster Recovery Plan	16
Disaster Recovery Plan for Gaming Platform (Customer-facing Services)	16
Disaster Recovery Plan for Local & Wide Area Networks (LAN & WAN)	18
Disaster Recovery Plan for Voice Communications	19
Appendix B – Suggested Forms	20
Damage Assessment Form	20
Management of DR Activities Form	20
Disaster Recovery Event Recording Form	21
Disaster Recovery Activity Report Form	21
Mobilizing the Disaster Recovery Team Form	22
Mobilizing the Business Recovery Team Form	22
Monitoring Business Recovery Task Progress Form	23
Preparing the Business Recovery Report Form	23
Communications Form	24
Returning Recovered Business Operations to Business Unit Leadership	24
Business Process/Function Recovery Completion Form	25

Information Technology Statement of Intent

This document delineates our policies and procedures for technology disaster recovery, as well as our process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This document summarizes our recommended procedures. In the event of an actual emergency, modifications to this document may be made to ensure physical safety of our people, our systems, and our data.

Our mission is to ensure information system uptime, data integrity and availability, and business continuity.

Policy Statement

Corporate management has approved the following policy statement:

- The company shall develop a comprehensive IT disaster recovery plan.
- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
- The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be kept up to date to take changing circumstances into account.

Objectives

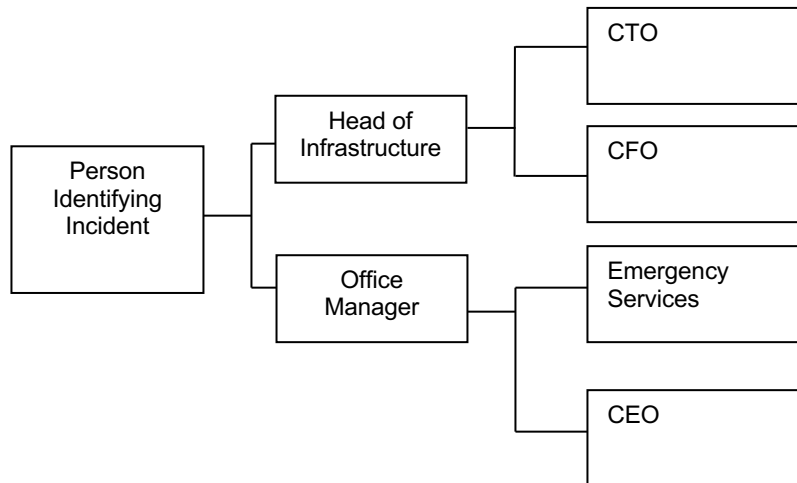
The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective
- The need to consider implications on other company sites
- Disaster recovery capabilities as applicable to key customers, vendors and others

Key Personnel Contact Info

Name, Title	Contact Option	Contact Number
Head of Infrastructure	Work	<Redacted for Security>
	Alternate	<Redacted for Security>
	Mobile	<Redacted for Security>
	Home	<Redacted for Security>
	Email Address	<Redacted for Security>
	Alternate Email	<Redacted for Security>
Office Manager	Work	<Redacted for Security>
	Alternate	<Redacted for Security>
	Mobile	<Redacted for Security>
	Home	<Redacted for Security>
	Email Address	<Redacted for Security>
	Alternate Email	<Redacted for Security>
CTO	Work	<Redacted for Security>
	Alternate	<Redacted for Security>
	Mobile	<Redacted for Security>
	Home	<Redacted for Security>
	Email Address	<Redacted for Security>
	Alternate Email	<Redacted for Security>
CFO	Work	<Redacted for Security>
	Alternate	<Redacted for Security>
	Mobile	<Redacted for Security>
	Home	<Redacted for Security>
	Email Address	<Redacted for Security>
	Alternate Email	<Redacted for Security>
CEO	Work	<Redacted for Security>
	Alternate	<Redacted for Security>
	Mobile	<Redacted for Security>
	Home	<Redacted for Security>
	Email Address	<Redacted for Security>
	Alternate Email	<Redacted for Security>

Notification Calling Tree



External Contacts

Name, Title	Contact Option	Contact Number
Landlord / Property Manager		
Account Number : N/A		
	Work	<Redacted for Security>
	Mobile	<Redacted for Security>
	Email Address	<Redacted for Security>
Power Company		
Account Number : <Redacted for Security>	Work	<Redacted for Security>
	Home	<Redacted for Security>
	Email Address	<Redacted for Security>
Telecom Carrier 1		
Account Number: <Redacted for Security>	Work	<Redacted for Security>
	Email Address	<Redacted for Security>
Workstation Supplier 1		
Account Number: <Redacted for Security>	Work	<Redacted for Security>
	Home	<Redacted for Security>
	Email Address	<Redacted for Security>
Insurance – Name		
Account Number: <Redacted for Security>	Work	<Redacted for Security>
	Email Address	<Redacted for Security>
Site Security		
Account Number: N/A	Work	<Redacted for Security>
	Email Address	<Redacted for Security>
Local Emergency Services		
Account Number: N/A	Public Toll Free	<Redacted for Security>

1 Plan Overview

1.1 Plan Updating

It is necessary for the DRP updating process to be properly structured and controlled. Whenever changes are made to the plan they are to be fully tested, and appropriate amendments should be made to the training materials. This will involve the use of formalized change control procedures under the control of the Head of Infrastructure.

1.2 Plan Documentation Storage

Copies of this Plan, and hard copies will be stored in secure locations to be defined by the company. Each member of senior management will be issued a soft and hard copy of this plan to be filed at home. Each member of the Disaster Recovery Team and the Business Recovery Team will be issued a soft and hard copy of this plan. A master protected copy will be stored on specific resources established for this purpose.

1.3 Backup Strategy

Key business processes and the agreed backup strategy for each are listed below.

Business IT

The company has chosen an IT strategy that intentionally uses business grade cloud-based Software as a Service (SaaS) solutions for all business IT functions to remove dependency on on-site IT infrastructure and associated backup requirements:

Google Workspace for Business:

- Productivity Suite (Google Docs, Sheets etc.)
- Document/File Storage
- Collaboration and Communication (Email, Conference calling etc.)

Slack:

- Company Instant Message System

Notion.com:

- Intranet

Intercom:

- Customer Help Desk

All essential staff members (Executives, Senior Managers and Key Operations Staff) have mobile workstations and mobile phones with broadband speed 4G/LTE subscriptions enabling them to work remotely during site disaster – either from home or any other location when required.

Customer-facing Services

All customer-facing services are hosted with leading Infrastructure as a Service (IaaS) cloud computing providers across multiple, physically separated and isolated availability zones providing geographic redundancy. Furthermore, all data is backed-up to multiple providers in case of catastrophic provider failure.

KEY BUSINESS PROCESS	BACKUP STRATEGY
IT Operations	Off-site SaaS. No dependency on on-site infrastructure
Tech Support - Hardware	Off-site SaaS. No dependency on on-site infrastructure
Tech Support - Software	Off-site SaaS. No dependency on on-site infrastructure
Facilities Management	Off-site SaaS. No dependency on on-site infrastructure
Email	Off-site SaaS. No dependency on on-site infrastructure
Purchasing	Off-site SaaS. No dependency on on-site infrastructure
Disaster Recovery	Off-site SaaS. No dependency on on-site infrastructure
Finance	Off-site SaaS. No dependency on on-site infrastructure
Contracts Admin	Off-site SaaS. No dependency on on-site infrastructure
Product Sales	Off-site SaaS. No dependency on on-site infrastructure
Human Resources	Off-site SaaS. No dependency on on-site infrastructure
Customer Service / Call Center	Off-site SaaS. No dependency on on-site infrastructure
Customer-facing services	Off-site SaaS & IaaS. No dependency on on-site infrastructure
Website	Off-site SaaS & IaaS. No dependency on on-site infrastructure

1.4 Risk Management

There are many potential disruptive threats which can occur at any time and affect normal business processes. We have considered a wide range of potential threats, and the results are detailed in this section. Each potential environmental disaster or emergency situation has been examined. The focus here is on the level of business disruption which could arise from each type of disaster.

Potential disasters have been assessed as follows:

Potential Disaster	Probability Rating	Impact Rating	Brief Description Of Potential Consequences & Remedial Actions
Flood	3	4	No critical equipment located on-site. Key staff can work remotely
Fire	3	4	No critical equipment located on-site. Key staff can work remotely Fire/smoke detectors and fire suppression systems on all floors for employee safety
Typhoon	2	4	No critical equipment located on-site. Key staff can work remotely
Tornado	5	4	No critical equipment located on-site. Key staff can work remotely
Electrical storms	5	4	No critical equipment located on-site. Key staff can work remotely
Act of terrorism	5	4	No critical equipment located on-site. Key staff can work remotely
Act of sabotage	5	4	No critical equipment located on-site. Key staff can work remotely
Electrical power failure	3	4	No critical equipment located on-site. Key staff can work remotely
Loss of communications network services	4	4	No critical equipment located on-site. Key staff can work remotely

Probability: 1=Very High, 5=Very Low

Impact: 1=Total destruction, 5=Minor annoyance

2 Emergency Response

2.1 Alert, escalation and plan invocation

2.1.1 Plan Triggering Events

Key trigger issues at headquarters that would lead to activation of the DRP are:

- Total loss of all communications
- Total loss of power
- Flooding of the premises
- Loss of the building

2.1.2 Assembly Points

Where the premises need to be evacuated, the DRP invocation plan identifies two evacuation assembly points:

- Primary – Assembly point in front of the building
- Alternate – In front of building across the street

2.1.3 Activation of Emergency Response Team

When an incident occurs the Emergency Response Team (ERT) must be activated. The ERT will then decide the extent to which the DRP must be invoked. All employees must be issued a Quick Reference card containing ERT contact details to be used in the event of a disaster.

Responsibilities of the ERT are to:

- Respond immediately to a potential disaster and call emergency services;
- Assess the extent of the disaster and its impact on the business;
- Decide which elements of the DR Plan should be activated;
- Establish and manage the disaster recovery team to maintain vital services and return to normal operation;
- Ensure employees are notified and allocate responsibilities and activities as required.

2.2 Disaster Recovery Team

The team will be contacted and assembled by the ERT. The team's responsibilities include:

- Establish facilities for an emergency level of service within 2.0 business hours;
- Restore key services within 4.0 business hours of the incident;
- Recover to business as usual within 8.0 to 24.0 hours after the incident;
- Coordinate activities with disaster recovery team, first responders, etc.
- Report to the emergency response team.

2.3 Emergency Alert, Escalation and DRP Activation

This policy and procedure has been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been established to ensure that communications can be quickly established while activating disaster recovery.

The DR plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology and business recovery. Suppliers of critical services will continue to support recovery of business operations as the company returns to normal operating mode.

2.3.1 Emergency Alert

The person discovering the incident calls a member of the Emergency Response Team in the order listed:

Emergency Response Team

- Office Manager
- Head of Infrastructure
- CTO (Chief Technology Officer)

If not available try:

- CFO (Chief Financial Officer)
- CEO (Chief Executive Officer)

The Emergency Response Team (ERT) is responsible for activating the DRP for disasters identified in this plan, as well as in the event of any other occurrence that affects the company's capability to perform normally.

One of the tasks during the early stages of the emergency is to notify the Disaster Recovery Team (DRT) that an emergency has occurred. The notification will request DRT members to assemble at the site of the problem and will involve sufficient information to have this request effectively communicated. The Business Recovery Team (BRT) will consist of senior representatives from the main business departments. The BRT Leader will be a senior member of the company's management team, and will be responsible for taking overall charge of the process and ensuring that the company returns to normal working operations as early as possible.

2.3.2 DR Procedures for Management

Members of the management team will keep a copy of the names and contact numbers of each employee in their departments. In addition, management team members will have a copy of the company's disaster recovery and business continuity plans on file in their homes in the event that the headquarters building is inaccessible, unusable, or destroyed.

2.3.3 Contact with Employees

Managers will serve as the focal points for their departments, while designated employees will call other employees to discuss the crisis/disaster and the company's immediate plans. Employees who cannot reach staff on their call list are advised to call the staff member's emergency contact to relay information on the disaster.

2.3.4 Backup Staff

If a manager or staff member designated to contact other staff members is unavailable or incapacitated, the designated backup staff member will perform notification duties.

2.3.5 Recorded Messages / Updates

For the latest information on the disaster and the organization's response, staff members can go to:

- #DR in the company instant message system (SaaS service, not hosted on-site, available on mobile)
- Disaster Recovery intranet page (SaaS service, not hosted on-site, available on mobile)

Included will be information on the nature of the disaster, assembly sites, and updates on work resumption.

2.3.7 Alternate Recovery Facilities

All essential staff members (Executives, Senior Managers and Key Operations Staff) have mobile workstations and mobile phones with broadband speed 4G/LTE subscriptions enabling them to work remotely during and after site disaster – either from home or any other location when required.

All non-essential staff members have mobile workstations enabling them to work from home in case of a disaster state at headquarters extending beyond 24 hours. In case of a prolonged disaster state at headquarters, procuring temporary office space and/or co-working space will be evaluated on a case-by-case basis.

2.3.8 Personnel and Family Notification

If the incident has resulted in a situation which would cause concern to an employee's immediate family such as hospitalization of injured persons, it will be necessary to notify their immediate family members quickly.

3 Media

3.1 Media Contact

Assigned staff will coordinate with the media, working according to guidelines that have been previously approved and issued for dealing with post-disaster communications.

3.2 Media Strategies

1. Avoiding adverse publicity
2. Take advantage of opportunities for useful publicity
3. Have answers to the following basic questions:
 - What happened?
 - How did it happen?
 - What are you going to do about it?

3.3 Media Team

- Communications Manager
- CCO (Chief Communications Officer)

3.4 Rules for Dealing with Media

Only the media team is permitted direct contact with the media; anyone else contacted should refer callers or in-person media representatives to the media team.

4 Financial and Legal Issues

4.1 Financial Assessment

The emergency response team shall prepare an initial assessment of the impact of the incident on the financial affairs of the company. The assessment should include:

- Loss of financial documents
- Loss of revenue
- Theft of check books, credit cards, etc.
- Loss of cash

4.2 Financial Requirements

The immediate financial needs of the company must be addressed. These can include:

- Cash flow position
- Temporary borrowing capability
- Upcoming payments for taxes, payroll taxes, Social Security, etc.
- Availability of company credit cards to pay for supplies and services required post-disaster

4.3 Legal Actions

The company legal department and ERT will jointly review the aftermath of the incident and decide whether there may be legal actions resulting from the event; in particular, the possibility of claims by or against the company for regulatory violations, etc.

5 DRP Exercising

Disaster recovery plan exercises are an essential part of the plan development process. In a DRP exercise no one passes or fails; everyone who participates learns from exercises – what needs to be improved, and how the improvements can be implemented. Plan exercising ensures that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities.

Successful DR plans launch into action smoothly and effectively when they are needed. This will only happen if everyone with a role to play in the plan has rehearsed the role. The plan should also be validated by simulating the circumstances within which it must work and seeing what happens.

Appendix A – Technology Disaster Recovery Plan

Disaster Recovery Plan for Gaming Platform (Customer-facing Services)

SYSTEM	GAMING PLATFORM
OVERVIEW	
PRODUCTION SYSTEM	Location: Primary Cloud Provider - Ireland Server Model: Kubernetes cluster running on elastic IaaS Operating System: CoreOS Container Linux CPUs: Elastic Memory: Elastic Total Disk: Elastic System Handle: Gaming Platform System Serial #: N/A DNS Entry: www.cloudbet.com IP Address: elastic Other:
HOT SITE	N/A – service is natively geographically redundant (Multi-AZ)
APPLICATIONS (Use bold for Hot Site)	Customer API Back-office API Casino Transactions API Sports API
ASSOCIATED SERVERS	N/A
KEY CONTACTS	
Hardware Vendor	N/A – SaaS & IaaS Services
System Owners	CTO, Head of Infrastructure
Database Owner	Head of Infrastructure
Application Owners	Front-end Team Lead, Back-office Team Lead, Casino Team Lead, Sports Team Lead
Software Vendors	Primary Cloud Provider
Offsite Storage	Secondary Cloud Provider
BACKUP STRATEGY FOR GAMING PLATFORM	
Daily	- All production databases have replicated standby instances - All databases are backed up daily with recovery logs allowing point-in-time recovery - All databases are backed-up offsite daily with Secondary Cloud Provider
Monthly	Monthly backup is kept for the last 12 months
Quarterly	See Monthly

GAMING PLATFORM DISASTER RECOVERY PROCEDURE	
<u>Scenario 1</u> Total Loss of Data	Restore latest available database backup in this order: - Local database backup with Primary Cloud Provider - Offsite backup from Secondary Cloud Provider
<u>Scenario 2</u> Total Loss of HW	Deploy new Kubernetes cluster infrastructure at best available option in this order: - Primary Cloud Provider, primary geographic region if failure is localized - Primary Cloud Provider, secondary geographic region if failure affects entire region - Secondary Cloud Provider for catastrophic provider failure (very low probability) Restore latest available database backup in this order: - Local database backup with Primary Cloud Provider - Offsite backup from Secondary Cloud Provider

ADDENDUM

CONTACTS	CTO
	Head of Infrastructure
	Platform Team
	Front-end Team Lead
	Back-office Team Lead
	Casino Team Lead
	Sports Team Lead

Disaster Recovery Plan for Local & Wide Area Networks (LAN & WAN)

SYSTEM	HQ OFFICE NETWORK
---------------	--------------------------

OVERVIEW	
EQUIPMENT	Location: Headquarters Device Type: PPPoE Router Model No.: <Redacted for Security> Technical Specifications: <Redacted for Security> Network Interfaces: <Redacted for Security> Power Requirements: <Redacted for Security> System Serial #: <Redacted for Security> DNS Entry: N/A IP Address: <Redacted for Security> Other:
HOT SITE EQUIPMENT	N/A
SPECIAL APPLICATIONS	N/A
ASSOCIATED DEVICES	N/A

KEY CONTACTS	
Hardware Vendor	<Redacted for Security>
System Owners	Head of Infrastructure
Database Owner	N/A
Application Owners	N/A
Software Vendors	N/A
Offsite Storage	N/A
Network Services	Head of Infrastructure

BACKUP STRATEGY for HQ OFFICE NETWORK	
Daily	Router configuration is backed up daily
Monthly	N/A
Quarterly	N/A

HQ OFFICE NETWORK DISASTER RECOVERY PROCEDURE	
<u>Scenario 1</u> Total Loss of Network	Essential staff use company mobile phones with broadband speed 4G/LTE subscriptions
<u>Scenario 2</u> Total Loss of HW	Essential staff use company mobile phones with broadband speed 4G/LTE subscriptions Deploy backup router to restore service

Disaster Recovery Plan for Voice Communications

SYSTEM	VOICE COMMUNICATION
OVERVIEW	
EQUIPMENT	Location: Off-site SaaS (Google Workspace for Business) Device Type: - Google Workspace for Business - Company mobile phones Model No.: N/A Technical Specifications: N/A Network Interfaces: N/A Power Requirements: N/A System Serial #: N/A DNS Entry: N/A IP Address: N/A Other: N/A
HOT SITE EQUIPMENT	N/A - Off-site SaaS (Google Workspace for Business)
SPECIAL APPLICATIONS	None
ASSOCIATED DEVICES	None
KEY CONTACTS	
Hardware Vendor	N/A - Off-site SaaS (Google Workspace for Business)
System Owners	Head of Infrastructure
Database Owner	N/A
Application Owners	N/A
Software Vendors	Google Workspace Account Manager
Offsite Storage	Head of Infrastructure
Network Services	Head of Infrastructure
BACKUP STRATEGY for VOICE COMMUNICATIONS	
Daily	N/A - Off-site SaaS (Google Workspace for Business)
Monthly	N/A - Off-site SaaS (Google Workspace for Business)
Quarterly	N/A - Off-site SaaS (Google Workspace for Business)
VOICE COMMUNICATION DISASTER RECOVERY PROCEDURE	
<u>Scenario 1</u> Total Loss of Switch	N/A - Off-site SaaS (Google Workspace for Business)
<u>Scenario 2</u> Total Loss of Network	N/A - Off-site SaaS (Google Workspace for Business) Essential staff use company mobile phones with broadband speed 4G/LTE subscriptions

Appendix B – Suggested Forms

Damage Assessment Form

Key Business Process Affected	Description Of Problem	Extent Of Damage

Management of DR Activities Form

- During the disaster recovery process all activities will be determined using a standard structure;
- Where practical, this plan will need to be updated on a regular basis throughout the disaster recovery period;
- All actions that occur during this phase will need to be recorded.

Activity Name:
Reference Number:
Brief Description:

Commencement Date/Time	Completion Date/Time	Resources Involved	In Charge

Disaster Recovery Event Recording Form

- All key events that occur during the disaster recovery phase must be recorded.
- An event log shall be maintained by the disaster recovery team leader.
- This event log should be started at the commencement of the emergency and a copy of the log passed on to the business recovery team once the initial dangers have been controlled.
- The following event log should be completed by the disaster recovery team leader to record all key events during disaster recovery, until such time as responsibility is handed over to the business recovery team.

Description of Disaster:
Commencement Date:
Date/Time DR Team Mobilized:

Activities Undertaken by DR Team	Date and Time	Outcome	Follow-On Action Required

Disaster Recovery Team's Work Completed: <Date>
Event Log Passed to Business Recovery Team: <Date>

Disaster Recovery Activity Report Form

- On completion of the initial disaster recovery response the DRT leader should prepare a report on the activities undertaken.
- The report should contain information on the emergency, who was notified and when, action taken by members of the DRT together with outcomes arising from those actions.
- The report will also contain an assessment of the impact to normal business operations.
- The report should be given to business recovery team leader, with a copy to senior management, as appropriate.
- A disaster recovery report will be prepared by the DRT leader on completion of the initial disaster recovery response.
- In addition to the business recovery team leader, the report will be distributed to senior management

The report will include:

- A description of the emergency or incident
- Those people notified of the emergency (including dates)
- Action taken by members of the DRT
- Outcomes arising from actions taken
- An assessment of the impact to normal business operations
- Assessment of the effectiveness of the BCP and lessons learned
- Lessons learned

Mobilizing the Disaster Recovery Team Form

- Following an emergency requiring recovery of technology infrastructure assets, the disaster recovery team should be notified of the situation and placed on standby.
- The format shown below can be used for recording the activation of the DR team once the work of the damage assessment and emergency response teams has been completed.

Description of Emergency:					
Date Occurred:					
Date Work of Disaster Recovery Team Completed:					
Name of Team Member	Contact Details	Contacted On (Time / Date)	By Whom	Response	Start Date Required
Relevant Comments (e.g., Specific Instructions Issued)					

Mobilizing the Business Recovery Team Form

- Following an emergency requiring activation of the disaster recovery team, the business recovery team should be notified of the situation and placed on standby.
- The format shown below will be used for recording the activation of the business recovery team once the work of the disaster recovery team has been completed.

Description of Emergency:					
Date Occurred:					
Date Work of Business Recovery Team Completed:					
Name of Team Member	Contact Details	Contacted On (Time / Date)	By Whom	Response	Start Date Required
Relevant Comments (e.g., Specific Instructions Issued)					

Monitoring Business Recovery Task Progress Form

- The progress of technology and business recovery tasks must be closely monitored during this period of time.
- Since difficulties experienced by one group could significantly affect other dependent tasks it is important to ensure that each task is adequately resourced and that the efforts required to restore normal business operations have not been underestimated.

Note: A priority sequence must be identified although, where possible, activities will be carried out simultaneously.

Recovery Tasks (Order of Priority)	Person(s) Responsible	Completion Date		Milestones Identified	Other Relevant Information
		Estimated	Actual		
1.					
2.					
3.					
4.					
5.					
6.					
7.					

Preparing the Business Recovery Report Form

- On completion of business recovery activities the BRT leader should prepare a report on the activities undertaken and completed.
- The report should contain information on the disruptive event, who was notified and when, action taken by members of the BRT together with outcomes arising from those actions.
- The report will also contain an assessment of the impact to normal business operations.
- The report should be distributed to senior management, as appropriate.

The contents of the report shall include:

- A description of the incident
- People notified of the emergency (including dates)
- Action taken by the business recovery team
- Outcomes arising from actions taken
- An assessment of the impact to normal business operations
- Problems identified
- Suggestions for enhancing the disaster recovery and/or business continuity plan
- Lessons learned

Communications Form

- It is very important during the disaster recovery and business recovery activities that all affected persons and organizations are kept properly informed.
- The information given to all parties must be accurate and timely.
- In particular, any estimate of the timing to return to normal working operations should be announced with care.
- It is also very important that only authorized personnel deal with media queries.

Groups of Persons or Organizations Affected by Disruption	Persons Selected To Coordinate Communications to Affected Persons / Organizations		
	Name	Position	Contact Details
Customers			
Management & Staff			
Suppliers			
Media			
Stakeholders			
Others			

Returning Recovered Business Operations to Business Unit Leadership

- Once normal business operations have been restored it will be necessary to return the responsibility for specific operations to the appropriate business unit leader.
- This process should be formalized in order to ensure that all parties understand the change in overall responsibility, and the transition to business-as-usual.
- It is likely that during the recovery process, overall responsibility may have been assigned to the business recovery process lead.
- It is assumed that business unit management will be fully involved throughout the recovery, but in order for the recovery process to be fully effective, overall responsibility during the recovery period should probably be with a business recovery process team.

Business Process/Function Recovery Completion Form

The following transition form should be completed and signed by the business recovery team leader and the responsible business unit leader, for each process recovered.

A separate form should be used for each recovered business process.

Name Of Business Process	
Completion Date of Work Provided by Business Recovery Team	
Date of Transition Back to Business Unit Management <i>(If different than completion date)</i>	
I confirm that the work of the business recovery team has been completed in accordance with the disaster recovery plan for the above process, and that normal business operations have been effectively restored. Business Recovery Team Leader Name: _____ Signature: _____ Date: _____ <i>(Any relevant comments by the BRT leader in connection with the return of this business process should be made here.)</i>	
I confirm that above business process is now acceptable for normal working conditions. Name: _____ Title: _____ Signature: _____ Date: _____	