

Disaster Recovery Plan (DRP)

Datacenter in Curaçao

1. Objectives

Purpose: Ensure the quick and effective recovery of the datacenter to minimize business disruption.

Goals:

1. Protect critical data and infrastructure.
2. Restore essential services within predefined timelines.
3. Maintain effective communication during and after a disaster.

2. Key Contacts

Role	Name	Phone	Email	Backup Contact
Director of IT	Larry Gonzalez	XXXXX	larry.gonzalez@chancers.com	IT@chancers.com
Compliance Officer	Mario Rodriguez	XXXXX	mario.rodriguez@chancers.com	IT@chancers.com

3. Critical Systems

System	Priority	RTO	RPO	Backup Method
Virtual Machines	High	2 hours	15 mins	Daily full, real-time syncing
Databases	High	2 hours	15 mins	Daily full, real-time syncing
Secondary systems	High	2 hours	15 mins	Daily full, real-time syncing

4. Risk Assessment

Threat	Probability	Impact	Mitigation Strategy
Power Outage	High	High	Backup generators, UPS systems

Flooding	Medium	High	Backup generators, UPS systems
Earthquake	Medium	High	Backup generators, UPS systems

5. Recovery Procedures

Scenario 1: Power Outage

Actions:

4. 1. Switch to backup generators.
5. 2. Verify UPS systems are functional.
6. 3. Notify key personnel of the situation.

Scenario 2: Hardware Failure

Actions:

7. 1. Replace failed component with on-site spare.
8. 2. If unavailable, escalate to vendor support.
9. 3. Restore system from backups if data integrity is compromised.

Scenario 3: Hurricane Impact

Actions:

10. 1. Evacuate personnel if necessary.
11. 2. Assess physical damage and prioritize repairs.
12. 3. Activate hot-site recovery if primary site is unusable.

6. Backup Strategy

Backup Type	Frequency	Location
Virtual Machines	Weekly	Off-site storage/cloud
Databases	Weekly	Off-site storage/cloud
Secondary systems	Weekly	Off-site storage/cloud

7. Communication Plan

Audience	Channel	Frequency	Responsible Party
Internal Teams	Email, Messaging	As needed	DRP Coordinator

8. Testing and Maintenance

Testing Schedule: Quarterly tabletop exercises, semi-annual full recovery simulations.

Maintenance: Review and update plan annually or after major incidents.

Key Metrics: Time to restore systems, data recovery accuracy.

9. Internet Failover Plan

Purpose: To ensure continuous internet connectivity during provider outages. The following failover plan is designed to minimize disruptions to critical services and operations.

Failover Configuration

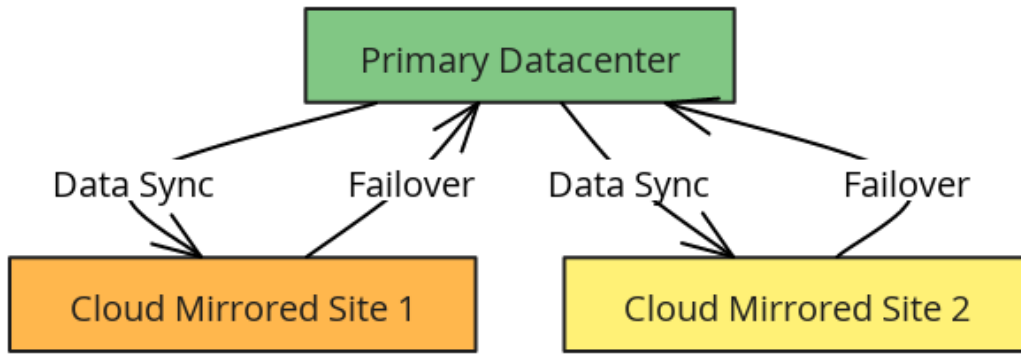
Provider	Connection Type	Priority	Failover Mechanism
ISP1	Fiber	Primary	Automatic failover via router configuration
ISP2	4G LTE	Secondary	Automatic failover for emergency use
ISP3	Satellite	Tertiary	Manual activation when primary and secondary fail

Failover Steps

13. 1. Monitor the health of all internet connections using automated tools (e.g., network monitoring software).
14. 2. When a failure is detected in the primary connection:
 - Automatically switch to the secondary connection if configured.
 - Notify the IT team and internet service provider for resolution.
15. 3. If the secondary connection also fails, activate the tertiary connection manually.
16. 4. Document the outage and actions taken for future reference.

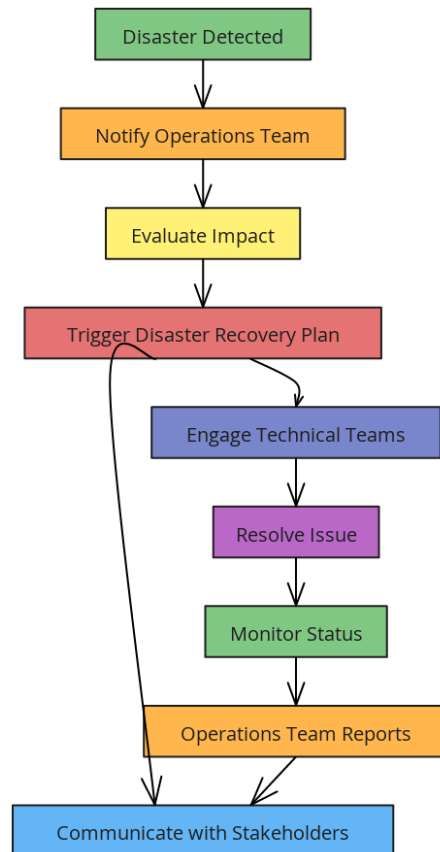
6.1 Datacenter Failover to Cloud Sites

The diagram below illustrates the failover strategy from the primary datacenter to cloud mirrored sites. This ensures continuity of operations in the event of a disaster affecting the primary datacenter.



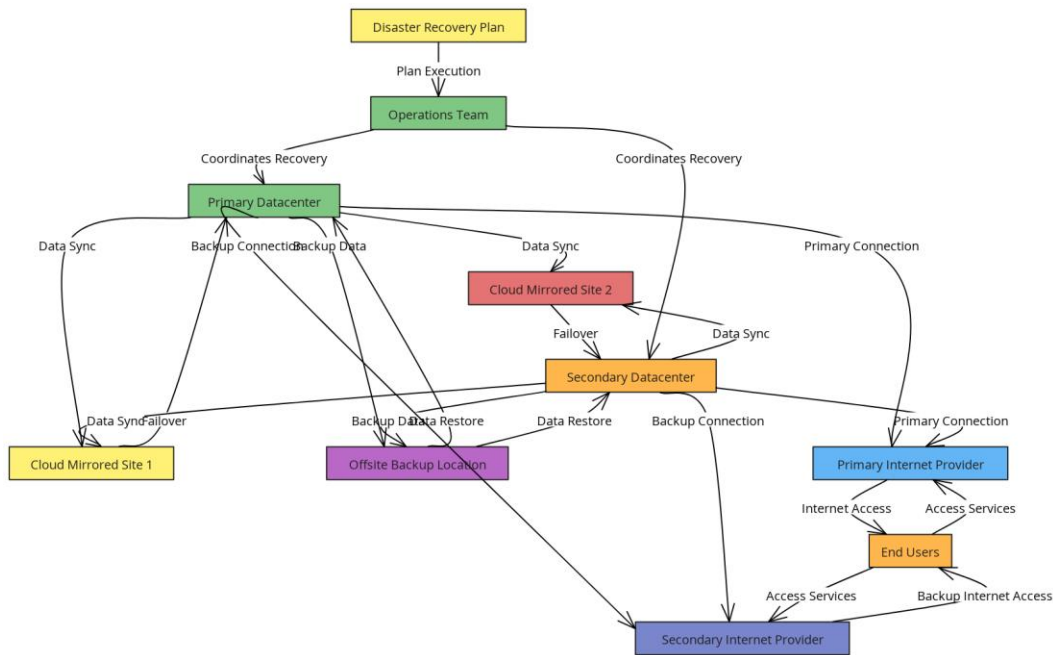
5.1 Disaster Response Flowchart

This flowchart outlines the steps to be taken when a disaster is detected. It ensures a structured and efficient response, covering notification, impact evaluation, recovery plan execution, and communication with stakeholders.



9.1 Internet Failover Channels

The following diagram demonstrates the use of multiple internet service providers (ISPs) to ensure failover capabilities and continuous connectivity during an ISP outage. This redundancy mitigates risks of losing internet access for critical services.



4.1 Failover and Data Synchronization

The diagram below showcases the synchronization and failover setup between the primary datacenter and backup locations. This ensures data integrity and accessibility during disaster scenarios.

