Disaster Recovery Plan

Doc. Control Number	Version
SNL-63	0.2

Document Reference

Item	Description
Title	Disaster Recovery Plan
Department	Cybersecurity department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	9 September 2023
Revision-Date	9 September 2024

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	5/9/2023

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	9/9/2023

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	9/9/2023

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	Sep 2023	Muhaned Ali	First Release
0.2	11 Aug 2024	Muhaned Ali	The document has been reviewed

Contents

1. Purpose

The purpose of this Disaster Recovery (DR) Plan is to ensure the organization's ability to recover assets and establish effective communication following a major disruption to business operations. This plan outlines the procedures and responsibilities for recovering critical systems, data, and communication channels.

2. Scope

This plan applies to all departments, personnel, and facilities within the organization. It encompasses the recovery of assets and the restoration of communication channels.

3. Plan Maintenance and Communication

3.1 Responsible Parties

a) The DR Plan will be maintained and updated by the designated DR team. Updates and changes will be communicated to all relevant stakeholders.

3.2 Frequency of Updates

a) The DR Plan will be reviewed and updated annually, or as significant changes occur in the SNLC's infrastructure or operations.

4. Risk Management

There are many potential disruptive threats which can occur at any time and affect the normal business process. We have considered a wide range of potential threats, and the results of our deliberations are included in this section. Each potential environmental disaster or emergency 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	All critical equipment is located on 2nd Floor
Fire	3	4	FM200 suppression system installed in main computer centers. Fire and smoke detectors on all floors.
Tornado	5		
Electrical storms	5		
Equipment failure incident	3	3	Replace the failure hardware immediately.
Act of terrorism	5		
Act of sabotage	5		
Electrical power failure	3	4	Redundant UPS array together with auto standby generator that is tested weekly & remotely monitored 24/7. UPSs also remotely monitored.
Loss of communications network services	4	4	WAN redundancy, voice network resilience
Loss of VSAT Network services	4	4	**Hub Chassis:** Can host up to 20 Line Cards and it supports up to five satellites comes with two power supply units and two GPS modules working as 1+1 for redundancy hot failover. Spare Chassis is available On-site and pre-configured as standby. **Two Protocol Processor (PP) servers:** each PP can handle up to 250 remote sites, and they are Working as 1+1 with load balance techniques to handle remote traffic acceleration. **Two Network Management System (NMS) servers:** Our network is running with one primary NMS and one Back up NMS are synchronized with each other containing all remotes and network database and configurations data.

Probability: 1=Very High, 5=Very Low

Impact: 1=Destruction, 5=Minor annoyance

5. Emergency Response

5.1 Alert, escalation, and plan invocation

a) Plan Triggering Events

Key trigger issues at HUB, and SNL branches that would lead to activation of the DRP are:

- Total loss of all VSAT communications.
- Total loss of all Network communications.
- Total loss of power.
- Flooding of the premises
- Loss of the building
- Equipment failure incident

5.2 Activation of Emergency Response Team

a) 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, data center, etc.
- Decide which elements of the DR Plan should be activated.
- Establish and manage disaster recovery team to maintain vital services and return to normal operation.
- Ensure employees are notified and allocate responsibilities and activities as required.

5.3 Disaster Recovery Team

a) 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.

6. DR Procedures

6.1 Equipment failure incident

Types of incidents e.g.: Fire, flood, Earthquake.

a) Disaster Recovery Plan

- Task 01- Immediate Response

  This task provides the necessary command and control to enable the SNLC Incident Response Team to conduct an initial assessment of the Disaster and to co-ordinate SNLC's initial response to the disaster.

  Incident Response Team

Team Leader	Team Members
V.P	CTO
	Business Development Director
	Managed Service Director
	Health, Safety and Environment Dept
	Cyber Security Dept

Incident Response Team Leader to: Steps to be undertaken:

- In case of an equipment failure incident, promptly identify the issue through monitoring systems, alerts, or reports from affected employees.
- The IT team, along with relevant personnel, assesses the nature and severity of the equipment failure, including its impact on critical business functions.

- Ensure the safety of personnel in the vicinity of equipment failure. Follow any safety protocols or evacuation procedures if necessary.
- If the equipment failure poses a risk to other systems or equipment, isolate the affected area to prevent further damage or data loss.
- Document the incident, including the date, time, location, affected equipment, and initial assessment.
- Notify relevant stakeholders, including IT team members, department heads, and management, about the incident. Establish a clear communication chain for updates.
- Task 02- Commence operations from Backup Spare parts

This job outlines the actions required to begin core SNLC operations from the alternate equipment spare part.

Incident Response Team

Team Leader	Team Members
V.P	CTO
	Business Development Director
	Managed Service Director
	Health, Safety and Environment Dept
	Cyber Security Dept

Recovery Procedure

Steps to be taken:

- The business owner shall arrange for the replacement or repair of the faulty equipment. Coordinate with vendors or suppliers for replacement parts or equipment.
- Restore data from backups as per the established backup and recovery procedures. Verify data integrity and completeness.

Recovery Time Objective

- This task must be completed within 24 hours after the incident. This is determined by the criticality of the equipment.

Recovery Location

- Riyadh Office / Khobar Office

6.2 Disruption of power supply

a) Disaster Recovery Plan

- Task 01 Immediate Response

This task provides the necessary command and control to enable the SNLC Incident Response Team to conduct an initial assessment of the Disaster and to co-ordinate SNLC's initial response to the disaster.

Incident Response Team

Team Leader	Team Members
V.P	CTO
	Business Development Director
	Managed Service Director
	Health, Safety and Environment Dept
	Cyber Security Dept

Recovery Procedure

- In the event of a power supply, identify the issue through monitoring systems, alarms, or reports from affected employees.
- The IT and Facilities teams, in coordination with relevant personnel, assess the nature and scope of the disruption, including its impact on critical business functions.
- Ensure the safety of personnel in affected areas. If necessary, follow safety protocols, including evacuation procedures.

- Take immediate steps to mitigate the impact, by activating backup power sources.
- Document the incident, including the date, time, location, affected systems, and initial assessment.
- Notify relevant stakeholders, including IT team members, department heads, and management, about the incident.
- Task 02- Commence operations from Backup UPS

  This job outlines the actions required to begin core SNLC operations from the alternate power source.
- Incident Response Team

Team Leader	Team Members
V.P	CTO
	Business Development Director
	Managed Service Director
	Health, Safety and Environment Dept
	Cyber Security Dept

Recovery Procedure

Steps to be taken:

- Determine the cause of the power supply disruption, whether it's an internal issue, external grid failure, or other factors.
- If backup power sources (e.g., generators, uninterruptible power supplies) are available, activate them to maintain essential operations.
- If the disruption is due to internal issues, coordinate with relevant vendors or technicians for repairs. In the case of external grid failures, monitor updates from utility providers regarding restoration timelines.
- Conduct testing to verify the functionality of power.

Recovery Time Objective

- This task must be completed within 24 hours after the incident. This is determined by the criticality of the equipment.

Recovery Location

- Riyadh Office / Khobar Office

6.3 Application Failure or Corruption of Database

a) Disaster Recovery Plan

- Task 01 Immediate Response

  This task provides the necessary command and control to enable the SNLC Incident Response Team to conduct an initial assessment of the Disaster and to co-ordinate SNLC's initial response to the disaster.
- Incident Response Team

Team Leader	Team Members
V.P	CTO
	Business Development Director
	Managed Service Director
	IT Dept
	Cyber Security Dept

Recovery Procedure

- The IT team, in coordination with relevant personnel, assesses the nature and scope of the issue, including its impact on critical business functions.
- Ensure the safety of personnel and data during the recovery process. Isolate affected systems to prevent further damage.

- Document the incident, including the date, time, location, affected systems, and initial assessment.
- Notify relevant stakeholders, including IT team members, department heads, and management, about the incident.
- The IT team conducts a detailed assessment to determine the cause of the application failure or database corruption.
- Task02 Commence operations from the Backup storage.

  This task provides the necessary steps to commence core SNLC operations from the Backup storage.
- Incident Response Team

Team Leader	Team Members
V.P	CTO
	Business Development Director
	Managed Service Director
	IT Dept
	Cyber Security Dept

Recovery Procedure

Steps to be taken:

- The IT Team must alert the Cybersecurity Department for a thorough investigation.
- The IT Team must recover the backup for database corruption.
- The IT Team must validate the backup process.
- The Cybersecurity Team must validate the data's integrity.

Recovery Time Objective

- This task must be completed within 24 hours after the incident. This is determined by the criticality of the equipment.

Recovery Location

- Riyadh Office / Khobar Office

6.4 Human Error, Sabotage, or Strike

a) Disaster Recovery Plan

- Task 01 Immediate Response

  This task provides the necessary command and control to enable the SNLC Incident Response Team to conduct an initial assessment of the Disaster and to co-ordinate SNLC's initial response to the disaster.
- Incident Response Team

Team Leader	Team Members
V.P	CTO
	Business Development Director
	Managed Service Director
	IT Dept
	Cyber Security Dept
	HR Dept

Recovery Procedure

- The IT Team shall assess the nature and scope of the incident, including its impact on critical business functions and the potential threat to personnel and assets.
- Ensure the safety of personnel and assets. Follow safety protocols, including evacuation procedures, if necessary.
- Isolate affected systems or areas to prevent further damage or compromise.
- Document the incident, including the date, time, location, affected areas, and initial assessment.

- Notify relevant stakeholders, including department heads, security personnel, and management, about the incident. Establish a clear communication chain for updates.
- Task 02 Fix the issue.

  This task is to resolve the problem and restore normalcy.
- Incident Response Team

Team Leader	Team Members
V.P	CTO
	Business Development Director
	Managed Service Director
	IT Dept
	Cyber Security Dept
	HR Dept

Recovery Procedure

Steps to be taken:

- Initiate an investigation into the incident to determine its cause, whether it was human error, sabotage, or related to a strike action.
- Evaluate the impact on critical business functions, infrastructure, and personnel. Assess the extent of the damage or disruption.
- Contact police
- Replace any impacted devices.
- The IT team will ensure that everything is back to normal.

Recovery Time Objective

- This task must be completed within 24 hours after the incident. This is determined by the criticality of the equipment.

Recovery Location

- Riyadh Office / Khobar Office

6.5 Malicious Software Attack, Hacking or Other Internet Attacks

a) Disaster Recovery Plan

- Task 01 Immediate Response

  This task provides the necessary command and control to enable the SNLC Incident Response Team to conduct an initial assessment of the Disaster and to co-ordinate SNLC's initial response to the disaster.
- Incident Response Team

Team Leader	Team Members
V.P	CTO
	Business Development Director
	Managed Service Director
	IT Dept
	Cyber Security Dept

Recovery Procedure

- The INFOSEC team, in coordination with relevant personnel, assesses the nature and scope of the attack, including its impact on critical business functions and potential data breaches.
- Immediately isolate affected systems or networks to prevent the spread of malware or unauthorized access.
- INFOSEC shall Implement containment measures to stop the attack from further compromising systems or data.
- Document the incident, including the date, time, location, affected systems, and initial assessment.

- Notify relevant stakeholders, including department heads, IT security personnel, legal counsel, and management, about the incident.
- INFOSEC shall Initiate a forensic investigation to determine the source, extent, and method of the attack.
- Evaluate the impact on critical business functions, data breaches, and potential data loss.
- Task 02 Recovery Actions
- Incident Response Team

Team Leader	Team Members
V.P	CTO
	Business Development Director
	Managed Service Director
	IT Dept
	Cyber Security Dept

Recovery Procedure

Steps to be taken:

- INFOSEC shall Implement immediate measures to stop the attack and prevent further damage, such as disabling compromised accounts or disconnecting affected systems from the network.
- IT team shall Restore affected systems from known clean backups. Ensure backups are validated for integrity and completeness.
- INFOSEC Team shall review and enhance security measures, including firewall rules, intrusion detection systems, and access controls.
- The IT Team shall apply patches and updates to vulnerable systems to prevent future exploitation.

Recovery Time Objective

- This task must be completed within 12 hours after the incident. This is determined by the criticality of the equipment.

Recovery Location

Riyadh Office / Khobar Office

6.6 Social Unrest or Terrorist Attacks

a) Disaster Recovery Plan

- Task 01 Immediate Response

This task provides the necessary command and control to enable the SNLC Incident Response Team to conduct an initial assessment of the Disaster and to co-ordinate SNLC's initial response to the disaster.

Incident Response Team

Team Leader	Team Members
V.P	CTO
	Business Development Director
	Managed Service Director
	IT Dept
	Cyber Security Dept
	HR Dept

Recovery Procedure

- Security personnel, in coordination with relevant authorities and personnel, assess the nature and scope of the incident, including its impact on critical business functions, personnel safety, and infrastructure damage.

- Ensure the safety of all personnel. Follow safety protocols, including immediate evacuation or shelter-in-place procedures, if necessary.
- If required, initiate a safe and orderly evacuation of personnel from affected areas to designated assembly points.
- Document the incident, including the date, time, location, affected areas, and initial assessment.
- The IT Team shall assess the extent of damage to infrastructure, facilities, and critical assets.
- Task 02 Recovery Actions
- Incident Response Team

Team Leader	Team Members
V.P	CTO
	Business Development Director
	Managed Service Director
	IT Dept
	Cyber Security Dept
	HR Dept

Recovery Procedure

Steps to be taken:

- Provide medical assistance to injured personnel and coordinate with local medical services for additional support.
- INFOSEC shall review and enhance security measures, including access controls, surveillance, and perimeter security, to prevent further incidents.
- Collaborate with local law enforcement and relevant authorities to ensure security and investigate the incident.
- If necessary, HR shall establish temporary work locations to continue critical business functions.

Recovery Time Objective

- This task must be completed within 1 weeks after the incident.

Recovery Location

- Riyadh Office / Khobar Office

6.7 Environmental Disasters

a) Disaster Recovery Plan

- Task 01 Immediate Response

This task provides the necessary command and control to enable the SNLC Incident Response Team to conduct an initial assessment of the Disaster and to co-ordinate SNLC's initial response to the disaster.

Incident Response Team

Team Leader	Team Members
V.P	CTO
	Business Development Director
	Managed Service Director
	IT Dept
	Cyber Security Dept
	HR Dept
	Health, Safety and Environment Dept

Recovery Procedure

Incident Response Team Leader to: Steps to be undertaken:

- Ensure site has been evacuated.

- Secure site and prevent access.
- Contact emergency services and police.
- Identify any injuries and render assistance.
- Undertake an initial assessment of damage and risks.
- Instigate the “Complete Hardware failure” response plan.
- Determine time frame to switch to disaster recovery site.

<u>Recovery Time Objective</u>

- The timeframe for this activity is within 24 hours of the incident.

<u>Recovery Location:</u>

Khobar Office/Riyadh Office

- <u>Task02 Commence operations from the Disaster Recovery Site</u>

This task provides the necessary steps to commence core SNLC operations from the Disaster Recovery site and commence the planning for restoration of services in the short and longer term.

<u>Incident Response Team</u>

Team Leader	**Team Members**
V.P	CTO
	Business Development Director
	Managed Service Director
	IT Dept
	Cyber Security Dept
	HR Dept
	Health, Safety and Environment Dept

<u>Recovery Procedure</u>

Steps to be taken:

- Establish a disaster recovery site.

Responsible Person: Health, Safety and Environment Dept

- Layout workspace utilizing tables and chairs from community center.
- Communicate with other Incident Response Team members to assess what must be replaced right once and what can be recovered.
- Address IT needs

Responsible Person: IT Dept

- Find accessible machines and set up an alternate server facility.
- Recover data backups.
- Request quotes for replacing hardware or an alternate cloud-based solution.
- Establish the disaster recovery site for full operations in the medium to longer term.

Responsible Person: V.P

- Recover data to pre disaster state.
- Contact all necessary persons to inform of incident, expected delays and seek documentation where necessary.
- Establish necessary equipment and infrastructure requirements to provide full operations from recovery site.

<u>Recovery Time Objective</u>

- This task must be completed within 4 weeks after the incident.

<u>Recovery Location</u>

- Riyadh Office / Khobar Office

6.8 Internet services failure

a) Disaster Recovery Plan

- Task 01 Immediate Response

This task provides the necessary command and control to enable the SNLC Incident Response Team to conduct an initial assessment of the Disaster and to co-ordinate SNLC's initial response to the disaster.

Incident Response Team

Team Leader	Team Members
V.P	CTO
	Business Development Director
	Managed Service Director
	IT Dept
	Cyber Security Dept

Recovery Procedure

- The IT team, in coordination with relevant personnel, assesses the nature and scope of the failure, including its impact on critical business functions and the extent of the internet service outage.
- Document the incident, including the date, time, location, affected systems, and initial assessment.
- The incident must be reported to all customers by the NOC.
- The IT team conducts a technical assessment to determine the cause of the internet services failure, whether it's an internal issue, service provider problem, or other factors.
- Task 02 Recovery Actions

Incident Response Team

Team Leader	Team Members
V.P	CTO
	Business Development Director
	Managed Service Director
	IT Dept
	Cyber Security Dept

Recovery Procedure

Steps to be taken:

- The IT Team must evaluate the impact on critical business functions and services. Determine the extent of downtime.
- NOC must contact the internet service provider (Salam) to report the outage and seek information on the cause and expected resolution time.
- If the issue is internal, the Network team should diagnose and resolve the problem promptly. This may include fixing network hardware, adjusting configurations, or replacing faulty equipment.
- Network Team must activate backup internet connectivity through secondary service providers.
- Network Team must Verify that internet services are fully restored and functioning correctly.
- Maintain detailed records of the incident, actions taken, timelines, and communications.

Recovery Time Objective

- This task must be completed within 1 hour after the incident.

Recovery Location

- Khobar Hub

6.9 SNL Critical Data

a) Disaster Recovery Plan

- Task 01 Immediate Response

  This task provides the necessary command and control to enable the SNLC Incident Response Team to conduct an initial assessment of the Disaster and to co-ordinate SNLC's initial response to the disaster.
- Incident Response Team

Team Leader	Team Members
V.P	CTO
	Business Development Director
	Managed Service Director
	IT Dept
	Cyber Security Dept

Recovery Procedure

- The IT team, in coordination with relevant personnel, assesses the nature and scope of the data loss, including the impacted data, the cause of the loss, and the potential impact on critical business functions.
- Isolate affected systems or data repositories to prevent further data loss or corruption.
- Implement measures to protect the remaining data, such as adjusting access controls or activating backup systems.
- Document the data loss incident, including the date, time, location, affected systems, and initial assessment.
- Notify relevant stakeholders, including department heads, IT team members, and management, about the incident.
- Task 02 Recovery Actions

Incident Response Team

Team Leader	Team Members
V.P	CTO
	Business Development Director
	Managed Service Director
	IT Dept
	Cyber Security Dept

Recovery Procedure

Steps to be taken:

- The IT Team Identify the most recent, clean backup from which the lost data can be restored.
- The IT Team shall restore the lost data from the identified backup source. Ensure the backup is validated for integrity and completeness.
- Verify the integrity of the restored data through data consistency checks and testing.
- The IT Team must validate the accuracy and completeness of the restored data to ensure it matches the state before the data loss incident.

6.10 VSAT services failure

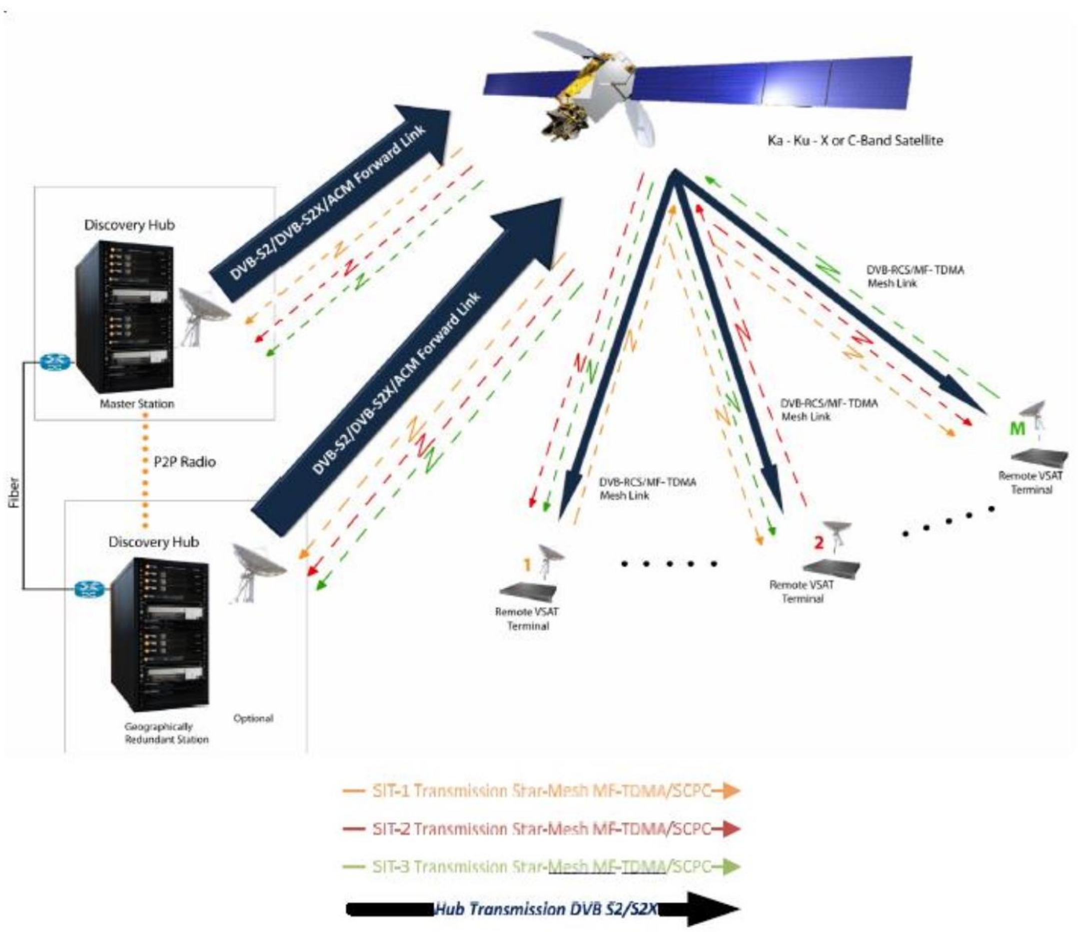
a) Disaster Recovery Plan

- Redundancy

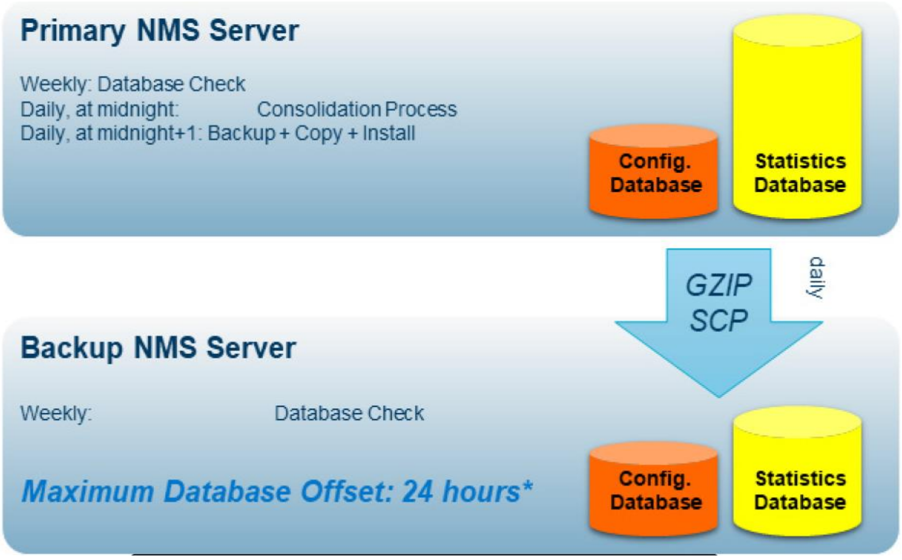
  Geographic redundancy provides enhanced network availability in two ways. First, by having two gateway locations separated by a suitable distance; the network is protected from adverse propagation effects such as heavy rain at the gateway location. Should heavy rain disrupt the transmission and reception at the primary gateway, the traffic is transferred to the secondary gateway, which is unlikely to be suffering the same propagation disturbances at the same time.

The second manner that network availability is enhanced is by providing a duplicate equipment complement in the case of a catastrophic equipment failure at the primary location. Here is a typical VSAT network design of redundancy solution at Saudi Net Link.

Our Active VSAT network is operating on iDirect Hub system included of following components:


Ka - Ku - X or C-Band Satellite
DVB-S2/DVB-S2X/ACM Forward Link
DVB-S2/DVB-S2X/ACM Forward Link
Discovery Hub
Master Station
P2P Radio
Fiber
Discovery Hub
Geographically Redundant Station
Optional
DVB-RCS/MF-TDMA Mesh Link
DVB-RCS/MF-TDMA Mesh Link
DVB-RCS/MF-TDMA Mesh Link
1
Remote VSAT Terminal
2
Remote VSAT Terminal
M
Remote VSAT Terminal
SIT-1 Transmission Star-Mesh MF-TDMA/SCPC
SIT-2 Transmission Star-Mesh MF-TDMA/SCPC
SIT-3 Transmission Star-Mesh MF-TDMA/SCPC
Hub Transmission DVB S2/S2X

- **Hub Chassis:** Can host up to 20 Line Cards and it supports up to five satellites comes with two power supply units and two GPS modules working as 1+1 for redundancy hot failover. Spare Chassis is available On-site and pre-configured as standby.
- **Two Protocol Processor (PP) servers:** each PP can handle until 250 remote sites, and they are Working as 1+1 with load balance techniques to handle remote traffic acceleration, QoS and allocation of burst time plan including the data & traffic interchange between upstream/ customer network and remotes Current CPU utilization does not exceed 30% and in case of one PP fail still other PP capable to handle all Process and traffic without any downtime. The failover process on PP is performed automatically without Operator intervention.
- **Two Network Management System (NMS) servers:** Our network is running with one primary NMS and one Back up NMS are synchronized with each other containing all remotes and network database and configurations data. It has the user interface to monitor traffic & control most network components. Data backup process and database updates from PNMS to BNMS is configured on daily basis as follow:



Primary NMS Server

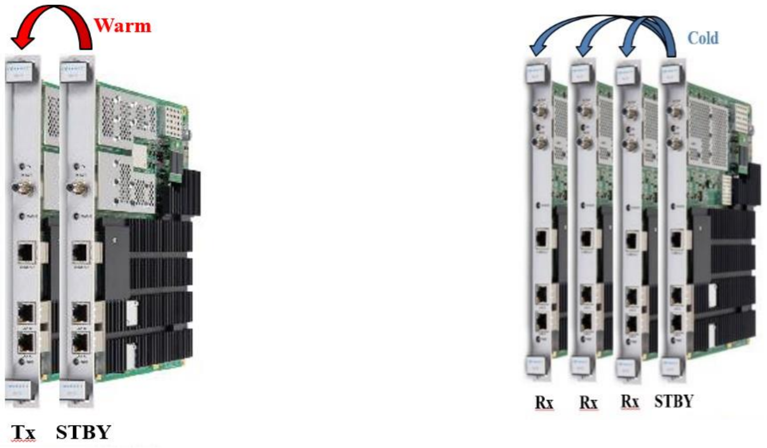
Weekly: Database Check
Daily, at midnight: Consolidation Process
Daily, at midnight+1: Backup + Copy + Install

Backup NMS Server

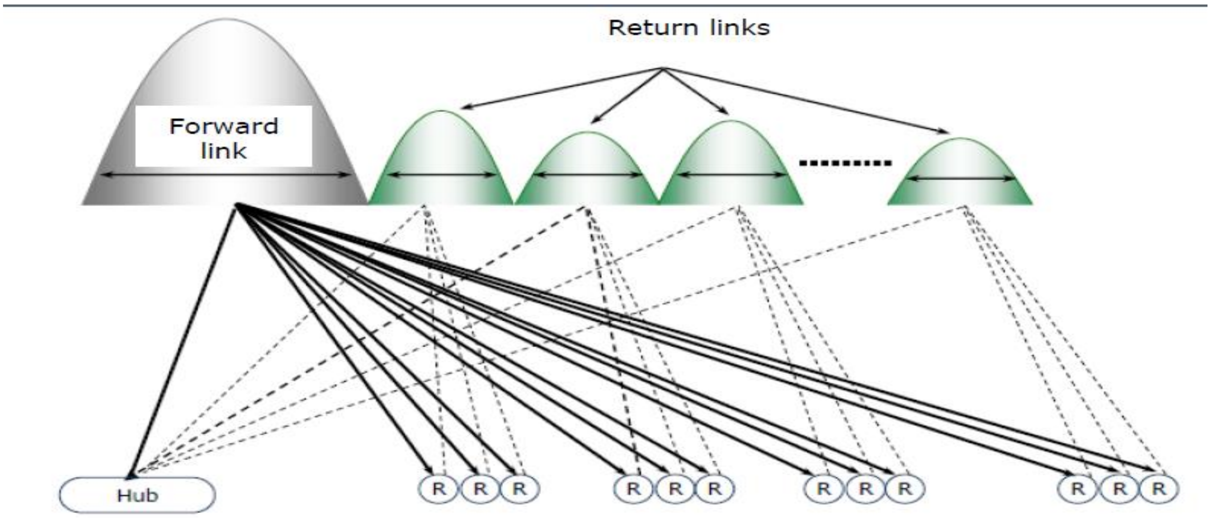
Weekly: Database Check

*Maximum Database Offset: 24 hours**

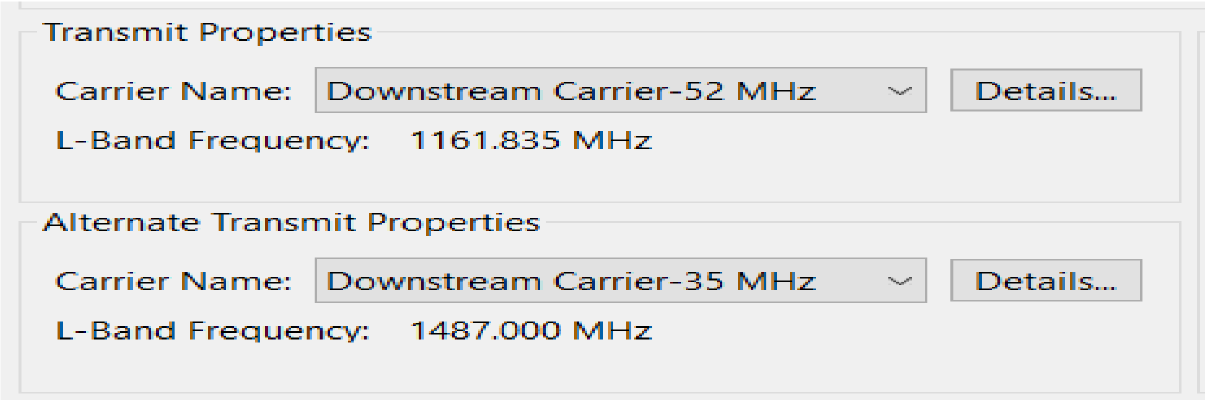
- **Line Cards:** One active TX line card and the other one is hot standby installed in chassis for auto swap Also, there are seven (7) RX line cards with cold relation as one standby for multiple cards.



Our Network is composed of one Forward Link (Outbound Carrier) and a Cluster of Return Links



- **Return Links:** Working on frequency hopping technique that allows remotes sites to share the available time slots and transmit its traffic per their assigned burst plan by the carrier in each time group. This will prevent any down time in case of any return carrier or RX line cards fail. Some of RX line cards support Multiple return carriers as it loaded with a license to activate multiple frequencies in one line card.
- **Forward Link:** it configured as DVB-2 with adaptive Code Modulation technique. There are two transmit Carriers are configured symmetric to each other on the same satellite with different frequencies as follow:



Transmit Properties

Carrier Name: Downstream Carrier-52 MHz

L-Band Frequency: 1161.835 MHz

Alternate Transmit Properties

Carrier Name: Downstream Carrier-35 MHz

L-Band Frequency: 1487.000 MHz

7. Testing and Training

7.1 Testing

a) Conduct annually disaster recovery drills and exercises to ensure that personnel are familiar with the recovery procedures.

7.2 Training

a) Provide training to relevant personnel on their roles and responsibilities during a disaster recovery scenario.

8. Documentation and Reporting

8.1 Incident Documentation

a) Maintain detailed records of the incident, including the cause, impact, and response.

8.2 Reporting

a) Report the incident to relevant authorities, regulatory bodies, and stakeholders as required by law or company policy.

9. Contacts and Resources

9.1 Emergency Contacts

a) Maintain an up-to-date list of emergency contacts, including key personnel, vendors, and local authorities.

9.2 Resources

a) Ensure access to necessary resources such as backup data, recovery hardware, and communication tools.

10. Activation and Escalation

10.1 Activation

a) Activate the DR Plan promptly when a major disruption occurs.

10.2 Escalation

a) Establish clear escalation procedures for situations that require additional resources or expertise.

11. Review and Audit

11.1 Conduct regular reviews and audits of the DR Plan to identify areas for improvement and ensure ongoing effectiveness.

Appendix A – Contact Information

A-1 Disaster Recovery Team

Name	Role / Position	Contact Information
Mohamed Saeed	Sr. System Engineer	mds@saudinetlink.com
Muhaned Kamal Ali	Information Security Specialist	0555220624
Sheikh Rameez Uddin	Satellite Support and VSAT Operation	0555890449
Eslam Ahmed	Sales Engineer	0540409799
Ali Abdullah Al-Ghamdi	Field Coordinator	0581170001
Sajim A Usman	VSAT Technician	0541367273
Asmaa Shady	NOC Team Leader	ais@saudinetlink.com

A-2 Contact list – Internal

Person	Position	Contact number/s
Abdullah Al Shuhail	V.P	057484264
Yasir Awad	CTO	056827803
Mohammed ElFaisal	Business Development Director	0557192900
Rami Abdalmutelb	Managed Service Director	0568383382
Marwah Alsubaiei	HR officer	0563637628
Muhaned Ali	Information Security Specialist	0559105835
Mohammed Ibrahim	IT & Network Engineer	0540407547
Sheikh Rameez Uddin	Satellite Support and VSAT Operation	0555890449
Masood Ahmed	Safety Consultant	0555804105
Hany Ahmed	Accountant	0536305984

A-3 Contact list – External

Person	Position	Contact number/s
Mohammed Khamis	Account Manager (SALAM)	0540523592
Maroon Khalil	Regional Sales Manager (ABS)	+971505095919
Yasir Hassan	Director of Transmission Operations (Arabsat)	0504463680
ABS-TAC	Customer Support	+63472529012
Arabsat	Customer Support	+966114030392
SALAM	Salam Business Care	0114062444
Riyadh Aljameel	Account Manager (STC)	0505412225
Mohamed Gailani	Sales Engineer (Rectangle Co)	0530801812