



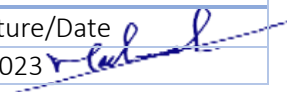
# Business Continuity Plan

Doc. Control Number	Version
SNL-62	0.2



## Document Reference

Item	Description
Title	Business Continuity 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	13/9/2023 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	13/9/2023 

## 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 policy has been reviewed



## Contents

1. Introduction .....	4
2. Objectives .....	4
3. Risk Assessment .....	4
4. Business Impact Analysis .....	6
5. Business continuity owner .....	7
6. Incident Response Plans .....	7
7. Key Contact Sheet .....	20
8. Event Log.....	20
9. Training and Testing.....	21
10. Plan Maintenance and Review .....	21

## 1. Introduction

This Business Continuity (BC) plan outlines the strategies and procedures to be followed in the event of various scenarios that could disrupt normal business operations. The primary objective of this plan is to minimize the impact of disruptions and ensure the continuity of critical business functions. It is essential to document, maintain, and communicate this plan to appropriate parties to ensure a swift and coordinated response to any unforeseen events. The following scenarios are addressed:

- a) Equipment failure
- b) Disruption of power supply or communication
- c) Application failure or corruption of the database
- d) Human error, sabotage, or strike
- e) Malicious software attack
- f) Hacking or other internet attacks
- g) Social unrest or terrorist attacks
- h) Environmental disasters
- i) Emergency contact information for personnel

## 2. Objectives

This plan provides preventative actions and contingency plans for an event which could disrupt SNLC's core business functions.

The objectives of this plan are to:

- a) Define SNLC's critical business functions.
- b) Detail SNLC's immediate and recovery response to those risks assessed as a high or extreme risks.
- c) Detail strategies and actions to be taken to enable SNLC to continue to provide critical business functions in the event of an emergency or disaster.
- d) Review and update this plan on an annual basis.

## 3. Risk Assessment

The risks addressed on the following pages for the SNLC Infrastructure have been identified and assessed in SNLCs' risk register.

SNLC's risk register identifies "Failure to maintain business continuity in emergency situations" as an enterprise risk that has an inherent risk level of extreme. The risk treatment requires SNLC to "Establish and maintain an effective business continuity plan". The assessed residual risk after the business continuity plan has been established is rated at low.

It is considered that failure to maintain business continuity is the inability to provide SNLC core services.

### 3.1 Equipment failure incident

Total loss of Equipment due to fire, or damage

- a) Initiate Incident Response Plan.
- b) Assess scope of damage and engage preferred suppliers to source hardware replacement/repair and determine the outage time.
- c) Engage the offsite recovery option if applicable.
- d) Maintain a list of approved vendors for timely equipment repairs or replacements.
- e) Inform the customers (if they will be impacted).
- f) Activate the IRT to assess the impact, implement temporary workarounds, and initiate recovery processes.

### 3.2 Disruption of power supply or communication

- a) Initiate Incident Response Plan
- b) Ensure enough UPS capacity to allow for critical transfer of communications to alternative sources.
- c) Start and run emergency generators.

- d) Develop communication protocols to reach employees, customers, and vendors during disruptions.
- e) The IRT will coordinate recovery efforts, ensuring minimal downtime.
- 3.3 Application Failure or Corruption of Database
  - a) Initiate Incident Response Plan
  - b) Invite the IT Team
  - c) The IT Team shall assess scope of failure and engage preferred suppliers to source software replacement/repair and determine the outage time.
  - d) Instigate manual or recovery processes for key functions if required.
  - e) In the event of failure or corruption, the IRT will initiate restoration procedures promptly.
  - f) Re-establish and bring all information up to date.
- 3.4 Human Error, Sabotage, or Strike
  - a) Initiate Incident Response Plan.
  - b) Examine the scope of the failure and determine whether it is an intentional error.
  - c) Contact police.
  - d) Clearly define protocols for reporting and investigating potential sabotage or security breaches.
  - e) Implement counselling or disciplinary action for staff after investigation is completed (if required).
- 3.5 Malicious Software Attack, Hacking or Other Internet Attacks
  - a) Initiate Incident Response Plan.
  - b) Get in touch with the INFOSEC department.
  - c) Contact police.
  - d) The IT team should go over the backup and restore the data from the backup storage.
  - e) Engage preferred supplier for replacement of equipment and restoration of IT data/software systems etc.
  - f) Implement counselling or disciplinary action for staff after investigation is completed (if required).
- 3.6 Social Unrest or Terrorist Attacks
  - a) Initiate Incident Response Plan
  - b) Contact police.
  - c) Ensure the safety of employees and customers during such incidents.
  - d) Implement counselling or disciplinary action for staff after investigation is completed (if required).
- 3.7 Environmental Disasters
 

Total loss of Khobar Office or Riyadh Office

  - a) Initiate Incident Response Plan.
  - b) Contact police.
  - c) Salvage equipment, furniture etc.
  - d) Implement diversion to mobile phones.
  - e) Relocate staff to another facility – refer to IT failure contingencies for IT related incidents.
  - f) Where possible relocate critical equipment to alternate sites to ensure basic operation of services.
  - g) Source replacement items immediately from a preferred supplier.
  - h) Engage preferred supplier for replacement of equipment and restoration of IT data/software systems etc.
  - i) Notify customers of alternate site via email or phone.
  - j) Undertake assessment of damage, obtain quotes, and engage suppliers.

### 3.8 Internet services failure

- Initiate Incident Response Plan.
- Secure other sources for the Internet.
- Communicate with the service provider.
- If the outage is greater than 24 hours notify customers.

### 3.9 VSAT services failure

- Initiate Incident Response Plan.
- Activate the backup satellite.
- Communicate with the Satellite Operator.
- If the outage is greater than 24 hours notify customers.

## 4. Business Impact Analysis

As part of the Business Continuity Plan, a Business Impact Analysis has been undertaken which uses the information in the Risk Assessments to assess the identified risks and impacts in relation to critical business activities and determine basic recovery requirements.

### a) Critical Business Activities- External

Critical Business Activity	Description	Priority	Impact of Loss	Recovery Time Objective
<b>SNL VSAT Managed Services</b>	SNL provides our customers with VAST Managed Services.	High	Customers will be unable to contact with their sites or services since there will be no connectivity.	15 Minutes
<b>SNL IT Managed Services</b>	SNL offers IT management services to our customers, including AVL system and collocation services.	High	As a result of the outage, the services will be unavailable, and beneficiaries will be unable to access them.	2 Hours

### b) Critical Business Activities- Internal

Critical Business Activity	Description	Priority	Impact of Loss	Recovery Time Objective
<b>SNL Email System</b>	For official communication with customers and employees, SNL will use an email system.	High	There will be no emails lost but staff will not be able to send or receive emails via their SNLC accounts until the system is restored.	12 Hours
<b>SNL ERP System</b>	For best efficiency, SNL uses ERP system	Medium	Employees will be unable to	48 Hours

	to automate and manage critical business activities.		access the ERP system because of the outage; all operations will be performed manually until the service is restored.	
<b>SNL Critical Data</b>	This represents all of SNL's critical data, including projects, customers, commercial, employee, and financial information.	High	Valid and accurate data is crucial for day-to-day operations and decision making.	12 Hours

## 5. Business continuity owner

The Business Continuity Owner is a key stakeholder responsible for the oversight, coordination, and management of the company's business continuity efforts.

Rami Abdalmutelb - Managed Service Director

Business Continuity Manager

## 6. Incident Response Plans

The following incident response plans present detailed plans to address the highest risk areas identified in the risk management assessment outlined earlier in this plan.

The plans are not exhaustive as any major incident will require more detailed and potential long-term considerations; however, the plans below provide a structured response to major incidents that are of the highest threat to service provision and SNLC operations.

### 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

##### Recovery Procedure

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

#### b) 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.

Recovery Time Objective

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

Recovery Location:

Khobar Office/Riyadh Office

- Task02 Commence operations from the Disaster Recovery Site

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.

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

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.

Recovery Time Objective

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

Recovery Location

- Riyadh Office / Khobar Office

6.8 Internet services failure

c) 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

b) 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

Saudi Net Link is focusing on implementing a business continuity plan to assure the service continuity to our customers in general and will be consider for Saudi Electricity Company provided solutions and managed services. Apart of the complete proposal there are some significant and major elements are highly required to be consider for service provider infrastructure as following:

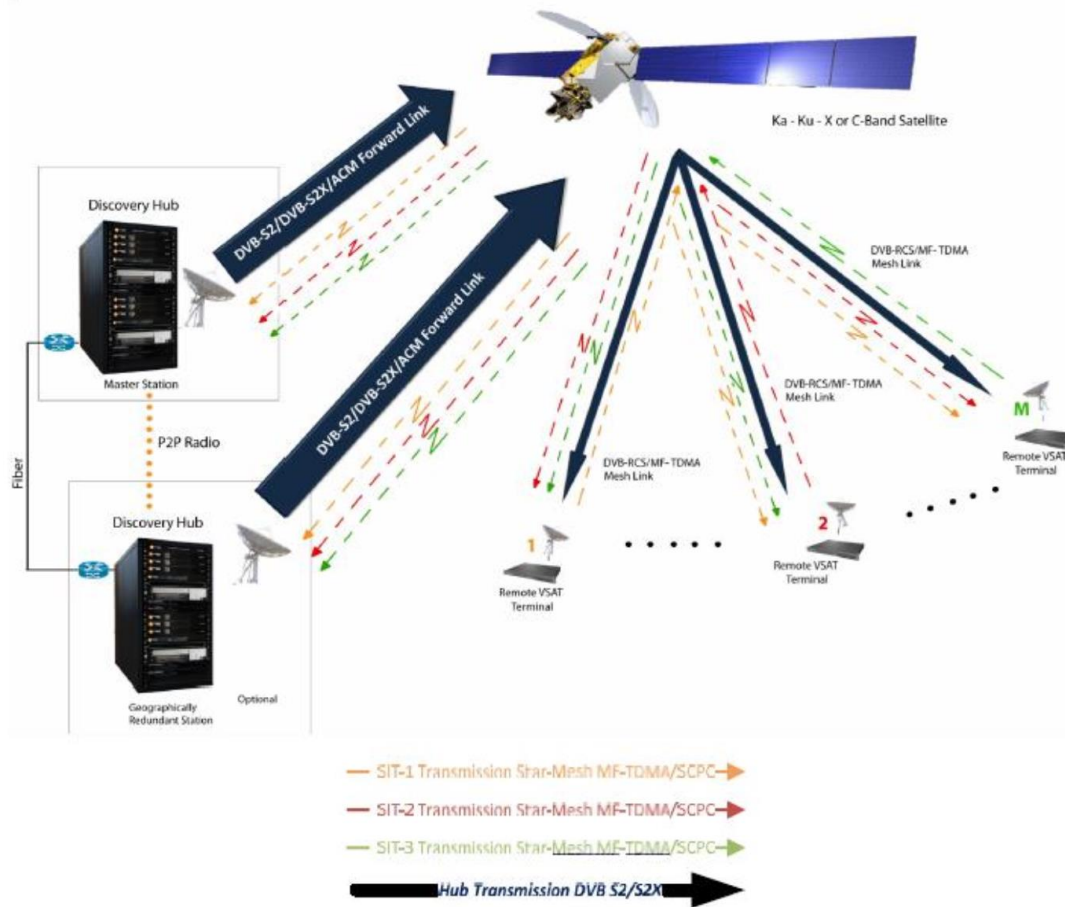
a) Redundancy



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.

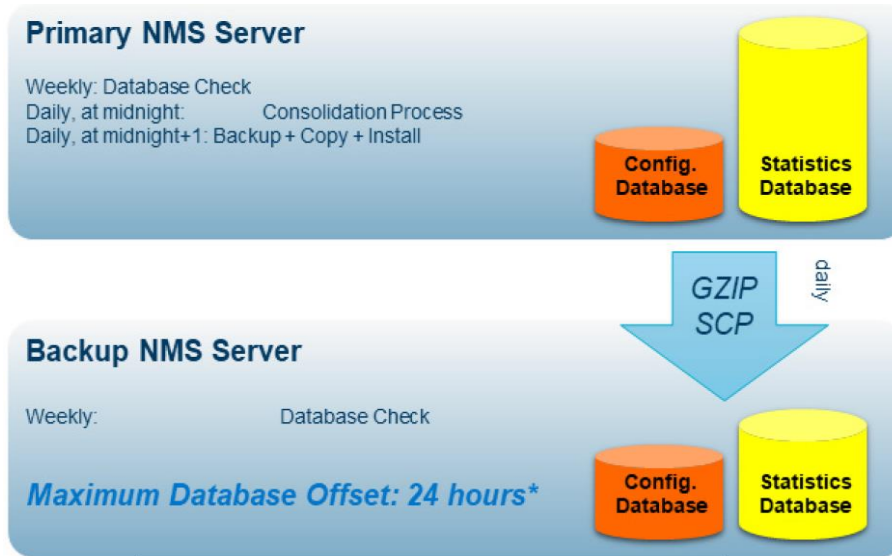
The second manner that network availability is enhanced is by providing a duplicate equipment complement in the case of a catastrophic equipment failure at the primary location. Here is a typical VSAT network design of redundancy solution at Saudi Net Link.

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



- **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

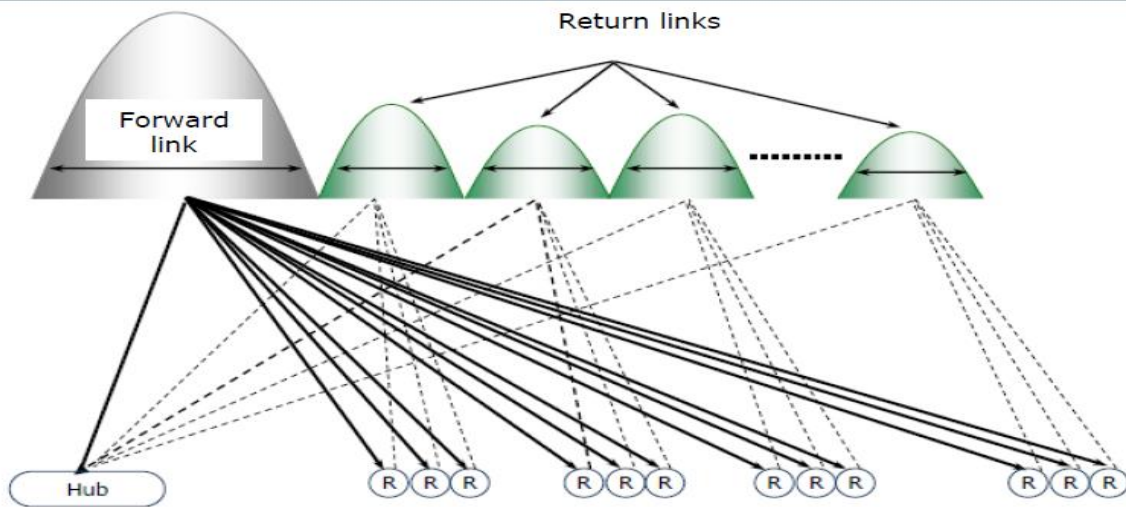
monitor traffic & control most network components. Data backup process and database updates from PNMS to BNMS is configured on daily basis as follow:



- **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 <input type="button" value="Details..."/>
L-Band Frequency:	1161.835 MHz
Alternate Transmit Properties	
Carrier Name:	Downstream Carrier-35 MHz <input type="button" value="Details..."/>
L-Band Frequency:	1487.000 MHz

- Summary of Existing VSAT Active Network Resiliency and Recovery Plan:
  - a) Our VSAT gateway located in the building where marine cable for internet is landed in Saudi Arabia eastern province and hosted in Salam (local ISP) Data center.
  - b) Our iDirect baseband system is fully redundant of Hub components.
  - c) Two NMS servers one as primary and the other as a backup Holds all the HUB database with adjusted backup process to be occurred daily from PNMS to BNMS so all HUB databases will be saved and exist in both servers.
  - d) Two PP servers (Primary and Backup) with Load balance and CPU utilization does not exceed 30 % so even if one of them failed then the network can be run with the second one alone with no effect on the network performance.

- e) 4 TX line cards equipped in the chassis, if we have any issue in one of our TX line cards it will be easy to swap a standby one with the failure one immediately.
- f) 7 Rx line cards equipped in the chassis, if we have any issue in one of our Rx line cards it will be easy to swap a standby one with the failure one immediately.
- g) RF cables are routed through different directions over Fiber Cables and multiple Hub Antennas are installed to be used during diester emergency or recovery plan.
- Implemented measures and process for high level of identified Risks:
  - a) Satellite capacity availability  
SNL has contracted with several satellite operators to provide satellite capacity and ensure the service Availability for the customers in case of service outage due to satellite issue. SNL has existing contract With Eutelsat, ABS, Intelsat and Arabsat are the leading satellite companies over the world.
  - b) Teleport facility and infrastructure
    - SNL leased and operated two teleports, one in Riyadh and other one in Khobar.
    - An active contract with Salam (local) ISP to provide hosting facility for SNL VSAT gateways including Internet backbone and leased lines services.
    - SNL and Arabsat have an agreement to uplink from Dirab teleport located in Riyadh owned by Arabsat.

## 7. Key Contact Sheet

### a) 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	Operation Manager	0555890449
Masood Ahmed	Safety Consultant	0555804105
Hany Ahmed	Accountant	0536305984

### b) 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

## 8. Event Log

The Event Log is to be used to record information, decisions and actions in the period immediately following the critical event or incident.

Date	Time	Information / Decisions / Actions	Initials




## 9. Training and Testing

- 9.1 Regular training sessions will be conducted for employees to familiarize them with the BC plan and their roles during incidents. Periodic testing and simulation exercises will also be performed to evaluate the plan's effectiveness and make necessary improvements.
- 9.2 SNLC must conduct Business Continuity drills at least annually.

## 10. Plan Maintenance and Review

- 10.1 The BC plan will be reviewed at least annually or whenever significant changes occur in the SNLC's structure, technology, or operations. Feedback from testing and real incidents will be used to update and improve the plan continuously.