



## IT BUSINESS CONTINUITY PLAN (BCP)

FEBRUARY 2024

**DOC POLICY NO:**

-----  
**Developed By**  
-----

**Assistant General Manager, Information Technology and Security Compliance**

---

### Executive Summary

The IT Business Continuity Plan (BCP) for NSPCL is designed to ensure the uninterrupted operation of critical IT services and business functions in the face of unforeseen disruptions. Recognizing the reliance on a complex IT infrastructure, which includes Microsoft Azure, FortiGate Firewall, various ISPs (Phase 3 Fibre, Airtel, MTN, Starlink), and the Unifi Network System, this BCP establishes comprehensive procedures and processes to mitigate risks and facilitate rapid recovery.


	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO: DATE OF ISSUE: REVISED DATE: <b>N/A</b>
	DOCUMENT TITLE: <b>IT BUSINESS CONTINUITY PLAN (BCP)</b>	

Table of Contents

1. Purpose ..... 3

2. Scope ..... 3

3. Objectives ..... 3

4. Business Impact Analysis ..... 3

5. Continuity Strategies ..... 3

6. Incident Response and Recovery ..... 4


7. Roles and Responsibilities ..... 4

8. Training and Awareness ..... 5

9. Testing and Maintenance ..... 5

10. Review and Revision ..... 5

Commented [OA1]: Format for structure

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO:	
	DOCUMENT TITLE: <b>IT BUSINESS CONTINUITY PLAN (BCP)</b>	DATE OF ISSUE: REVISED DATE: <b>N/A</b>	

1. Purpose

The purpose of this IT Business Continuity Plan (BCP) is to ensure the continuity of NSPCL's IT services and operations in the event of a disruption. This plan outlines the procedures and processes to be followed to maintain critical business functions and minimize the impact of incidents.

2. Scope

This BCP applies to all IT services, applications, software, servers, and tools managed by NSPCL, specifically focusing on the use of Microsoft Azure, FortiGate Firewall, ISPs (Phase 3 Fibre, Airtel, MTN, Starlink), and Unifi Network System for local network distributions.

3. Objectives

- Ensure the availability and reliability of critical IT services and applications.
- Minimize downtime and data loss during disruptions.
- Provide a clear framework for responding to and recovering from incidents.
- Maintain compliance with regulatory and business requirements.

4. Business Impact Analysis (BIA)

4.1. Critical IT Services and Applications

- **Microsoft Azure:** All business solution applications, software, servers, and tools.
- **FortiGate Firewall:** Network security and protection.
- **ISPs:** Internet connectivity (Phase 3 Fibre, Airtel, MTN, Starlink).
- **Unifi Network System:** Local network distribution and management.

4.2. Potential Risks and Impacts

- **Cloud Service Disruption:** Loss of access to critical applications and data.
- **Network Security Breach:** Compromise of sensitive information and systems.
- **ISP Outage:** Loss of internet connectivity affecting business operations.
- **Local Network Failure:** Disruption of internal communications and data flow.

5. Continuity Strategies

5.1. Cloud Services (Microsoft Azure)


- **Redundancy and Failover:** Utilize built-in redundancy and failover to ensure availability.
- **Data Backup:** Regularly back up data to geographically dispersed locations within Azure.
- **Disaster Recovery:** Implement Azure Site Recovery to replicate and recover applications and data in the event of disruption.

5.2. Network Security (FortiGate Firewall)

- **Firewall Redundancy:** Deploy redundant Firewalls to ensure continuous protection.
- **Regular Updates:** Keep firewall firmware and security policies up to date.
- **Monitoring and Alerts:** Implement continuous monitoring and alerts for suspicious activities.

Commented [IO2]: Is this a different policy? If yes, please provide for review.

Commented [EO3R2]: This are the Inbuilt Firewall Security Policies

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO:	
	DOCUMENT TITLE: <b>IT BUSINESS CONTINUITY PLAN (BCP)</b>	DATE OF ISSUE: REVISED DATE: <b>N/A</b>	

### 5.3. Internet Connectivity (ISPs)

- **Multiple ISPs:** Maintain contracts with multiple ISPs (Phase 3 Fibre, Airtel, MTN, Starlink) to ensure redundancy.
- **Automatic Failover:** Configure automatic failover between ISPs to maintain connectivity during outages.
- **Bandwidth Management:** Monitor and manage bandwidth usage to optimize performance.

### 5.4. Local Network (Unifi Network System)

- **Network Redundancy:** Implement redundant network paths and devices to ensure continuous connectivity.
- **Regular Maintenance:** Conduct regular maintenance and updates on network equipment.
- **Monitoring and Alerts:** Use Unifi's monitoring tools to detect and respond to network issues promptly.

## 6. Incident Response and Recovery

### 6.1. Incident Detection and Reporting

- **Detection:** Use automated monitoring tools to detect incidents in real-time.
- **Reporting:** Establish clear procedures for reporting incidents to the ITSC team.

### 6.2. Incident Response


- **Initial Assessment:** Conduct an initial assessment to determine the scope and impact of the incident.
- **Containment:** Implement measures to contain the incident and prevent further damage.
- **Communication:** Notify relevant stakeholders and provide regular updates on the incident status.

### 6.3. Recovery

- **Data Restoration:** Restore data from backups as needed.
- **System Recovery:** Use Azure Site Recovery and other tools to restore affected systems and applications.
- **Verification:** Verify that all systems are functioning correctly and that no residual issues remain.

## 7. Roles and Responsibilities

- **ITSC Team:** Responsible for implementing and maintaining the BCP, responding to incidents, and ensuring the continuity of IT services.
- **Incident Manager:** Oversees the incident response process and coordinates recovery efforts.
- **Users:** Report incidents promptly and follow established procedures during disruptions.
- **Stakeholders:** Support the BCP and ensure compliance with policies and procedures.

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO:	
	DOCUMENT TITLE: <b>IT BUSINESS CONTINUITY PLAN (BCP)</b>	DATE OF ISSUE: REVISED DATE: <b>N/A</b>	

#### 8. Training and Awareness

- **User Training:** Provide regular training on BCP procedures and best practices.
- **Awareness Programs:** Conduct awareness programs to keep users informed about the importance of business continuity.

#### 9. Testing and Maintenance

- **Regular Testing:** Conduct regular tests of the BCP to ensure its effectiveness.
- **Plan Updates:** Review and update the BCP annually or as needed to reflect changes in the IT environment or business requirements.

#### 10. Review and Revision

This policy will undergo a formal review every two (2) years to ensure its continued relevance and effectiveness. The review will be conducted by the IT Team in collaboration with key stakeholders. If significant changes in technology, regulatory requirements, or threat landscape arise before the next scheduled review, an addendum will be issued and attached as an update to relevant sections of the policy. Such interim updates will remain in effect until the next comprehensive review and integration into the core policy.