



## IT DISASTER RECOVERY PLAN

JUNE 2025

**DOC POLICY NO:**


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

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

---

### Executive Summary

The North South Power ITSC Disaster Recovery Plan (DRP) establishes the framework, responsibilities, and procedures to enable the timely recovery and continuity of critical IT systems and services following a disaster event. This plan ensures that disruptions caused by cyberattacks, hardware failures, natural disasters, or network outages do not compromise the integrity, availability, and confidentiality of North South Power's business operations. The DRP supports North South Power's commitment to service resilience, regulatory compliance, and continuous improvement of its business continuity strategy.

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO:
	DOCUMENT TITLE: <b>IT DISASTER RECOVERY PLAN</b>	DATE OF ISSUE: REVISED DATE: <b>N/A</b>

### 1. Purpose

This DRP outlines actionable steps and structured processes for restoring North South Power’s IT infrastructure in the event of a disaster. Its primary aim is to:

- Minimize downtime and data loss.
- Support the rapid recovery of IT services.
- Ensure business continuity through structured recovery processes.
- Define roles, responsibilities, and escalation procedures.
- Comply with applicable regulatory and business standards.

### 2. Scope

This DRP applies to all IT-managed systems within North South Power, including but not limited to:

- Cloud Services: Microsoft Azure
- Network Security: FortiGate Firewall
- ISPs: Phase 3 Fibre, Airtel, MTN, Starlink
- Local Network Distribution: Unifi Network System
- Security Infrastructure: CCTV surveillance systems
- Telecommunication: IP Telephony
- Endpoint Security: Antivirus solutions


### 3. Objectives

- Restore critical IT services and applications within defined RTOs/RPOs.
- Maintain critical business functions with minimal disruption.
- Protect sensitive data during and after incidents.
- Improve recovery efficiency through consistent drills and reviews.
- Clearly define roles, tools, and procedures for recovery.
- Provide a clear framework for responding to and recovering from disasters.
- Maintain compliance with regulatory and business requirements.

### 4. Disaster Recovery Team

Role	Responsibilities
Disaster Recovery Manager	Responsible for overseeing the DRP, coordinating recovery efforts, timely communication, report to executive leadership.
ITSC Team Members	Responsible for executing the DRP, including data backup, system restoration, system health checks and network recovery.
Communication Coordinator	Responsible for communicating with stakeholders, users, and external partners during the recovery process

Commented [OA1]: No table of contents

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO:
	DOCUMENT TITLE: <b>IT DISASTER RECOVERY PLAN</b>	DATE OF ISSUE: REVISED DATE: <b>N/A</b>

Security Officer	Responsible for ensuring the security of data and systems during the recovery process
------------------	---

5. Risk Assessment and Business Impact Analysis (BIA)

5.1. Potential Risks

- **Cloud Service Disruption:** Loss of access to critical applications and data hosted on Microsoft Azure.
- **Network Security Breach:** Compromise of sensitive information and systems protected by FortiGate Firewall.
- **ISP Outage:** Loss of internet connectivity affecting business operations.
- **Local Network Failure:** Disruption of internal communications and data flow managed by Unifi Network System.
- **CCTV System Failure:** Loss of surveillance capabilities impacting security monitoring.
- **IP Telephony Disruption:** Loss of voice communication services affecting business operations.
- **Antivirus Failure:** Increased risk of malware infections and data breaches.
- **Azure Downtime:** Outage in cloud-hosted applications or data services.
- **Firewall Breach:** Intrusion due to misconfiguration or outdated firmware.
- **ISP Disruption:** Internet connectivity loss due to regional or ISP-specific issues.
- **LAN Failure:** Switch/router/hub failures impacting Unifi infrastructure.
- **CCTV Downtime:** Critical security footage loss.
- **VoIP Interruption:** IP Telephony outage impacting internal/external communication
- **Antivirus Failure:** Exposure to malware, ransomware, or data theft

5.2. Business Impact Analysis


BIA Components

Service	RTO	RPO	Criticality
Azure Services	2 hours	30 minutes	High
FortiGate Firewall	1 hour	15 minutes	High
ISP (Primary)	30 minutes	5 minutes	High
Unifi Network	1 hour	15 minutes	High
CCTV Footage	8 hours	1 hour	Medium
IP Telephony	2 hours	30 minutes	Medium
Antivirus Protection	Immediate	Near-zero	High

6. Disaster Recovery Strategies

6.1. Cloud Services (Microsoft Azure)

- **Redundancy and Failover:** Utilize Azure's built-in redundancy and failover capabilities to ensure high availability.
- **Data Backup:** Regularly back up data to geographically dispersed locations within Azure.

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO: DATE OF ISSUE: REVISED DATE: <b>N/A</b>
	DOCUMENT TITLE: <b>IT DISASTER RECOVERY PLAN</b>	

- **Disaster Recovery:** Implement Azure Site Recovery to replicate and recover applications and data in the event of a disaster.

#### 6.2. Network Security (FortiGate Firewall)

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

#### 6.3. 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.

#### 6.4. 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.

#### 6.5. CCTV System


- **Redundancy:** Implement redundant recording systems to ensure continuous surveillance.
- **Data Backup:** Regularly back up CCTV footage to secure storage locations.
- **Monitoring and Alerts:** Use automated monitoring tools to detect and respond to system failures.

#### 6.6. IP Telephony

- **Redundancy:** Deploy redundant IP telephony systems to ensure continuous voice communication services.
- **Data Backup:** Regularly back up configuration data and call logs.
- **Monitoring and Alerts:** Implement continuous monitoring and alerting for system performance and failures.

#### 6.7. Antivirus Solutions

- **Regular Updates:** Ensure antivirus software is regularly updated with the latest virus definitions.

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO:
	DOCUMENT TITLE: <b>IT DISASTER RECOVERY PLAN</b>	DATE OF ISSUE: REVISED DATE: <b>N/A</b>

- **Monitoring and Alerts:** Implement continuous monitoring for malware detection and alerts for suspicious activities.
- **Incident Response:** Develop and implement procedures for responding to malware infections and data breaches.

### 7. Disaster Recovery Procedures

#### 7.1. Incident Detection and Reporting

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

#### 7.2. Initial Assessment and Activation

- **Assessment:** Conduct an initial assessment to determine the scope and impact of the disaster.
- **Activation:** Activate the DRP if the disaster meets the criteria for activation.

#### 7.3. Communication

- **Internal Communication:** Notify the Disaster Recovery Team and relevant stakeholders.
- **External Communication:** Communicate with external partners, vendors, and customers as needed.

#### 7.4. Data Backup and Restoration

- **Data Backup:** Ensure that all critical data is backed up according to the backup schedule.
- **Data Restoration:** Restore data from backups to the appropriate systems.

#### 7.5. System Recovery

- **Cloud Services:** Use Azure Site Recovery to restore applications and data.
- **Network Security:** Ensure that FortiGate Firewalls are operational and secure.
- **Internet Connectivity:** Verify that ISP failover mechanisms are functioning.
- **Local Network:** Restore local network connectivity using Unifi Network System.
- **CCTV System:** Restore surveillance capabilities and verify functionality.
- **IP Telephony:** Restore voice communication services and verify functionality.
- **Antivirus Solutions:** Ensure antivirus software is operational and up to date.


#### 7.6. Verification and Testing

- **Verification:** Verify that all systems and services are functioning correctly.
- **Testing:** Conduct thorough testing to ensure that no residual issues remain.

### 8. Post-Disaster Review

- **Review:** Conduct a post-disaster review to analyze the response and recovery process.
- **Documentation:** Document all findings, lessons learned and areas for improvement.
- **Process Improvement:** Update the DRP based on the review to enhance future response efforts.

Formatted: Indent: Before: 1.27 cm, No bullets or numbering

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO:	
	DOCUMENT TITLE: <b>IT DISASTER RECOVERY PLAN</b>	DATE OF ISSUE: REVISED DATE: <b>N/A</b>	

#### 9. Training and Awareness

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

#### 10. Testing and Maintenance

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

#### 11. 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 Security 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.