Information Technology Disaster Recovery Plan

FY 23/24

Abstract

This document delineates describes our NWF Health Network's policies and procedures for technology disaster recovery, as well as process-level plans for recovering critical technology platforms and the telecommunications infrastructure.

Kervin Rene

Kervin.Rene@nwfhealth.org

NWFHN IT Disaster Recovery Plan

Contents

1. AUTHORIZATION FOR INFORMATION TECHNOLOGY (IT) DISASTER RECOVERY PLAN

This document describes NWF Health Network's (NWFHN's) policies and procedures for technology disaster recovery, as well as process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This plan summarizes NWFHN's recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure the physical safety of our people, our systems, and our data. The goal of this plan is to define the agency's actions to ensure information system uptime, data integrity and availability, and business continuity.

NWFHN's management has approved the following policy statements:

1. NWFHN shall develop a comprehensive IT disaster recovery plan.
2. A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
3. The disaster recovery plan should cover all essential and critical IT infrastructure elements, systems and networks, in accordance with key business activities.
4. The IT Disaster Recovery Plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
5. All staff must be made aware of the IT Disaster Recovery Plan and their own respective roles.
6. This plan is to be kept up to date to take into account changing circumstances.

1.1 POLICY/ADMINISTRATIVE REGULATION

The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan designed to help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective
- The need to consider implications on other company sites
- Disaster recovery capabilities as applicable to key customers, vendors and others

This plan has been created as per the requirements of the following administrative regulations:

1. NWF Health Network's Emergency Preparedness & Continuity of Operations Plan
2. NWFHN *Operating Policy 1403 – Emergency & Disaster Preparedness*

1.2 OBJECTIVES

NWFHN IT Department has developed this IT disaster recovery plan to be used in the event of a significant disruption to critical IT services at NWFHN service centers. The goal of this plan is to outline the key recovery steps to be performed during and after a disruption so that critical IT and

telecommunication services continue within an appropriate period of time after an incident has occurred. The top priority of NWFHN will be to enact the steps outlined in this plan to bring all of the organization's groups and departments back to business-as-usual as quickly as possible. This includes:

- *Preventing the loss of the organization's resources such as hardware, data and physical IT assets*
- *Minimizing downtime related to IT*
- *Keeping the business running in the event of a disaster*

EXTERNAL CONTACTS

Property Manager/Landlord: _____ Account Number: _____

First Name	Last Name	Title	Contact Type	Contact information
				Work
				Mobile
				Email
				Work
				Mobile
				Email
				Work
				Mobile
				Email
				Work
				Mobile
				Email
				Work
				Mobile
				Email
				Work
				Mobile
				Email

2. SCOPE OF DISASTER RECOVERY PLAN

List of services covered in this plan:

Service Tier	IT Service or Application Name	Recovery Time Objective (Hours)	Recovery Point Objective (Hours)
0	Data Centre Facility	4	N/A
0	Core Routing	12	24
0	Storage Services	12	24
1	Server Services	12	24

Service Tier	IT Service or Application Name	Recovery Time Objective (Hours)	Recovery Point Objective (Hours)
0	WAN Connectivity	8	12
0	Firewall Services	12	24
2	Active Directory	12	24
1	Payroll	8	12
2	Email	8	24

2.1 ASSUMPTIONS

This IT disaster recovery plan intends to provide NWFHN authority with the necessary information needed to resume information technology services in a proper and timely manner to support the identified essential business processes for the following scenarios:

- destruction or inability to access data centre/server room facility;
- loss of systems (network and/or applications); and
- loss of employees.

In addition, the detailed recovery procedures as well as recovery strategies, estimated recovery time objectives and recovery point objectives are based on the following general assumptions and will need to be validated:

- continuous efforts to allocate the space required in the current data centre to restore information systems in case this site is deemed unavailable;
- continuous efforts to establish the alternate site for the current data centre in case the data centre is deemed unavailable; and
- backups are readily available to initiate restoration efforts.

Staff

- Key IT staff or their alternates required to assist in the recovery efforts will be available.
- IT staff involved in recovery efforts have the necessary technical skills to restore critical information systems identified in this document.

Users

- Key users will have their laptops or a suitable device with them during a disaster.
- Key users will have internet access and telephone/voice communication capability available to work from a remote location.

Networking

- There is ample bandwidth at the recovery site to connect to the internet.
- Bandwidth expansion is possible at the recovery site.

Configuration files can be uploaded to network devices through a laptop or other type of device.

Note: assumptions for each specific IT service are listed in a different section.

3. FACILITY AND INFRASTRUCTURE PLAN

- **When Alerted of an Impending Disaster, the IT Manager shall: (to the extent that time permits and as instructed by the (IT) Emergency Response Team (ERT))**
    1. Be prepared to execute the Disaster Recovery Plan.
    2. Be prepared to activate the IT Alternate Site Plan.
    3. Perform a special backup of all systems; secure backup disks offsite.
    4. Secure work area during a warning.
    5. Inform all users of a pending system shutdown.
    6. If necessary, shutdown all systems.
    7. If necessary, implement appropriate evacuation, shelter-in-place and safety plans.

- **When a disaster has impacted the NWFHN Service Centers, the IT Manager shall:**
    1. Discontinue all normal business activities.
    2. If necessary and if time permits, shutdown all systems.
    3. Implement appropriate evacuation, shelter-in-place and safety plans.

POST-DISASTER ACTIVITIES (DEPENDING UPON THE LEVEL OF DAMAGE AND AS INSTRUCTED BY THE ERT)

Response

1. Do not turn on electrical equipment if corrosive contaminants are present or if the power supply is unreliable.
2. If applicable, disconnect all electrical equipment. As a safety precaution, first disconnect electrical power at the main circuit breaker.
3. Contact telecommunication providers.
4. Assess damages, identify destroyed & salvageable equipment, and send assessment to the ERT.
    - Computers
    - File Servers
    - Telecommunication Equipment
    - Peripheral Equipment
    - Data
    - Other
5. Be prepared to implement the Disaster Recovery Plan.
6. Be prepared to activate the IT Alternate Site Plan.
7. Order replacement equipment if the disaster is clearly restricted to hardware.
8. Contact critical suppliers and vendors.

Recovery

1. Initiate the Data Center cleanup, reconstruction and/or relocation efforts.

2. Relay information regarding personnel to Administration.
3. Maintain the IT Alternate Site.
4. Contact critical subcontractors and vendors.
5. Make critical (if only temporary) repairs.
6. Repair salvageable equipment and institute the replacement of critical equipment.
7. As soon as a physical facility with reliable power and communication capability is secured, initiate the replacement of destroyed or disabled equipment.

Long Term

1. Review the Department Plan.
2. Review vendor, subcontractor and supplier performance.

- **PRIMARY RECOVERY RESPONSIBILITIES**

1. Execute the Disaster Recovery Plan.
2. Execute the IT Alternate Site Plan if directed.
3. Systems support to mission-critical business services.
4. Telecommunications to mission-critical business services.
5. Assess damage to workspace & equipment.

3.1 FACILITY PLAN

If necessary, a hot site will be activated and notification will be given via recorded messages or through communications with managers once a decision on location has been determined. Hot site staffing will consist of members of the disaster recovery team only for the first 24-36 hours, with other staff members joining at the hot site as necessary.

Facility Requirements

Requirement	Description
Power	Generator or location with power
Infrastructure	Lan Drops, cabling,
Space	Closet, room to establish communication

If the facility director determines that the primary facility is no longer sufficiently functional or operational to restore normal business operations, the team will be instructed that the recovery of systems will be done at a determined recovery facility. Once this determination has been made, the facilities team will be

engaged to bring the alternate facility to a functional state. The facilities director will co-ordinate logistics to ensure that the team can operate out of the alternate site.

If the recovery facility is unavailable, the facilities team will look at hotels, other public buildings to see if they can provide the required space and power.

In accordance with our Business Continuity and Disaster Recovery (BCDR) plan, it is imperative to promptly notify WellCare in the event of activating an alternate plan for call handling or transferring workload to an alternate site. This notification ensures effective coordination and communication between our teams, enabling WellCare to adjust their operations accordingly and maintain service continuity. Timely updates regarding the activation, its duration, and any pertinent details facilitate mutual understanding and collaboration throughout the recovery process, ultimately minimizing the impact of disruptions on our services and ensuring a seamless customer experience.

3.2 INFRASTRUCTURE PLAN

List of Critical Infrastructure Services:

System
Voice Communications
Local Area Network (LAN)
Wide Area Network (WAN)
Server – Hosts
Storage – BCDR(Datto)
Core Network
Firewalls
Remote Connectivity

Voice Communications Service Recovery Plan

1. Contact DMS phone provider and redirect main numbers to the standby number designated by Leadership team.
2. Arrange for temporary lines (this may be in serviced office or at Director's location). This is only to be actioned if a significant long-term event has occurred, as line provision will take 10 days minimum.
3. Contact RingCentral VOIP provider and set up a temporary VOIP provision. Consider forwarding numbers to that system.
4. Test phone system functions, including inbound, outbound, voicemail, Caller Line Identification, call forwarding and hunt groups.

WAN/Local Area Network Recovery Plan

The Network Team will be responsible for assessing damage specific to any network infrastructure and for provisioning data and voice network connectivity including WAN, LAN, and any telephony connections internally within the organization as well as telephony and data connections with the outside world. They will be primarily responsible for providing baseline network functionality and may assist other DR Teams as required.

- *In the event of a disaster that does not require migration to / from NWFHN service centers, the*

team will determine which network services are not functioning at the primary locations

- *If multiple network services are impacted, the team will prioritize the recovery of services in the manner and order that has the least business impact.*
- *If network services are provided by third parties, the team will communicate and co-ordinate with these third parties to ensure recovery of connectivity.*
- *In the event of a disaster that does require migration to temp location and use of temp ISP providers, the team will ensure that all network services are brought online at the secondary availability location*
- *Once critical systems have been provided with connectivity, employees will be provided with connectivity in the following order:*
- *All members of the DR Teams*
- *All Executive Staff*
- *All IT employees*
- *All remaining employees*
- *Install and implement any tools, hardware, software and systems required in the standby availability zone*
- *Install and implement any tools, hardware, software and systems required in the*
- *After NWFHN is back to business as usual, this team will be summarizing any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster*

Server Recovery Plan

The following information outlines the plan to implement network and workstation computers in the event the current NWFHN offices is rendered unusable and all equipment is damaged. Every weekday a full backup and incremental backups are done of all the data files on the servers and synced to an offsite cloud.

In the event of a disaster to the NWFHN BCDR solution, DIS, our third-party support vendor can, recover our data in the DATTO Private Cloud immediately after a disaster and be up and running within 48 to 96 hours. DATTO Public Cloud Recovery, if all existing hardware is destroyed in a disaster, then new hardware would have to be procured, and professional services would be required to rebuild and recover the server environment. In the event of a catastrophe, fees for the “Disaster Recovery Service” will be $ 2,500.00 plus all applicable freight and shipment costs to deliver a new DRS that will contain the most current data loaded at the Data Center. Additionally, any service required to provide access to that data is included.

Each year, an emergency backup (current make/model) will be configured with the current NWFHN network/software and kept as part of the off-site backup and is accessible by the Technology Director. That computer backup will be kept up to date monthly, and will have all the additional application software that is needed to configure/image any NWFHN server and computer.

In the event of a disaster, the NWFHN will purchase approved make and model of laptops with the approved method and will have technicians to reload any new computers which have been purchased due to the disaster. It should be noted that all staff may have agency laptops at home, enabling those people to work

remote with limited access to email and access to the network drives. The new laptops will be distributed to any additional employees deemed necessary, based on need and whose computers have been damaged.

VPN software (or current remote connection software) will be installed and configured to work on the laptops. Laptops will be given to the appropriate personnel, so they can access server data files from a remote location. The remote location would need internet connectivity (such as a home, office, hotel with wireless internet connectivity). Currently laptops are configured to connect through wireless.

When new computers are purchased, the Adobe software will be loaded for those who need it. As part of the disaster recovery plan, all email will be accessible via login to office.com online if access to provided computing equipment is not available. Personal Folders and information that is kept locally on the computer is backed up every two months, so depending on when the disaster occurred, some information may be unrecoverable if it was stored locally on the machine.

This section explains where all of the organization's data resides as well as where it is backed up. Use this information to locate and restore data in the event of a disaster.

Rank	Data	Data Type	Back-up Frequency	Backup Location/DATTO Solution Backup Product (Cloud Backup / Reflection)
1	MIP	Financial	Daily	NAS, onsite Datta, Datto Cloud
2	BBCBC1	Shared Files Print Server	Daily	On prem Datto, Datto Cloud
3	NWFHN-DC1-PAN NWFHN-PAN	Domain Controller Shared File Access	Daily	On prem Datto, Datto Cloud
4	NWFHN-DC1-MLK	Domain Controller	Daily	On prem Datto, Datto Cloud
5	NWFHN-DC-THA	Domain Controller	Daily	Onprem Datto, Datto Cloud
6	BBCBC-THA	Shared File Print Server	Daily	On Prem Datto, Datto Cloud
7	BBCBC-MESQRT	ME Data Reporting	Daily	NAS, Synology Cloud

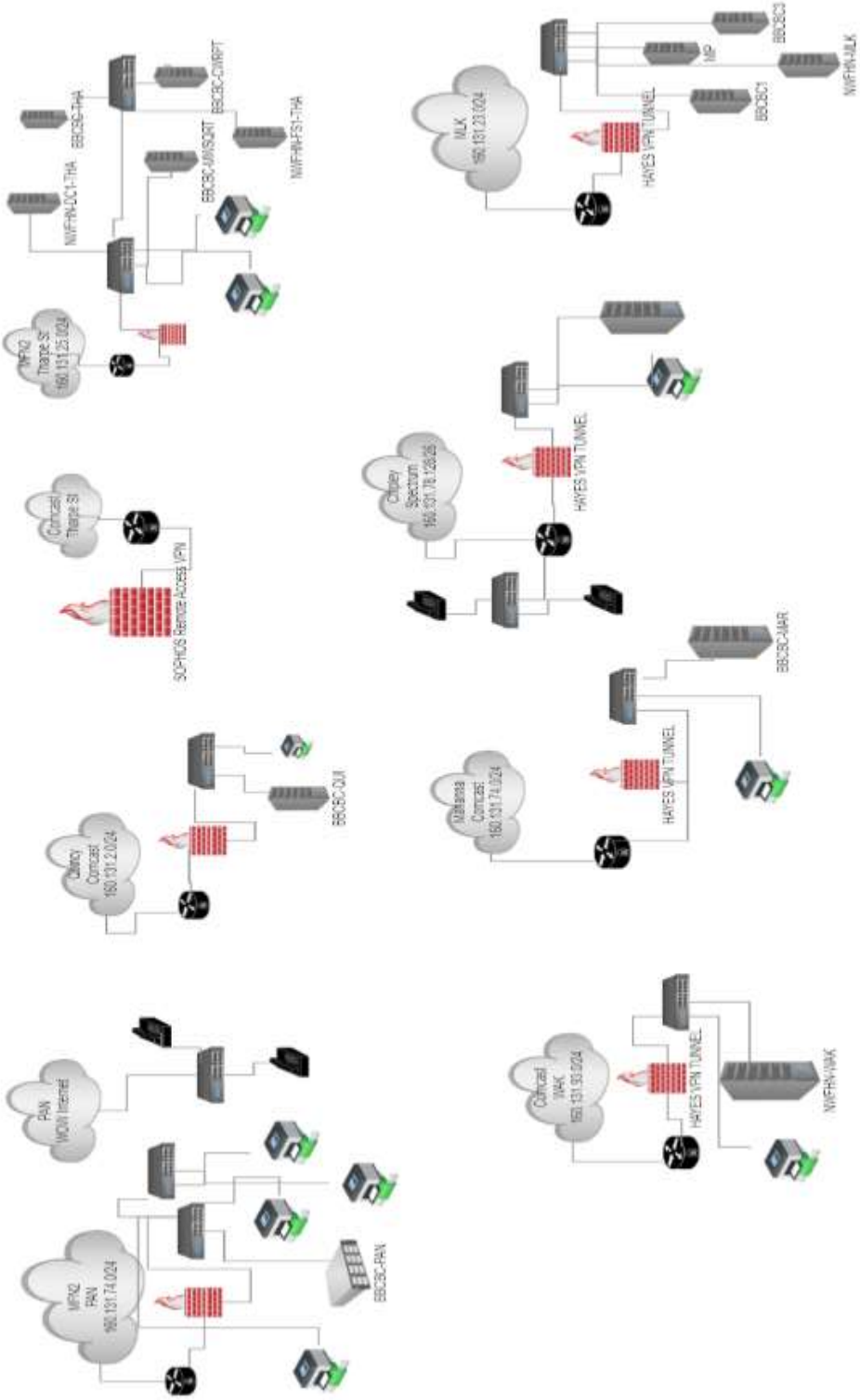
Storage Recovery Plans

- When possible, the desire is to recover data as rapidly as possible and ensure that the redundancy systems have kicked in and determine the need for intervention. Secondary to that, if there is a system failure, recover data as rapidly as possible to either a standby server or to a server of equal capability to ensure that staff access to network resources is minimized and remain online.
- In the event of catastrophic data center loss, recover the data from the DATTO Cloud SAN and begin the process of acquiring and rebuilding servers utilizing disk imaging system to assist with rapid deployment of servers into the domain.

Core Network Recovery Plans

Should a disaster actually occur and NWFHN need to exercise this plan, this section will be referred to frequently as it will contain all of the information that describes the manner in which NWFHN's information system will be recovered.

Current System Architecture



Firewalls Recovery Plans

Should the firewall appliance be damaged, another would need to be ordered via DMS or NWFHN approved reseller to replace the damaged item. A SunCom service request would need to be initiated to have the new device programmed for NWFHN and State access.

Dedicated high-performance Cisco ASA/Sophos XGS firewalls are used to achieve complete isolation between environments. Because our security needs are unique, and we are dedicated to the security of NWFHN data, our staff work directly with the firewall administrators at Hayes Computing and our MSP to tune our firewall rules for your data security. The Firewalls limit ingress and egress traffic, perform stateful packet inspections and establish VPN connectivity to our offices and for our remote users.

IT Systems

NWFHN's IT Systems in order of their criticality and each system's components that will need to be brought back online in the event of a disaster.

Rank	IT System	System Components (In order of importance)
1	Active Directory	Bbcbc.mis AD Domain(s)
2	MIP	NWFHN-MIP
3	Shared File resource(s)	BBCBC1, BBCBC-THA, NWFHN-PAN, BBCBC-MAR, BBCBC-CHI
4	Data Reporting	BBCBC-MESQRT, BBCBC-CWRPT
5	IT Image Deployment	NWFHN-FS1-THA
6	Sophos central	Sophos Cloud

Connectivity

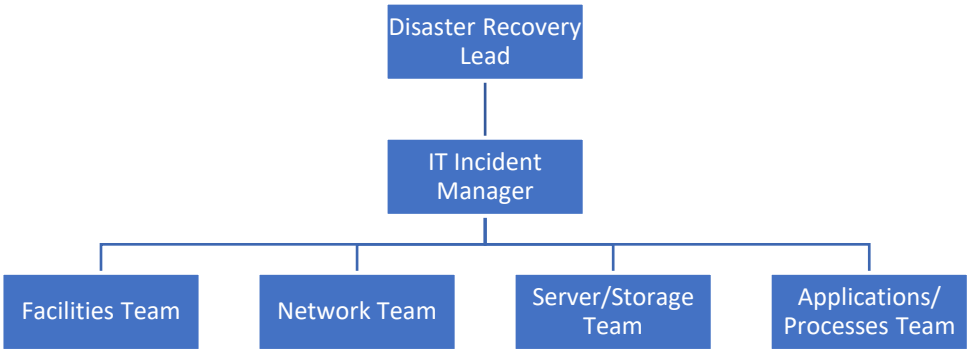
PROVIDER	CIRCUIT TYPE	BANDWIDTH	CPE	CPE GEAR MODEL	ADDRESS	ONSITE LOCATION	NOTES
MetroNet	Internet	1GB	No	Sophos XG310	1000 W Tharpe St Ste #15 Tallahassee, FL 32303	Network Closet FLoor 2 Rack	Primary Internet Circuit
Comcast	Internet	1GB	No	Sophos XG310	1000 W Tharpe St Ste #15 Tallahassee, FL 32303	Network Closet FLoor 2 Rack	Internet Circuit (Partners)
MetroNet	Internet	1 Gbps	Yes	Cisco ASA	525 N Martin Luther King, Jr. Blvd Tallahassee, FL 32301	Network Closet 2nd FLoor rack	Fiber Internet Circuit Hayes VPN
Comcast	Internet	1 Gbps	No	Cisco ASA	69 High Drive Crawfordville, FL 32327	Network Closet First FLoor Closet	Internet Circuit Hayes VPN
Comcast	Internet	1 Gbps	No	Cisco ASA	305 W Crawford St Quincy, FL32351	Network Closet First FLoor Server Room	Internet Circuit Hayes VPN
Comcast	Internet	1Gbps	No	Cisco ASA	4152 Jireh Court Marianna, FL32448	Network Closet First FLoor Server Room	Internet Circuit Hayes VPN
Spectrum	Internet	1Gbps	No	Cisco ASA	1352 South Boulevard Chipley, FL 32428	Network Closet	Hayes VPN Tunnel
MFN2	Internet	45 Mbps	Yes	Sophos XGS3100	910 Harrison Ave Panama City, FL32401	Network Close 1st FLoor Server Room	Primary Internet Circuit
WOW	Internet	1Gbps	No	Sophos XGS5100	910 Harrison Ave Panama City, FL32401	Network Close 1st FLoor Server Room	Internet Circuit (Partners)

4. PLAN IMPLEMENTATION

4.1 ROLES AND RESPONSIBILITIES

IT Disaster Recovery Team Organizational Chart

The following chart shows the key roles involved in preparing for and responding to a disaster. It also shows that the IT incident manager usually reports to an incident commander who is in charge of the overall response to a disaster.



Disaster Recovery Team Lead

NWFHN Management would designate staff to fulfill this role. COO, etc.

Incident Manager (IT Lead)

The disaster recovery incident manager is responsible for making all decisions related to the IT disaster recovery efforts. This person's primary role is to guide the disaster recovery process. The entire IT recovery team reports to this person during an incident.

Responsibilities

- Initiate the IT disaster recovery call tree.
- Provide status updates to senior leaders and information needed for making decisions.
- Co-ordinate communications.

Facilities Team

The facilities team is responsible for all issues related to the physical facilities that house IT systems, including both the primary and recovery facilities. They also are responsible for assessing the damage and overseeing the repairs to the primary location in the event of the primary location's destruction or damage.

Responsibilities

- Ensure that the recovery facility is maintained in working order.
- Ensure transportation, sufficient supplies, food and water and sleeping arrangements are provided for all employees working at the recovery facility.

- Assess physical damage to the primary facility.
- Ensure that measures are taken to prevent further damage to the primary facility and appropriate resources are provisioned to rebuild or repair the main facilities if necessary.

Network Team

The network team is responsible for assessing damage to network infrastructure and for providing data and voice network connectivity during a disaster.

Responsibilities

- Assess damage to network infrastructure at the primary facility and prioritize the recovery of services in the manner and order that has the least impact.
- Communicate and co-ordinate with third parties to ensure recovery of connectivity.
- Ensure that needed network services are available at the recovery facility (if needed).
- Restore network services at the primary facility.

Server/Storage Team

The server/storage team is responsible for providing the physical server and storage infrastructure required to run IT operations and applications.

Responsibilities

- Assess damage to servers/storage and prioritize the recovery of servers and storage devices in the manner and order that has the least impact.
- Ensure that servers and storage services are kept up-to-date with patches and copies of data.
- Ensure appropriate back-ups.
- Install and implement required tools, hardware and systems in the facilities.

Applications and Processes Team

The applications and processes team are responsible for ensuring that all applications operate as required to meet organization objectives as well as managing IT processes that are fundamental to support the recovery of IT services and applications (for example: incident management, change management, etc.).

Responsibilities

- Assess impact to applications and prioritize the recovery of applications in the manner and order that has the least impact.
- Ensure that the following IT processes are followed when managing applications:
    - incident management;
    - change management;
    - access provisioning;
    - security; and

- other.

- Ensure that servers in the facilities are kept up-to-date with application patches and copies of data.
- Install and implement any tools, software and patches required in the facilities as appropriate.

CALL LIST

Name	Role/Title	Work Phone	Mobile Phone
Courtney Stanford	COO	(850) 747-5755	(850) 850-5846
Rae Kerr	CFO	(850) 410-1020	(850) 363-9204
Kervin Rene	IT Manager	(850) 250-2772	(850) 545-8661
Todd Gainey	Facilities Director	(850) 410-1020	(850) 510-0972

4.2 DISASTER RESPONSE PROCESSES

Responding to a disaster occurs in several phases as shown below. After an event occurs, the team assesses the event and determines whether to declare a disaster. If a disaster has occurred, the team initiates recovery of the IT service(s), in an alternate location if necessary. Once required IT services are up and running, the team can focus on resuming normal operations. The final phase is to conduct a post-event review to discuss lessons learned and ways to improve the process.

Processes for Assess Phase

Process to Assess Severity of Incident or Event

Response

1. Do not turn on electrical equipment if corrosive contaminants are present or if the power supply is unreliable.
2. If applicable, disconnect all electrical equipment. As a safety precaution, first disconnect electrical power at the main circuit breaker.
3. Contact telecommunication providers.
4. Assess damages, identify destroyed & salvageable equipment, and send assessment to the ERT.
    - Computers
    - File Servers
    - Telecommunication Equipment
    - Peripheral Equipment
    - Data
    - Other
5. Be prepared to implement the Disaster Recovery Plan.
6. Be prepared to activate the IT Alternate Site Plan.
7. Order replacement equipment if the disaster is clearly restricted to hardware.
8. Contact critical suppliers and vendors.

Processes for Recover Phase

Recovery

1. Initiate the Service Center cleanup, reconstruction and/or relocation efforts.
2. Relay information regarding personnel to Administration.
3. Maintain the IT Alternate Site.
4. Contact critical subcontractors and vendors.
5. Make critical (if only temporary) repairs.
6. Repair salvageable equipment and institute the replacement of critical equipment.
7. As soon as a physical facility with reliable power and communication capability is secured, initiate the replacement of destroyed or disabled equipment.

Long Term

1. Review the Department Plan.
2. Review vendor, subcontractor and supplier performance.

PRIMARY RECOVERY RESPONSIBILITIES

1. Execute the Disaster Recovery Plan.
2. Execute the IT Alternate Site Plan if directed.
3. Systems support to mission-critical business services.
4. Telecommunications to mission-critical business services.
5. Assess damage to workspace & equipment.

4.3 IT SERVICE RECOVERY PLANS

Sample List of IT Services:

System
Payroll
Shared Files

Payroll Service Recovery Plan

The accounting department within NWFHN uses application software called MIP. It is connected to BBCBC3 server via the Internet and accessed through the Intranet and SOPHOS VPN. It is configured and to run remotely via BBCBC3 servers at MLK office. In the event the MLK office is destroyed, the accounting department could access MIP from a remote location through VPN. The backup server for NWFHN is at the MLK office. In the event that a service center was destroyed, the BCDR server would be used to run the MIP Software. The accounting department could access If both Tharpe St and the MLK offices were destroyed, a third plan would have to be negotiated with DATTO to recover the offsite cloud backups from their backups, have the Vendor restore the application on a Virtual server to restore functionality while the restore of data from the cloud is performed on physical servers.

NWFHN would be able to use the existing licenses for O365/Adobe Acrobat DC, and Sophos for any equipment that needs to be purchased. All other software is on the servers and included on the emergency backups.

A few printers may also have to be purchased and or leased from OBS depending on the set of circumstances.

Shared Files

In the event of a disaster to the NWFHN service center locations, DIS, our third-party support vendor can, to a degree, recover our data in the DATTO Private Cloud immediately after a disaster and be up and running within 48 to 96 hours. DATTO Public Cloud Recovery, if all existing hardware is destroyed in a disaster, then new hardware would have to be procured, and professional services would be required to rebuild and recover the server environment. In the event of a catastrophe, fees for the "Disaster Recovery Service" will be $ 2,500.00 plus all applicable freight and shipment costs to deliver

a new DRS that will contain the most current data loaded at the Data Center. Additionally, any service required to provide access to that data is included.

5. PLAN TESTING

Disaster recovery plan reviews are an essential part of the plan development process. Building a quality IT disaster recovery plan is a team activity, so practice and testing are critical to success.

Periodic disaster recovery plan reviews need to happen, because non-technical changes can affect the plans.

1. Reflect any updated organizational priorities, changes or goals.
2. Ensure that all team lists are up to date.
3. Ensure that call lists are up to date.
4. Confirm that changes due to configuration changes in the environment have been made.

The goal of a good disaster recovery plan is that it can be executed smoothly and effectively at any time. To make this happen, everyone that has a role to play in the plan needs to be involved in practicing.

The disaster recovery plan will be tested every six months in order to ensure that it is still effective. Each period, a table top walkthrough, disaster simulation, or full failover testing will be executed (see step 5.4 in the *IT Disaster Recovery Planning Guide* for more details about the different types of tests).

On a regular basis, the IT Manager shall:

1. Ensure IT employees are familiar with the Emergency Response Plan for Employees and know what to do in an emergency situation.
2. Backup critical data daily and regularly secure this information at an offsite location.
3. Maintain documentation for, and back up of, all electronic equipment, software and system configurations.
4. Keep records of all software purchases and licenses.
5. For critical subcontractors and suppliers, specify at least one of the following:
    - Insist that they have an effective emergency plan that will enable them to continue to provide services/supplies in the event of a disaster at their business.
    - Identify backup subcontractors and suppliers. (This is especially important for local providers that are also vulnerable to the same local community-wide disasters.)
    - Do business with multiple subcontractors and suppliers.
6. Maintain the IT department's Disaster Recovery Plan (DRP).
7. Develop and maintain an IT Alternate Site Plan.
8. Identify all important equipment and document the vendor(s), alternate vendor(s), estimated replacement time, and level of importance.
9. Update anti-virus software on a regular basis and maintain an Information Security Plan.

APPENDIX A – IT DISASTER RECOVERY PLAN MAINTENANCE

Over time, the disaster recovery needs of NWFHN will change. The following responsibilities and processes need to be executed to ensure a useful plan remains in place.

RESPONSIBILITY FOR IT OPERATIONS

The IT operations team will be responsible for the day-to-day management of the disaster recovery plan. The specific responsibility is delegated to the change advisory board (CAB). Whenever changes are made to the environment CAB is responsible for ensuring that they are fully reflected and tested in the disaster recovery plan.

This will make updating the disaster recovery plan a part of the formalized change control procedures under the management of the IT director.

PROJECT TEAM RESPONSIBILITIES

Each project will, as part of their transition to operations, plan to ensure that all documentation related to recovery of the system is updated when making a change.

DOCUMENTATION STORAGE

Each member of the disaster recovery team will be issued copied with the disaster recovery plan documentation. A master copy will be stored in a shared resource location. Printed copies of the plan are to be kept with all IT staff.

APPENDIX B – CRITICAL SERVICES

The following list contains critical services that NWFHN typically provide.

Department	Critical Services or Functions
Finance	• Cash and liquidity management • Receiving and paying invoices and disbursements
Human Resources	• Corporate communication • Moral support • Processing payroll
Facilities	• Emergency property acquisition and infrastructure setup • Physical security • Contract services and unplanned maintenance • Providing utilities (power, gas, water and sewage)
Information Technology	• Help desk • Access management • Change management • IT procurement • Request fulfillment
Others	• General council • Critical incident response team

APPENDIX C – SERVICE RECOVERY PLAN

Responsibility

Service Recovery is managed by the IT Manager and IT Project Coordinator in the event the IT Manager is not available.

Service Context

MIP

1. Accounting/Finance – Finance Department
2. Payroll processing - Weekly Check runs or year-end processes
3. IT Project Coordinator will be the POC and liaison to MIP support with IT Manager as backup.

Service Classification

MIP – Critical
Shared Files Access - Critical

Recovery Strategy and Location

1. Execute the Disaster Recovery Plan.
2. Execute the IT Alternate Site Plan if directed.
3. Systems support to mission-critical business services.
4. Telecommunications to mission-critical business services.
5. Assess damage to workspace & equipment.

Assumptions

Provided power, internet connectivity, and hardware is available to perform restoration.

Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

MIP – RTO is averaged to be about 6 hours and RPO of about 12 hours
File Shares is averaged RTO of 12 hours and RPO up to 36 Hours

Recovery Platform

Datto SaaS Cloud recovery portal will be used to perform the restoration of this service.

Recovery Procedure

Response Levels

- Critical (Priority 1 – 1 hour)
  - The problem results in extremely serious interruptions to the system. It has affected, or could affect, all users. Tasks that should be executed
  - immediately cannot be executed because of a complete crash of the system or interruptions in main functions of the system.

- Urgent (Priority 2 – same business day)
  - The problem results in serious interruptions to normal operations. Important tasks cannot be performed, but the error does not impair essential operations; processing can still continue in a restricted manner. The problem hinders productivity by users. The service request requires timely processing, because a long-term malfunction could cause serious interruptions to several users or negatively impact business decisions.

- Important (Priority 3 – next business day)

- The problem causes interruptions in normal operations. It does not prevent operation of a system, or there could be minor degradation in performance. The error is attributed to malfunctioning or incorrect behavior of the software. The issue will only affect a few users or there is a reasonable way to work around the issue temporarily.

- Minor (Priority 4 – three business days)
  - The problem results in minimal or no interruptions to normal operations (no business impact). The issue consists of "how to" questions, configuration inquiries, enhancement requests, new reports, or documentation questions.

- If NWFHN Support estimates that a reported technical issue or business situation requires additional attention, an internal management escalation procedure will be followed. A management escalation process will be enacted when response-time targets are, or will be, exceeded, when a Work Order is necessary.

The following are the steps associated with bringing NWFHN critical servers back online in the event of a disaster or system failure.

Step	Action	Responsible Party
1	If no damage to physical hardware, Access DATTO VM for on premise data copies	IT Manager
2	Initiate virtual share copies of the affected resource, provision/share resource for staff access.	IT Manager
3	Enable network resource is available for staff	IT Manager
4	Procure replacement hardware, rebuild server	IT Manager
5	Restore data to server, provision security access, restore file server access	IT Manager

Test Procedure

1. Server Maintenance
   a. Scheduled Maintenance
      - NWFHN reserves a monthly maintenance window during the third week of the month between the hours of midnight and 3:00 AM EST to apply security updates, patches, and other software related updates that require a reboot of a system. Total downtime of a server should not exceed 15 minutes and could occur at any point within this window. For all Accounting staff, we will schedule this maintenance as best as we are able in accordance with your work schedules to ensure no disruption of service during your primary business hours. Clients will receive a notification via email at least 24 hours prior to any other scheduled out-of-band maintenance not within this window.

   b. Emergency Maintenance
      - If unplanned downtime occurs or is required to restore the availability of any server/services, all efforts will be made to notify clients. Various means of communication will be used, which may

include email, tickets, or phone call.

2. Monitoring Service
    - NWFHN employs James Moore for enterprise-level monitoring service to alert technicians to any potential issue in availability of any service. Technicians are on-call 24/7 if any alerts are received and issue will be analyzed immediately.

3. Service Level Agreement
    a. Network Uptime
        - NWFHN data center network has 99.9% uptime in a given month, excluding scheduled maintenance. The data center network NWFHN manages consists of switches, routers, and cabling.

    b. Infrastructure
        - NWFHN Tharpe St data center HVAC and power has only power backups to include UPS's, PDU's, and cabling. Infrastructure downtime exists when a particular server is shut down due to power or heat problems.

    c. Hardware
        - NWFHN employs redundant hardware systems where possible to prevent downtime related to hardware failure. If a failure occurs hardware will need to be replaced and staff will be notified if any downtime results. All hardware has a maximum life of 4 years and is replaced routinely without interruption of service.

APPENDIX D – SAMPLE VOICE COMMUNICATIONS SERVICE RECOVERY PLAN

Responsibility

- Kervin Rene, IT Director, Communications
- Backup:

Priority

Critical

Recovery Strategy and Location

- The updated procedure will be available when the standby arrangement with the third-party technology partners is determined. The current solution requires a disaster recovery team member to contact DMS to forward the main phone line to a standby line with a pre-recorded message.
- Acquisition of systems necessary for telephone communications. Contact RingCentral to prepare for the VoIP recovery & local phone vendors for Analog phone service once service has been restored.
- Telephone system will be restored at the DMS vendor data centre. Future strategy may change if the telephone system (partially or as a whole) will be migrated to an alternate location for daily operations.

Assumptions

- Necessary servers will be set up on a **best effort basis**.
- A standby arrangement with third party technology partners will be established in the future.
- A critical escalation support arrangement with third party technology is available.
- The configuration information can be restored from backup.
- Two telephone lines are readily available. One for customer broadcast and one for internal communication.

Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

- RTO: Best effort.
- RPO: Best effort.

Recovery Platform

Cloud based servers and DMS providers service restoration with similar configuration as in production environment.

Recovery Procedure

- The procedure will be updated when the standby arrangement with the third-party technology partners is determined. The following steps will be implemented:
    - Contact RingCentral to arrange technical support. When the recovered server is available, arrange RingCentral technician to restore/install the phone system.
    - Contact DMS to provide update on phone service restoration and alternative options for analog phone service.
- As a short-term solution, voice mailboxes can be arranged in advanced and pre-recorded messages can be implemented to keep customers and business partners aware of the incident status. The following phone lines will be addressed by the following procedure:
    - Reception phone number 850-410-1020 and line 850-747-5755 will share the standby line.
    - Other lines.
- During an incident, our designated member(s) will contact DMS using the contact information documented in NWFHN Vendor Escalation Contact List to activate the re-route. RTO can be revised once this solution is established.

- For fax services, our designated member(s) will be able to utilize RingCentral to start sending/receiving faxes. The designated member will follow the procedure documented in IT Operations Manual to retrieve the fax emails.

Test Procedure

- Logon to RingCentral portal as administrator. Connect to RingCentral Console and retrieve historical data to confirm connectivity.
- Follow up with SUNCOM to ensure analog services have been restored for DMS phone accounts.

Resume Procedure

- Contact RingCentral to arrange technical support. When the production server is available, arrange RingCentral technician to be on-site and transfer the configuration and user data from recovery system.
- Contact DMS to switch the main line back to the phone system.
- Login to RingCentral to redirect the faxes back to main fax line.

APPENDIX E – LOCAL AREA NETWORK RECOVERY PLAN

Responsibility

- Kervin Rene, IT Manager, Communications
- Jillian Jamison IT Project Coordinator

Priority

Critical

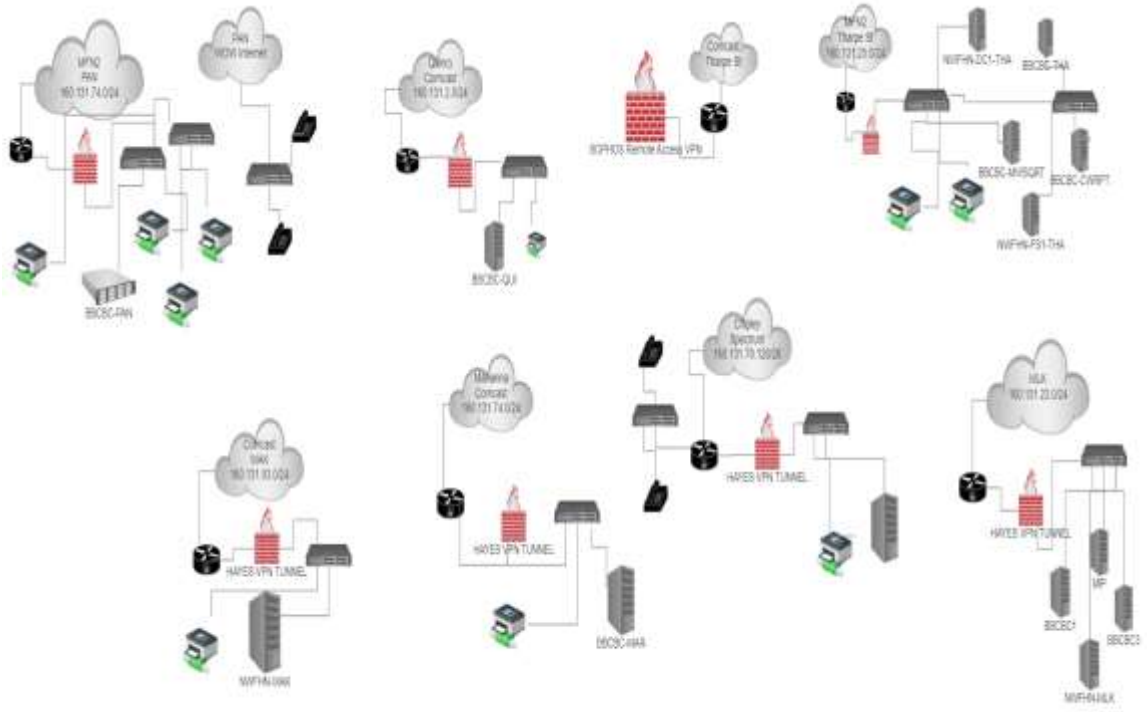
Recovery Strategy and Location

Determine if connectivity is available, assess switch hardware(s), if needed replace hardware, reconfigure switch for network access

Assumptions

- Racks and power are available
- Other

Network Diagram



Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

- RTO: 6 hours.
- RPO: 12 hours.

Recovery Platform

Datto/Datto Cloud, Synology NAS/Cloud….

Recovery Procedure

Overview of major steps:

1. Rack Gear
2. Patch to switches

3. Configure Router

Details for each step:

1. Rack Gear

    - Mount Gear
    - Confirm power
    - Patch to Servers
    - Connect to WAN
    - Login and update switch
    - Configure rules

APPENDIX F – GLOSSARY

APPLICATIONS AND SERVICES

Identify any IT applications or IT services required for the completion of the identified processes. Consider applications that are both supported internally and through third party vendors or are located in the cloud.

BUSINESS IMPACT

A business disruption can impact an organization in several ways. There are five main categories that are used to measure impact:

- safety/human life;
- financial;
- reputation;
- operations; and
- regulatory/legal/contractual.

Impact Rating

In order to effectively assess the impact of a disruption throughout the organization, it is necessary to use a common metric to assess impacts across the various business services and their individual processes. For each of the identified processes, identify the impact in each of the applicable categories based on the values found in the table below. Note that it may be prudent to give dollar figures for the financial and regulatory/legal/contractual categories where the loss exposure (the amount of potential monetary losses) is a known amount.

The timeframe for the impact should be based on the time-sensitivity values previously identified.

Rating	Description / Example
Catastrophic	The consequences would threaten the provision of essential school authority processes, causing major problems for clients and require immediate executive involvement and action. Disruption would have extreme consequences for school authority (e.g., major damage or destruction, imminent threat to human safety, loss of life or major/multiple injuries, extreme monetary losses to school authority).
Major	The consequences would threaten continued effective provision of school authority processes and require executive involvement. Disruption would have very high consequences for school authority (e.g., significant damage or destruction, some minor injuries or threat to human safety with no loss of life, high monetary losses to processes).
Moderate	The consequences would not threaten the provision of school authority processes, but would mean the business operations and administration could be subject to significant review or changed ways of operating. Executive involvement would likely be required. Disruption would have medium consequences (e.g., no loss of life or injuries, moderate monetary losses to school authority).
Minor	The consequences would threaten the efficiency or effectiveness of some school authority processes but would be dealt with at the business unit or department level. Disruption would be of low consequence to school authority (e.g., no loss of life or injuries, low monetary losses to school authority).

CRITICALITY PERIOD

A criticality period is any point during which the identified process is critical and may affect the recovery time objective (RTO).

It is possible that a process may have multiple criticality periods or none at all; this is highly dependent on the nature of the process. Criticality periods may be cyclical or one-offs and may range from months to hours in length.

Examples of criticality periods include:

- year-end processing;
- regulatory deadlines;
- payroll processing; and
- scheduled events.

A manual workaround is a non-IT dependent action undertaken to circumvent the loss of IT systems in order to complete a process. Manual workarounds are usually short-term stopgaps and are not intended to be implemented indefinitely.

Identify any manual workarounds that may exist for each of your processes.

KNOWN RISK

A known risk is anything that may negatively impact business as usual. Identify any concerns or threats you have identified or feel may affect your normal operations.

PROCESS

A process is a service the business unit carries out in the course of normal day-to-day operations. It is essential to account for all processes when conducting a business impact analysis in order to assign categories of time-sensitivity and tailor contingency plans accordingly.

RECOVERY POINT OBJECTIVE (RPO)

The goal for the point at which to restore data or information after a disruption (based on the acceptable amount of data or information loss)[1]. For example, a recovery point objective of 6 hours for payroll services means that the payroll data must be backed-up every 6 hours so that no more than 6 hours of data entered into the payroll application is lost after a disruption.

RECOVERY TIME OBJECTIVE (RTO)

The goal for how fast to restore technology services after a disruption (based on the acceptable amount of down time and level of performance)[1]. For example, a recovery time objective of 24 hours with local accessibility for payroll services means that the payroll application must be up and running within 24 hours as well as accessible locally.

SERVICE CLASSIFICATION

Classification	Maximum Recovery Time
Critical	within 24 hours
Vital	within 72 hours
Necessary	within 2 weeks
Desired	longer than 2 weeks but necessary to return to normal operating conditions

SERVICE TIER

The logical grouping of services to be recovered such as Tier 0, Tier 1, etc. Core infrastructure services need to be recovered first and would be included in Tier 0. Lower numbered tiers are recovered first as they are either more critical or higher numbered tiers depend on them in order to function.