NIPEC/16/07

NIPEC

NORTHERN IRELAND PRACTICE AND EDUCATION COUNCIL FOR NURSING AND MIDWIFERY

IT Contingency Policy

February 2016

Review date: March 2017

Centre House
79 Chichester Street
BELFAST
BT1 4JE

Tel: 0300 300 0066

www.nipec.hscni.net

CONTENTS

1 Introduction

This Contingency Plan is a tested plan for the rapid recovery of a computer network in the event of fire, flood, or any other disaster to the building that NIPEC is currently resident. It provides an organised method for restoring the network to a usable level that will support crucial business functions during times of emergency or until full and permanent operations can be restored. In addition, it defines the responsibilities of each person expected to play a role during the emergency.

The IT Contingency Plan addresses the elements necessary to ensure continuity of service for the network and to minimise the impact of potential catastrophes by:

- Reducing the likelihood of disaster, through preventive measures, which encompass the areas of the personnel, maintenance, security, equipment, communications, and software.

- Planning a structured response to the events and eventualities that may beset the computing environment, ensuring that not only the procedures, but also the responsibilities, are well defined.

If followed, the disaster recovery and contingency planning practices will help to ensure a more reliable day-to-day processing environment as well as reduce the exposure to major interruptions of service.

The network is a Cat 6 cable environment, on which is running a PC Platform using the Windows 8 Operating System. All machines should connect to a server, located within BSO ITS ITS, daily on start-up. In addition, this server also acts as a Blackberry BES Server, which carries out all operations relating to the handheld Blackberry Leap handheld devices currently providing access to emails and internet to 9 members of staff within the organisation. All network traffic is controlled by a Switch (Cisco C3KX-NM-1G, which offers the organisation a speed of up to 1 Gb per second and permits fast data transfer within the network.

The total number of machines at time of writing is 24, (including 3 Laptops). External to the network, NIPEC also has 9 laptops, and for the purposes of this policy, these will also be included.

All enquires about any part of the computer network, should be forwarded to the IT & Communications Manager on 028 9089 4041 (direct) or 0300 300 0066, extension 21.

2 Physical Security

The most important and often overlooked feature of physical security is that the protection should be consistent with the risk. Physical security at Centre House should be planned and supervised in co-ordination with data security, but with consideration for the unique features of the Building.

2.1 Physical Security Objectives

Physical Security Objectives are currently in operation through the security of admission into the building complex, and a further security code is required before entry to the NIPEC offices are permitted.

Each staff member is allocated an identity card with his or her photograph, and any visitors must be signed in at the building security reception (Ground Floor, Centre House).

Access into the computer room on the second floor, is restricted to the IT & Communications Manager (who requires entry on a daily basis, mainly for backup purposes) and any other appropriate staff who are deemed necessary. The computer room is protected through a pass code mechanism, to increase security. This pass code is known by a number of key people within the organisation. All other rooms (with the exception of the filing store, which has its own keypad pass code security) are viewed as low risk, and therefore there are no security restrictions to other members of staff.

2.2 Risk Analysis

Centre House is amongst the government offices of Chichester Street. It operates an Access control to the building (including parking outside), to persons attempting to gain entry. The owners of the building employ the security staff for the building and they are managed by the landlord’s agent for the property.

The NIPEC has two recognised fire exits, both situated to the south of Centre House, one at the rear of the NIPEC offices, and the other staircase number 2 near the front entrance of NIPEC office space. The floor occupied by NIPEC has three sets of double fire doors, which in the event of a fire will limit the spread of the fire. At present, there is no provision of an adequate Reliable electrical power backup should the electricity be interrupted. In the event of such an event, NIE would be called to remedy the problem.

Each room is fitted with a radiator, which is regulated by thermostats located in several locations around Centre House, and overall controlled by a heating panel located at the rear fire exit, although an element of local temperature adjustment is available via staff members within the office.

As with all government buildings, there exists a vulnerability to bomb threats or other violent activities. It is therefore vital that all staff should be on guard for any persons not wearing visitors’ badges, who are walking around the NIPEC unattended. It would also be advisable for staff to back-up files to the server when and where they feel the need arises. Staff should be reminded that only the files on the server, are backed up, and that any other files will not be able to be restored following any event.

2.3 Physical Protection Strategies

The computer room is located in a part of Centre House, which ensures that the majority of staff do not have to be aware of its existence. This isolated part of the building ensures that in the event of something occurring within NIPEC, the room has a reduced chance of being affected. The computer room has a totally separate environment in terms of access control and support systems, and therefore access restrictions are in place to ensure a continuation of the service currently provided.

2.4 Physical Security - Physical Protection and Protection Systems

Physical security is commonly divided into two areas:

1. Physical protection, protection of assets by physical means (security guards at specific entrances, door and window locks, etc.)

2. Protection systems; protection of assets via electronic means (smoke/fire alarms, water detection equipment, etc.).

2.4.1 Physical Protection

Access control is a critical and important facet of physical protection. Access control techniques are designed to limit access to particular areas to users with a legitimate need. Access control techniques should be built on three basic principles:

- Access control - Prohibiting unauthorised access to data processing resources.
- Use Control - Prohibiting unauthorised use of these resources.
- Monitoring - Recording the use of these resources.

Currently, visitors to Centre House are issued temporary visitor badges which they are required to wear for identification while in the building.

A keyed entry lock currently protects the office occupied by NIPEC, with the doors to this floor being locked at all times, via a chubb key pad security system. This facility lock combination is changed at designated intervals.

Individuals who require occasional access to the computer facility are escorted by an authorised person, and are required to sign in and out of a logbook kept for this purpose, so that a precise record of access may be kept. The log includes the person's name, the time that they entered, the purpose for which they entered, and the time they left. If escorted, the name of the responsible party also is included.

To enhance the effectiveness of access control and monitoring, personnel policies at the site support its importance by instituting and enforcing appropriate penalties for infractions of these procedures.

2.4.2 Protection Systems

Smoke detection equipment is strategically placed throughout the NIPEC offices, as well as the computer facility, and batteries are checked regularly.

2.5 Facility Centre Practices

The computer facility is a controlled environment. Those who require access to it are informed that certain substances and mechanical devices that may pose a threat to equipment are not permitted within the facility, namely, food, beverages, smoking, or magnetic devices.

3 Logical (Software and Data) Security

The major emphasis of logical or data security is the limiting of access to a system and its data, through software controls, such as passwords, and software configurations that make it difficult for data to be accidentally modified or deleted.

A major risk to a system and its data is always the threat of accidental or intentional modification or deletion of data. This risk comes from two sources

1. Unauthorised personnel gaining access to system, network, or data files;
2. Existing or recently terminated employees accidentally or intentionally accessing, modifying, or deleting files.

Both are preventable by sensible personnel policies regarding information systems, stringent physical security, and logical security measures.

3.1 Access to System Software

In the NIPEC, no personnel other than the IT & Communications Manager and BSO ITS ITS Support Team staff are granted access to system software files.

3.2 Access to Network Software

No personnel other than the IT & Communications Manager, BSO ITS ITS Support Team staff and contractors specifically charged with network management and support are allowed to access Network software.

3.3 Access to Data Files Stored on the Network

Controlling access to data files is the most important charge of the IT & Information Officer regarding the logical security of the network. The network has been set up to provide two layers of internal security which will be utilised by the IT & Communications Manager.

- **Passwords** User passwords are assigned by BSO ITS ITS. This protects the NIPEC System against unauthorised users as long as the passwords are kept secure.

- **Administrator Authorisations** Allows BSO ITS ITS and the IT & Communication Manager to set certain high-level functions within the NIPEC System.

These features provides good data security, except when users are given supervisor permissions to avoid the time-consuming necessity of supervisors having to remove holds at each workstation during normal processing. The practical consideration of streamlining work procedures has as a consequence removed the risk of potential accidental deletions.

3.4 Password Procedures

The network allows the IT & Communications Manager and BSO ITS ITS to specify the length of passwords (The default length is eight characters). The IT & Communications Manager should instruct users to select a password that others in the office are not likely to hear in conversation or associate with the user, for example, names of family members are not advised. It should be at least five characters, and should use at least one numeric digit somewhere in the password. Embedded underlines also make it more difficult for someone to guess the password.

Passwords are not written down, and no list of passwords is printed out. Only BSO ITS ITS have the ability to reset network passwords. In addition, users are instructed to change passwords regularly, approximately once every 40 days, as it decreases the likelihood that others will discover the password.

When an employee retires or leaves the employment of the NIPEC, the IT & Communications Manager immediately will raise an INFRA request to lock the user out of the network by altering the password. This guards against the possibility of destructive activity.

3.5 Work Procedures

Although the NIPEC System allows users to stay logged on all day, they should always log off or lock the screen if they will be away for more than a few minutes. This provides less opportunity for another person to accidentally or intentionally modify or delete case data.

Users should not allow other employees access to their workstation unless the staff member is in the same department or the IT & Communications Manager and/or BSO ITS ITS have legitimate troubleshooting services or diagnostics to perform.

3.6 USB Drives

It is strongly advised that data be stored on the hard disk of the machine. The use of USB devices is strictly prohibited, unless the devices are encrypted via a password. As external devices e.g. CDs, Flash drives, etc (especially commercially produced resources) remain a potential source of virus contagion, each machine in the NIPEC is equipped with a virus detection package, through which all external drives, and devices are tested before entry into the system through a user's workstation.

4 Off-site Processing Arrangements

In protecting a facility, a system, and its data against the possibility of disaster, certain preparations must be made for use of facilities in Centre House.

4.1 Data Storage

Regular backup procedures, as described in Section 6, are strictly followed. Daily backup are made through BSO ITS ITS, with new data appended. These files are produced electronically and tested daily by the IT & Communications Manager.

NIPEC also has an arrangement with BSO ITS ITS for the use of a contingency site in Castle Buildings, Stormont which can be made available to the HPSS for both testing and emergency purposes.

4.2 Additional Resources at the shared Contingency Facility

In addition to the equipment at NIPEC, the emergency site at Castle Buildings is equipped with a number of machines, which are capable of providing a limited temporary arrangement, for NIPEC. Additional machines will be procured in the event of an emergency. NIPEC's communications will be redirected by BSO ITS, thus allowing users to access data on the new machines. At the contingency site, in Castle Buildings, there are about a dozen PC's and a couple of small printers all connected together on a Novel network, but they are for BSO ITS backup purposes only. In either a test or an emergency situation NIPEC would provide BSO ITS with a copy of the most recent backup, which they would then load on to the appropriate machine and the communications' people in BSO ITS would configure NIPEC's access to it.

It is the goal of NIPEC, that the period of contingency should be as short as possible. While no IT systems with NIPEC can be viewed as "life threatening" or critical, it is important to note that there are those which could be classified as essential, i.e. very difficult to continue as normal. It is for this reason that a time-scale of contingency, which would include detection, consolidation and solution, should not if possible exceed one week.

5 Emergency Responses

This section describes the most likely causes of computer facility disaster, and outlines procedures and actions to be accomplished during contingency situations, which threaten computer operations, resources, or safety.

It is the policy of the NIPEC to protect equipment and supplies whenever adequate advanced warning of an impending disaster is issued. The steps below outline the procedure to follow in these situations.

Know the NIPEC Emergency guidelines

NIPEC policies and procedures relating to issues of human safety, facilities and property protection, can be obtained from the Corporate Services department. It is NIPEC policy that everyone in the organisation be familiar with the location of the emergency exits and the appropriate responses to each of the emergency situations discussed within this contingency plan.

Prioritise actions based on available time

In the event of a pending disaster, such as a fire or bomb attack, the following priorities should guide the decision-making process with respect to the time available before evacuation and minimising potential losses.

- PRIORITY 1: Human safety issues (including evacuation from the building) and "critical" personal belongings protection
- PRIORITY 2: Records and software protection
- PRIORITY 3: Electronic hardware and equipment protection

- PRIORITY 4: Furniture and less critical records and property protection

Evaluate how much can be done at each priority level within the safe amount of time available, then complete the remaining steps in the following procedure. Only complete as much as possible in the available time. Always focus on the level one priority.

5.1 Disaster Classifications

The following disruptive events have been identified as posing the greatest threat to the computer resources in the NIPEC.

- Fire
- Sabotage
- Power Failures
- Water Hazards
- Mechanical Failures

5.2 Basic Emergency Response Procedures

Actions set forth, as responses to the above disasters are basic procedures that should be followed immediately proceeding or during a contingency event. These procedures are designed to protect life; minimise damage, injury or disruption; and contribute to timely restart and recovery of the NIPEC System.

5.2.1 Fire

The following emergency response activities should be accomplished in the event of fire:

1. Sound alarm vocally.
2. Activate nearest fire alarm box.
3. Notify Centre House Security personnel.
4. Extinguish fire, if possible. However, under no circumstances should staff place themselves in serious danger by doing so.
5. If time, remove backup files, secure stored data. Shut off all power. If time permits, follow emergency power-down procedures for computer systems.
6. Notify prepared list of appropriate personnel.

5.2.2 Power Failures

The following actions should be taken in the event of a power failure.

1. Determine the extent of power loss.
2. Notify Security personnel, Corporate Services Manager and IT & Communications Manager.
3. Obtain an estimate of time to repair.
4. Notify appropriate Senior Management.

5.2.3 Mechanical Failures

The following emergency response activities should be accomplished in the event of a mechanical failure.

1. Notify Corporate Services Manager and other appropriate management staff.
2. Notify IT & Communications Manager.

3. Determine extent of outage.
4. Determine source of outage.
5. Obtain estimated time to complete repairs.

5.2.4 Sabotage

The following emergency response activities should be accomplished in the event of sabotage.

1. Consider personnel safety first.
2. Notify Corporate Services Manager and IT & Communications Manager immediately.
3. Conduct a visual search of the facility.
4. Do not touch strange or suspicious objects.
5. Notify senior management and evacuate the immediate area, if strange or suspicious object is found.
6. Shut off all power and open doors, desks, etc.
7. Identify and isolate the suspected saboteur.
8. Determine the extent of the sabotage.
9. If damage has been done to the facility, log off all active users and shut down.
10. Complete a report of incident.

5.2.5 Water Hazards

The following emergency response activities should be accomplished in the event of water damage from leaking pipes, overhead pipes, or faulty sprinkler heads.

If significant water threat develops without warning:

1. Power down immediately.
2. Shut off all power.
3. Remove any relevant disks and backup files.
4. Notify Centre House Security, Corporate Services Manager and IT & Communications Manager.
5. Notify appropriate Management.

If significant threat develops with warning:

1. Notify Centre House Security, Corporate Services Manager and IT & Communications Manager.
2. Notify BSO ITS IT Services
3. Prepare and Send appropriate broadcast message to users.
4. Terminate Jobs in progress.
5. Power down Server.
6. Secure or Remove Backup Files.
7. Turn off Electric Power.
8. Prepare to Evacuate.

5.3 Preparation for Disaster Situations

As part of the contingency plan, the NIPEC will put into place procedures in the following areas.

- Protective measures to minimise the damage;

- Key officials who will be notified and how;
- Members of the recovery team (at a minimum, the IT & Communications Manager, Head of Corporate Services, representatives from building maintenance, security, and Fire Officers) and how each will be notified;
- How to determine what has been lost and what must be done to recover;
- What will be done to return to operation; and
- What will be done to make a full recovery.

Backup, Restore, and Recovery Procedures

All systems are considered to be essential to operations, and are included in the disaster recovery backup strategy. The system is independently restorable to operations to the as-of-date of the backed up data, and backed up for disaster recovery on a daily basis. The IT & Communications Manager synchronises backups for all data files, including the documents, spreadsheets, presentations, employee mailboxes/calendars and all required processing and support software.

5.4 Backup Capabilities

LAN and application system backup is provided by the following hardware and software features:

- A hard drive crash can be expected on an average of once every 3 years. For protection against this exigency, the BSO ITS Server provides reliable error checking and correction where necessary, and is plaugged to a UPS to allow for power failure. The server will enable approximately 24-36 months of data (based on approximately 3,500 applications/ approximately 5 megabytes of data per day) to be stored on the server.

  BSO ITS have a RAID 1 solution to their server configuration, meaning that should one drive fail, the system automatically swaps operation to a duplicate drive, with no loss of service to NIPEC users. As a consequence of this, every file that is written to the server is actually written twice (once to the current drive, and once to the backup duplicate drive). Should the backup drive come into operation, these will give the NIPEC IT Section time to remedy the problem on the current drive.

  Running Windows Business Server 2013, the chances of operating system corrupted data while writing to the drive, is significantly reduced. In the highly unlikely case of both drives failing, only the loss of one day's data is the worst case. However, a daily file backup should safeguard against this threat.

- BSO IT’S A full electronic backup operation, which ensures that there are daily backups with the solution of being able to restore to a previous week, or month where necessary.

5.5 Backup Procedures

Backup procedures are vital to ensure that any interruption of service is minimised as far as is possible. The procedures that follow encompass daily backups of data and weekly backups of data and all operating and application software.

Backup Log
All backups, other than daily data backups, are described with the date, time, and type, and are recorded electronically via the Backup software on the BSO ITS server.

Daily Backups
Each evening, BSO ITS server backs up all data files residing on the server to file at the end of each working day. The backup is time and date stamped. These daily backups are checked the following workday morning for completeness and integrity.

Re-baselining
For each system change released, BSO ITS in co-operation with the IT & Communications Manager will organise to re-baseline the relevant software. First, back-up up for the application as it currently exists on the server, with a log being kept of the latest changes encompassed.

Documentation
For any change made to software, menus, or other aspects of the LAN or application systems, corresponding documentation is generated (or received from system developers) and a copy is stored at an alternative location.

5.6 Restore Procedures

There are three basic types of software recovery that must be anticipated, namely, data error recovery, hard disk recovery, and virus recovery. The guidelines for these procedures are as follows:

Data Error Recovery - use the last daily backup file. Overwrite the data with the contents of the file, using the appropriate vendor software.

Hard Disk Crash - use the last weekly backup file to re-install the system and application software. Follow up with the last daily backup file to recover the latest data.

Virus - once the start date of the virus has been determined, use the last weekly backup file before that date to restore the system and application software.

5.7 Virus Protection

The best protection to guard against the server being corrupted by a virus is by restricting access to the computer room, to those who have a designated authority to gain admission. All DOS, Network, and application files should be write protected. Users should have write access only to the data they create, however the IT & Communications Manager will retain the ability to modify or delete the files of many users, when appropriate. Users should also be instructed in constructing passwords (for example, embedding underlines or numbers in the password), and advised to change them frequently. These practices not only protect against viruses, but also ensure a better operating environment for the NIPEC.

If external storage devices are ever used in transferring data to NIPEC from an external source, they should first be verified by scanning them using the virus software installed on their machines, or if possible in a standalone PC equipped with virus detection software.

Each computer within NIPEC automatically connects on a designated day to the BSO ITS server to download the latest virus definitions, and runs a weekly virus scan. This helps to maintain the protection within the organisation.

Due to the amount of laptops that currently reside in staff homes, it has become necessary to draw up a schedule to ask staff to bring in laptops to enable the IT Section to load the latest virus definitions. This not only helps to ensure that the laptop is protected against virus or similar malicious software being downloaded from the internet, or via an external storage drive, but also it reduces the risk of a virus being brought, innocently by a member of staff, into the organisation.

6 Roles and Responsibilities

This section briefly outlines the responsibilities for the NIPEC System contingency planning and disaster recovery.

6.1 Head of Corporate Services

The HCS is responsible for directing that measures and plans be instituted to protect the NIPEC System implementation, and for authorising the personnel resources and funds to ensure that recovery planning and actions are carried out. The HCS is also responsible for the initial decision to move to the contingency site, and to resume normal operations in Centre House, after it is viewed that the contingency period has passed. These decisions, should be made in consultation with the members of the Emergency Response Team.

6.2 Corporate Services Manager

The CSM will designate appropriate personnel to determine how workload and productivity would be affected by emergency scenarios, to determine what backup capabilities will be activated in the event of a major disaster, and to ensure that mission critical priorities are adequately addressed.

6.3 IT & Communications Manager

In addition to normal duties in support of the NIPEC System network, the IT & Communications Manager has a responsibility to work with BSO ITS Support staff in setting up and equipping the emergency site at Castle Buildings, ensuring that all backups are current. The IT & Communications Manager is the head of the Communications/Hardware/Software team in the event of a disaster, and bears the primary responsibility for the NIPEC System file server.

The IT & Communications Manager establishes disaster recovery teams, outlines the tasks they will perform, and directs the members to develop and document detailed procedures for their responsibilities in the event of an emergency. During the contingency period, the IT & Communications Manager should also be available to inspect the Centre House site, to make a judgement on whether it is appropriate for the NIPEC to return to Centre House, and return to the normal way of operation. His decision should be forwarded to the HCS.

The Disaster Recovery Team includes the IT & Communications Manager, Head of Corporate Services, Corporate Services Manager and at least two staff members from BSO ITS. They will put into action the Disaster Recovery Plan, as outlined in Appendix A.

The IT & Communications Manager develops, with senior management, appropriate tests to verify that each scenario can be met effectively. The IT & Communications Manager ensures that all of the information in the plan is correct, and reviews each new version for accuracy. In addition, the disaster recovery co-ordinator establishes and maintains a staff alert roster containing after-hours telephone numbers.

When a disaster occurs, the IT & Communications Manager is the first-line manager of all recovery teams.

He is primarily responsible for the orderly shutdown of hardware in a disaster and for working with vendor personnel to inspect safety systems, acquire spare equipment, supplies, and replacement parts (in line with NIPEC Purchasing procedures).

6.4 System Users

NIPEC System users can support the disaster recovery effort by selecting representatives in each floor who are responsible for notifying their fellow employees to log-off and shut down their workstations in an emergency situation.

The following members of staff are assigned to these duties.

Officer	Responsible for
Corporate Services Manager	***All staff working on this floor i.e. Permanent, Temporary and Agency.***

The IT & Communications Manager, Information Officer, HCS, as well as external support staff will serve on the User Support team in a recovery situation. Users should be responsible for the securing of and protection of their own workstations. If required, they may be called on to assist the Operations team in an emergency situation.

6.5 Administrative Staff

Some members of the administrative staff should participate in the recovery team. They will prepare purchase orders for replacement equipment, and handle clerical, legal, personnel support, and general supplies in an emergency scenario.

The following members of staff are assigned to these duties.

Officer	Responsible for
Higher Clerical Officer (in consultation with the IT & Communications Manager and CSM)	Purchase orders for replacement machines
Receptionists & Clerical Officer	Clerical Duties, and as assistance to the Personal Secretary/Higher Clerical Officer in getting delivery of emergency supplies for the NIPEC.

6.6 Business Services Organisation (IT Services)

In addition to normal duties in support of the NIPEC System hardware and application, BSO ITS support staff will work with the IT & Communications Manager to establish and maintain the emergency site equipment, software, and supplies. In an emergency, the BSO ITS support staff would be members of and co-ordinating with all of the teams.

6.7 Security Personnel

Centre House Security personnel are primarily responsible for ensuring that people entering the facility area during an emergency are authorised and have necessary functions to perform. On encountering an emergency situation such as fire, severe weather, or bomb attack, a Security Officer will call either the HCS or the CE as the designated key-holders. The telephone numbers of these members of staff are provided to the security personnel for this purpose.

Security personnel, who patrol Centre House, will call the HCS, in the first instance. In the event that other staff are required, they will be contacted by the HCS and/or CE.

7 Testing and Training

A contingency plan cannot be called adequate or successful unless its recommended practices are followed and its procedures prove to be effective. The only way to validate the recommended responses to emergency scenarios is to develop and maintain emergency preparedness testing as an integral part of plan maintenance and modification.

In many cases, testing can also be used as a vehicle for training. Testing can be accomplished in phases, befitting the needs of the user and BSO ITS, and need not excessively disrupt the normal operations of the processing site. Testing ensures the validity of the overall recovery strategy and ensures that the following five major components of the recovery plan are operating properly:

<u>People</u>
Recovery team(s) personnel are tested for the knowledge required to effectively perform recovery procedures. Testing serves as a training exercise, and identifies recovery time estimates and capabilities. For example, testing would answer the following questions: Can the Operations Team successfully restore the NIPEC System application software on the backup server if necessary? Did the IT & Communications Manager list all of the correct vendors to replace damaged equipment?

<u>Data</u>
All system and data files required to recover computer applications are tested to ensure that they are complete and secured off-site. If the recovery and restore procedures are followed, restoration of the system data or system files with backups from the off-site location should be a simple procedure.

<u>Computer equipment</u>
Testing ensures that equipment designated for recovery operations has the capability and capacity to support a recovery operation of the scope defined in the plan. The designated backup server must be shown to be in a constant state of readiness to assume the full NIPEC System processing load.

<u>Resources</u>
Testing ensures that all supplies and materials necessary to support a recovery operation are properly identified and secured at all off-site locations. It ensures that replacement equipment is compatible with the existing configuration. This includes key spare parts, printer paper, a spare printer, and other items treated in Section 6.

<u>Procedures</u>
All recovery procedures are tested to ensure that implementation is carried out as quickly as possible with minimum down time. Testing provides feedback for improving and strengthening procedures. Scenarios that allow the saving of critical data and hardware (disasters with warning periods) should be given particular attention, as they can make a major difference in recovery.

7.1 Testing the Disaster Recovery Plan

The initial testing of the plan should ideally be conducted in modular fashion during the development of Centre House's specific disaster recovery plan. The exact team structure and responsibilities of designated team participants must be established before testing, and a general recovery strategy must be in place.

One of the more common scenarios, for instance, a file server crash or electrical failure, should be tested first. The test should be initiated as a realistic scenario, where the responsible parties are notified and the appropriate teams are activated. Use a checklist for the test, which documents the following information:

- Test activity
- Data/equipment involved
- Resources (e.g., spare equipment, backup files, etc.)
- Teams involved
- Procedure followed (Xerox of test procedure
- Results, remarks, and suggestions for improvement

The checklist can be expanded to include each component contingency plan as it is developed. This serves the dual purpose of developing an effective initial plan and baselining a test plan that can be used for future periodic testing of recovery procedures. The document will then reflect a workable plan and set of procedures that can be relied on in a crisis. Periodic testing of various aspects of this plan, outlined in the subsections below, will then primarily serve as a validation and verification exercise.

The IT & Communications Manager and the HCS will evaluate the test results and develop recommendations for modification or improvement which will be brought to the management team for consideration.

7.1.1 Information Update Testing

This level of testing is performed approximately every six months, to verify the phone numbers of contacts, vendors, and other involved personnel, within and outside of the processing site. At this time, any changes in team personnel, administrative personnel, or security personnel should also be included and the new contact information added. The notification procedure should also be reviewed at this time.

7.1.2 "Emergency Site" Testing

Approximately every six months, the Emergency Site will be inspected to ensure that the spare equipment works, and that all spare parts in its inventory are available. The IT & Communications Manager should provide a list of files and supplies to be checked. This test will help to assess weaknesses in estimating times, procedures, and backup listings. This test will be carried out by BSO ITS.

7.1.3 Emergency Scenario Testing

These tests will be essentially the same as the modular tests that were run during development of the disaster recovery plan. least once a year, the IT & Communications Manager should select one emergency scenario. Management team members should be queried to verify that they have a copy of the emergency plan. Once copies are provided, each team member should be asked what he or she is to do, how long it will take, and what is needed to accomplish the task. The team responsible for damage assessment should be asked to submit a dummy assessment report to see if it is adequately detailed and understandable. Then, the other teams should be assembled and questioned about their tasks, given the test scenario and assessed damage.

7.1.4 Critical System Testing

This test should be run at least twice a year as an extension of the Emergency Site Test. It is used to determine if the backup equipment can be actually used with the backup files to set up and process NIPEC System. The responsible teams should perform their assigned tasks and the following questions answered to refine the backup plan:

- Did all personnel know where to go and what to do?
- Did the backup server perform as expected?
- Did the restored system software run properly?
- Did the restored data contain what the label stated?
- Was there adequate disk space?
- Did the spare workstation and printer perform as expected?
- Were there any problems experienced?

7.1.5 Major System Disaster

This test, which simulates a major disaster in which the computer facility is destroyed or severely damaged, necessitating a move to the backup site, is recommended from the standpoint of testing the plan, but is not practical or cost-effective in the NIPEC System production environment. Adequate safeguards will exist to alleviate the need to perform this simulation.

7.2 Maintenance of the Plan

Distribution of the NIPEC IT Contingency Plan should be limited, to prevent exploitation of system vulnerabilities as disclosed in the plan. Personnel with overall responsibility should have a complete copy of the plan. Team members should get the portions of the plan applicable to their specific functions and recovery tasks. Copies of the entire plan should be kept at the primary facility, the Emergency Site, and at the home of the IT & Communications Manager.

Keeping the plan current is crucial to being able to respond properly to a contingency. At a minimum, annual reviews and updates of the plan should be performed. The plan-testing program discussed above is a convenient way to update and refine the plan on a regular basis.

Each significant change in the operating environment should be reflected: changes to the organisation, configuration, application, hardware, communications, or procedures. Update requests to the team managers should be sent out twice a year and changes verified and incorporated. The IT & Communications Manager should review all changes to the plan. As new versions are produced, older versions should be destroyed.

8 Disaster Recovery Plan

8.1 Chain of Command

In the event of a disaster in Centre House, the IT & Communications Manager will take command of the Centre until the HCS arrives onsite. In the absence of a staff member onsite, persons aware of the disaster should notify NIPEC staff members in the following order: Head of Corporate Services, IT & Communications Manager, Corporate Services Manager. Phone numbers of these staff are given in section 9.8

8.2 Replace Damaged Hardware

As soon as possible after a disaster, the IT & Communications Manager will take an inventory of hardware that needs to be repaired or replaced in Centre House. The Disaster Recovery Team will then oversee the repair or replacement of the damaged hardware. If the Computer Facility itself is damaged, the team will oversee the setting up of the hardware at the emergency site at Castle Buildings.

8.3 Restore Damaged Software

The IT & Communications Manager will oversee installation of the most recent backup file to restore the most vital software.

8.4 Provide Access to the Computer System

After the system has been restored, the Disaster Recovery Team will provide users with either terminal access to the computer system at a location near the system, or network access to their offices if that is possible. At this time users can resume working on the computer system. Users will need to be prepared if necessary to re-enter all data entered into the system from the time of the latest usable backup until the time of the disaster.

8.5 Provide Full Access to the Computer System

The Disaster Recovery Team will oversee the restoration of full computer network functionality to the NIPEC Offices as soon as is reasonably possible.

8.6 Office Personal Computers

The IT & Communications Manager will help individual member of staff get their personal computers functioning again. If the hard drives on these machines have been damaged, staff will need to be prepared to restore the missing data from backups which the IT & Communications Manager has made previously.

8.7 General Considerations

The nature and severity of the disaster will determine how much of the current functionality users will have in their offices. If individual staff personal computers were to remain intact, staff would be able to continue working on them without much interruption, even if they could not access the systems on the NIPEC-SBS. If the offices were to become uninhabitable or unusable, then offices would need to access the NIPEC-SBS and Blackberry server via newly procured machines and handheld devices respectably, to be set up in the emergency site at

Castle Buildings. Only after the offices were made habitable and the computer networks and peripherals were restored would normal computing activities be able to be resumed. In the event that damage was limited to the Computer Facility, the restoration of the hardware and software in the NIPEC would allow offices to function normally.

The Disaster Recovery Team recommends that all offices be prepared to conduct business using manual methods. Additionally, it would be advisable for staff to have a way of manually reconstructing the data needed for essential office functions that is stored on both the NIPEC-SBS computer systems, the Blackberry/Citrix server and on individual office personal computers. Availability of backups to completely restore the data on the NIPEC systems depends upon the nature and timing of the disaster. It may not always be possible to restore all the office data from backups. For example, data entered prior to the disaster but before backups have been done cannot be restored. Availability of backups for individual staff personal computers relies on individual staff members storing data onto the NIPEC-SBS, thus allowing for backup of data to take place.

8.8 NIPEC Disaster Recovery Team

Name	Position	Phone (Home)	Phone (Mobile)
Edmund Thom	Head of Corporate Services	-	-
Mark Jamison	IT & Communications Manager	-	-
Janet Hall	Corporate Services Manager		-
BSO ITS Support Desk	BSO ITS	-	-
Emergency Line	NI Water	-	-
Emergency Line	NIE	-	-

Contact details not shown in policy, as these are only held by the Disaster Recovery Team.