REGIONAL INFRASTRUCTURE FOR INFORMATION SHARING AND DEVELOPMENT AND ADAPTATION OF MODEL CONTINGENCY ICT PLAN

Model ICT Contingency Plan

Prepared for: Caribbean Disaster Emergency Management Agency (CDEMA) by BusinessTech Research, Inc. March, 2010

Institutional Support and Capacity Building for Disaster Management in the Caribbean Project

CDEMA
CARIBBEAN
DISASTER EMERGENCY
MANAGEMENT AGENCY
Resilient States · Safer Lives

TABLE OF CONTENTS

LIST OF ACRONYMS

CDEMA	Caribbean Disaster Emergency Management Agency
CDEMA CU	CDEMA Coordinating Unit (Headquarters in Barbados)
CDERA	Caribbean Disaster Emergency Response Agency
CDM	Comprehensive Disaster Management
CIDA	Canadian International Development Agency
EOC	Emergency Operations Centre
GIS	Geographic Information System
ICT	Information and Communications Technology
IDRC	International Development Research Centre
IP	Internet Protocol
IS	Information Systems
IT	Information Technology
NDC	National Disaster Coordinator
NDO	National Disaster Organization/ National Disaster Office
NEOC	National Emergency Operations Centre
TNC	Terminal Node Controller
VSAT	Very Small Aperture Terminal

EXECUTIVE SUMMARY

An *ICT Contingency Plan* refers to a plan for recovering Information and Communications Technology (ICT) services following a system disruption. Such measures may include the recovery of ICT functions using alternate equipment or the relocation of ICT systems and operations to an alternate site. The *Model ICT Contingency ICT Plan* provides guidance to ensure that National Disaster Organizations (NDOs) are able to do the following before, during and after a disruptive event:

- Process and manage critical information,
- Maintain national and international communications,
- Maintain Internet access,

There are a wide variety of disruptions that may affect ICT operations and their impact ranges from low (e.g. minimal downtime while a component is replaced) to high (e.g. several days of downtime and loss of critical information). To eliminate or minimise such risks NDO's need to acknowledge that some critical services (such as electricity and communications) are outside their control and that they will not be able to ensure their availability. Therefore, an effective contingency plan is necessary to mitigate the risk of system and service unavailability.

This document identifies standard causes of disruption to ICT functionality and provides a guide to common preventive measures and recovery strategies to be employed. The document also highlights the key components of a specific contingency plan within the model presented. These are:

1. **Risk Assessment.** This process identifies the factors that can potentially destroy or disrupt the functioning of the organization's ICT systems, and helps to identify and prioritize critical systems and components. A template is provided for assistance.
2. **Preparation and preventive measures.** These are operational measures introduced to reduce or eliminate the consequences of disruptive events to ICT systems. Measures such as backup policies, backup and restore testing and the establishment of contracts and Service Level Agreements with service and support providers are of particular significance.
3. **Recovery strategies.** The recovery strategies focus on the anticipated effect of a disruption and the actions required to restore the ICT service. Those presented are based on scenarios involving total loss of either premises or equipment, with guidance as to how they should be applied for partial failures.

The document presents a set of forms that can be adapted to assist the NDO contingency planning process. These cover:

- The identification of critical ICT resources
- Documentation of information concerning off-site storage locations
- Key external contacts information
- Recovery Strategy planning details for systems.

1. BACKGROUND

1.1 Introduction

The purpose of this document is to provide a “model” ICT Contingency Plan that can be adapted by the National Disaster Organizations (NDOs) of CDEMA Participating States to support their use of ICT. The objective of the Contingency Plan is to ensure that satisfactory arrangements are in place to respond to situations that result in the disruption of the operation of the NDO’s ICT systems. The approach is based on the use of established risk management procedures in both normal and abnormal circumstances and particularly in emergency situations.

The *Model ICT Contingency Plan* is one of the deliverables of the EDF-funded project entitled *Regional Infrastructure for Information Sharing and Development and Adaptation of a Model Contingency ICT Plan.* Development of the Plan is based on a recognition that national and regional disaster management organisations in the Caribbean must be able to use ICT to effectively process, manage and communicate information, as required to support their activities, before, during and after disaster events.

1.2 Definition, Scope and Objectives

For the purposes of this document, the interpretation of “Contingency Plan” is based on guidelines provided by the National Institute of Standards and Technology (NIST) of the US Department of Commerce (NIST, 2002, 2009). Using these guidelines, an ICT Contingency Plan can be defined as

> “A plan that documents a strategy, procedures and technical measures for recovery of the ICT systems and data of the target organizations after a disruption.”

The term ‘ICT’ covers a range of technologies for storing, retrieving, processing, analysing and transmitting information. This includes computers, networks, software and other processing and transmitting equipment, and can cover a wide range of system designs and configurations. Thus the scope of an ICT Contingency Plan can potentially be very broad. Given the context of this project however, this document focuses primarily computer systems and technologies that facilitate connectivity of such systems. Specifically, the scope of the plan covers:

- Computer Systems
- Telecommunications
- Internet access

Notwithstanding the above limitations applied to the scope for practical reasons, the principles described in the document can be applied to other ICTs.

ICT contingency planning should be part of the fundamental mission of the NDO's as responsible and reliable public institutions. Key objectives of ICT contingency planning are:

- Ensuring the continuous performance of the agency's information systems especially during emergencies.
- Protecting equipment, data, and other assets.
- Reducing or mitigating disruptions to operations.
- Reducing damage and losses.
- Achieving timely and orderly recovery from emergencies and resumption of full service to the public

Implementation and effective execution of ICT Contingency Plans will ensure that NDOs are able to do the following before, during and after a disruptive event:

- Process and manage critical information
- Maintain national and international communications
- Maintain Internet access

In order to achieve workable ICT contingency capability the NDOs should be able to maintain a certain level of readiness and implement contingency procedures when the need arises.

1.3 Structure of the Document

This document describes the main elements of a Model ICT Contingency Plan. Chapter 1 provides an introduction and background to the document. Chapter 2 establishes the assumptions and requirements upon which the Model Plan is based. Chapters 3 to 6 identify the specific recommended activities and deliverables (Risk Assessment, Prevention and Essential Procedures) involved in the development and execution of the Plan.

2. ASSUMPTIONS AND PREREQUISITES

The following assumptions were used when developing the Model ICT Contingency Plan.

- Facilities meet the construction and safety standards considered appropriate for emergency operations

- NDO’s own equipment that, at least, meets the minimum standards defined for *Level 1*

- Key personnel have been identified and trained in their emergency response and recovery roles for ICT; they are available to activate the contingency plan.

- Core equipment is maintained in a functional state at all times e.g. network server, backup server, ups, backup media technology (tape drive, removable disks), laptops

- Critical computer equipment e.g. network server is connected to an uninterruptible power supply (UPS) that provides short term backup power during power failure.

- Service agreements are maintained with key providers of hardware, software, technical support, telecommunications and any other critical services required to support recovery of the ICT platform.

- Current backups of core application software and critical data are diligently maintained and available at an offsite storage location.

- Critical data is not available on workstations i.e. is stored on the network server

Thus in undertaking the preparatory activities for developing and implementing a contingency plan, NDOs will need to ensure that their current situations are consistent with these assumptions. Where these assumptions are not met, corrective action should be taken.

3. RISK ASSESSMENT

One of the first steps within contingency planning is to conduct a *Risk Assessment*. This process is carried out to:

- Identify the potential risks and likely impact of ICT failure.
- Establish the preventive and recovery priorities for the NDO.

The existence of an up to date inventory listing of all hardware and software is important to this process. Risk assessment can be broken down into several phases:

- *Identifying the disruption* — what can go wrong? (e.g. network server crash)
- Evaluating the risk of the disruption — how likely is it to occur ?(e.g. high, medium, low likelihood)
- *Analysing the impact of the disruption* — what would be the consequences if the risk did occur (e.g. unable to access main disaster management information)
- *Managing the risk* — once the risk factors have been established preventive procedures to minimise the risk and potential impact should be put in place.

3.1 Disruption Categories

Potential causes of disruption for which standard preventative measures are generally employed can be categorised as follows:

Category	Description of Disruption
Physical	Physical damage to the premises or equipment
Data	Loss or corruption of data
Electricity Disruption (mains)	Outages, spikes, etc.
Connectivity	Loss of telephone, fax, internet service, etc
Human Action	Accidents, negligence or malicious actions
Hardware	Technical malfunction or failure of equipment
Software	Failure or instability of critical applications

The above categories should be used to guide the NDO in identifying the *risk* and *impact* as described below, and in identifying priority areas of focus for implementation of preparedness and prevention measures.

3.2 Risk and Impact Ratings

For every potential cause within each category of disruption, the following will need to be considered:

- **Risk**: The probability or likelihood that a failure will occur.
- **Impact**: The likely consequences of the effects if the failure occurs (cost in terms of functionality and operations).

Impact is specific to the environment - the same risk realised in two different NDOs can have different impacts, depending on the environment, ICT capability and preventive measures already in place.

Risks and impacts should be rated in significance as *Low*, *Medium* or *High* as indicated in the tables below:

Risk

Rating	Description & Action
HIGH	There is a high likelihood that the event will occur, so preventive measures and/ or a recovery plan to be established as soon as possible.
MEDIUM	There is a moderate chance that the event will occur. Preventive measures are required and a recovery plan should be established within a reasonable period.
LOW	It is unlikely that the even will occur. The NDO should assess whether preventive measures are worthwhile or decide to accept the risk

Impact

Rating	Description & Action
HIGH	This will disable or severely restrict the NDO's ability to perform essential functions. Recovery procedures must be identified.
MEDIUM	This will force the NDO to use alternative methods to perform essential functions. Recovery procedures must be identified.
LOW	The NDO should be able to perform essential functions with minor adjustments.

For guidance when applying these ratings:

- The **Risk** rating should guide the level of effort and investment expended in **Preventive Measures**

- The **Impact** rating should guide the level of planning and investment put into the **Recovery Strategies**

3.3 Critical ICT resources And Critical Data

NDOs need to determine which of their ICT systems are *mission critical* by:

- Identifying the critical services that the organization is required to provide, during an event.
- Identifying the data and systems that are required to support these services

Critical ICT resources are those that support the critical business processes of the organization.

This exercise should also result in identification of the NDO's critical data.

3.4 Risk Assessment Example

The risks and impacts should be prioritised based on the critical areas to be addressed.

The assessment example below illustrates the process:-

Category	Current Status	Risk	Impact
Physical	The EOC building is designed to meet the standard guidelines for this purpose. There are no arrangements for an alternate site.	LOW	HIGH
Data	Critical data is stored on the network server. Backups are done irregularly.	HIGH	HIGH
Electricity Disruption	The EOC has a backup generator that is tested regularly and remains functional.	MEDIUM	LOW
Connectivity	Internet and phone services are dependant upon the landline facility. No satellite facility is being maintained.	HIGH	HIGH
Human Action	The staff is well trained and experienced.	LOW	HIGH
Hardware	The workstations are new but the network server is old and aging.	MEDIUM	HIGH
Software	The NDO uses standard ‘off the shelf’ applications for most functions. There is no ‘home grown’ or highly customised software that is critical to the operations.	LOW	HIGH

Following the general risk assessment, NDOs should then “drill down” into the category details. Categories where either the risk or impact rating is “High” as determined by the risk and impact ratings. In this part of the exercise, the aim is to identify more specifically where the risks lie so that appropriate preventive or recovery measures can be put in place. Also, within a category, different assets may have different risk and impact ratings. For example, in the hardware category, the impact of server failure is likely to be higher than the impact of a workstation failure.

In the above example, further assessment will be required for categories such as *Data* and *Connectivity* risk categories, and both preventive measures and recovery plans will ***need*** to be established for those.

4. PREPARATION AND PREVENTIVE MEASURES

Preventive measures are part of the risk management process - implemented to identify and mitigate possible disruptions to an IT system in order to reduce or eliminate the consequences of those disruptions. They are operational activities that should be carried out regularly.

Information from the risk assessment will help in identifying the high risk areas where disruption can be significantly reduced by the implementation of preventive measures.

4.1 Common Measures

A wide variety of preventive measures are available. Common measures recommended to address the typical disruptions identified are:

- Frequent, scheduled backups
- Offsite storage of backup media and system documentation
- Network security measures to prevent intrusion
- Use of "anti-malware" software (anti-virus, anti-spyware, anti-rootkit, etc.)
- Firewall security
- Redundancy – Communications, Server, Site
- Staff training
- Information access policy
- Hardware and software service and support contracts

4.2 Preventive Measures for Disruption Categories

Specifically preventive measures can be employed as below:

Type of Disruption	Cause	Prevention/Action
Physical	Damage to Equipment	• Equipment installed high above floor level • Easily available equipment protection from water – plastic bags. • Redundant Equipment • Mobile solution
	Damage to Premises	• Alternate Site arrangement • Mobile Solution • Remote Site arrangement
Data – Loss or Corruption	Open access to files and databases	Control over user access to certain files by network operating system and User-Id's
	Virus	Anti-virus software installed at the network level to protect all workstations on the network.
	Interference from external parties (hackers)	Firewall installed to prevent unauthorised (external) internet users from accessing the NDO's private network.

Type of Disruption	Cause	Prevention/Action
Electricity	Power (spikes and loss)	Install a UPS on the server and key pieces of equipment to protect against electrical spikes and provide emergency power (for a limited time) when mains power fails. The limited power provided enables a switch to an alternative power source or a proper power down of the protected equipment.
Connectivity	Telephone (loss)	Have available working cell phones and satellite phone
	Internet (loss)	Have available a working Internet capable Satellite phone system
Personnel	Accidental	Ensure a minimum standard of training for all staff required to interact with data. Ensure correct procedures are defined, understood and enforced.
	Disgruntled Employee	Ensure restricted access to data is maintained. Employ a 'need to know approach'. Access should be prevented for employees that have left or been fired.
Hardware	Malfunction/Failure	A cold, dust free environment should be maintained to ensure that the equipment can run at its best. The NDO should provide for routine technical maintenance of all technical equipment to prevent the development of major problems.
Software	Failure or instability.	Ensure critical software is licensed. Draw on software support either through arrangements with the software supplier or third party IT support services.

5. ESSENTIAL CONTINGENCY PROCEDURES

5.1 Backups

Maintenance of *backups* (copies of data) is one of the most important components of an ICT contingency plan. The purpose of backups is to prevent irrecoverable loss of data and to shorten recovery time.

Copies of critical data must be made ***regularly*** and stored in a safe place so that these copies can be used to restore the original data after any data loss event. Backups can be used to restore the entire data set after a disruptive event or they can be used to restore individual files after loss or corruption due to accidents or system failure.

Backups should be made of all critical data. There are many backup strategies available. The appropriate type and scheduling of the backups must be chosen based on how critical the data is, how often it is likely to be changed and how frequently new data is likely to be added. Combinations of full (all files), incremental (files created or changed since last backup) and differential (files created or changed since last *full* backup) methods can be used to ensure the NDO's recovery requirements are met. Considerations in choosing a backup method include:

- Type and life of backup media
- Storage capacity of backup media
- Time to backup data
- Ease of data restoration
- Time to restore data

Backups can be made to media such as disks, tapes, CDs and removable drives. They can also be made directly to another computer system remotely via a Wide Area Network (WAN) or the Internet. A backup policy must be developed to stipulate the frequency, type, media and method to be used, and the naming convention for all required backups. The backup policy should aim to minimise the organisation's level of exposure to data loss and should ensure:

- A regular and diligent backup schedule
- Multiple copies of the backup where required, to enable off-site storage of one copy
- Periodic testing by performing a data restore from backups

The following should be used to guide the development of the backup policy:-

- **What data should be backed up?** – Critical data must be identified.
- **What is the *Recovery Time Objective* (RTO) to be achieved?** – i.e. within what timeframe after disruption must the systems and data be restored? E.g. 24 hours. This should be based on the proposed strategies.
- **What is the *Recovery Point Objective* (RPO) required?** – To which point in time should the data be restored following a disruptive event e.g. end of the previous day, week, or month before an event or at the point just before the event.
- **Where to back it up?** – Tape, Disk (External, NAS Virtualisation etc.), Removable Drive, Internet, DVD.

- **How often to back it up?** – Regular schedule of daily, weekly, fortnightly, monthly etc
- **What kind of backup?** – Full, Incremental, Differential combinations
- **Who is responsible for creating the backups?** – At least one individual must be responsible and accountable for correctly performing and maintaining the backups
- **Who is responsible for ensuring the success of the backups?** – Successful completion should be verified.
- **Who is responsible for testing the backups?** – It is necessary to carry out periodic data restores from the backups.

5.2 Off-Site Storage of Backups

Backups of critical data and the network server must be made to removable media (flash drives, external hard drives, tapes, CDs, etc) and stored at an alternative location as a contingency for events that may destroy backups on site or make the premises inoperable. Relevant documentation with necessary information and instructions for recovery should be stored with the backup media.

5.3 Recovery Testing of Backups

The agency should regularly test the process of recovering data from the backups to:

- Ensure that the backups are reliable and that all other necessary resources (compatible devices, storage space and software) are available and working.
- Be able to estimate how much time is required to restore key services from the backup media and work to develop the ability to execute recovery within a specified period. The able below shows the proposed RTOs for NDOs, based on the level of ICT capability:

NDO ICT Capability Level	**Proposed Recovery Time Objective (RTO)**
Level 1	24 hours
Level II	12 hours
Level III	4 hours

5.4 Contractual Arrangements & Service Level Agreements

NDOs should consider establishing contractual arrangements with third-parties or entering into Service Level Agreements (SLAs) with vendors and service providers, to provide maintenance and support services for ICT systems. SLAs commit the provider to ensuring the client receives an agreed minimum level of service. This can be specified in different ways, depending on the type of service. Examples include minimum uptime rate (e.g. 99.9% uptime), maximum response time (e.g. response to a service request within 1 hour) and bandwidth availability (e.g. guarantee that available Internet bandwidth will not fall below 512 Mbps).

The following should be considered:

Hardware . If the agency does not have a hardware technician on staff, it should establish maintenance contracts for all of its main equipment (computers, printers, plotters etc) to ensure that these items are regularly maintained. This will help to extend the equipment life and reduce downtime due to faults. These contracts should also cover technical support outside of normal working hours. Key equipment such as the server should be covered by the vendor's maintenance service agreement in order to facilitate speedy replacement of parts or the complete machine.

Software. All software in use should be appropriately licensed. Unlicensed software leaves the agency vulnerable as it will not be entitled to technical support or have access to information regarding upgrades. Unlicensed products may be incomplete, contaminated with "malware" or have impaired functionality. Licensing terms are set by the vendor and therefore vary from product to product.

Utilities services. NDO's should develop close relationships with the key utilities to ensure the NDO gets priority treatment for critical service updates and service recovery. NDOs can typically access such privileges due to their roles and responsibilities.

The vendor and support agreements can be designed to include emergency services, emergency response times and the NDO's emergency priority status. All agreement documentation with key contact names and numbers should be maintained with the organisation's contingency plan.

6. NOTIFICATION AND ACTIVATION

Notification and activation covers the actions to be taken once a system disruption is identified or an emergency event has taken place or is expected. They include:

- Steps to be taken to notify the relevant personnel
- System damage assessment procedures
- Activities to implement the recovery strategies

6.1 Notification

Notification procedures should be documented for situations where there is advance warning and situations where there is not. They should include details on:

- Who is responsible for notifying
- Who needs to receive notification
- Primary and alternate methods of notification
- Information that needs to conveyed in the notification
- Notification procedures outside of working hours.

6.2 Damage Assessment

Assessment of the type and extent of damage/disruption to the ICT system is necessary to ensure a speedy and successful recovery. NDO's need to identify the:

- Cause of the emergency or disruption
- Potential for further disruptions or damage
- Area affected by the event
- Status of physical infrastructure (e.g., structural integrity of computer room, condition of electric power, telecommunications, and heating, ventilation, and air-conditioning [HVAC])
- Inventory and functional status of the technical equipment
- Type of damage to technical equipment or data (e.g., water damage, fire and heat, physical impact, and electrical surge)
- Items to be replaced (e.g., hardware, software, and supporting materials)
- Estimated time to restore normal services

6.3 Activation

Once the assessment is available, the appropriate recovery strategies can be activated through notification of those associated.

The recovery activities will focus on contingency measures to enable temporary ICT processing capabilities, repair damage to the original system, and restore operational capabilities at the original or alternate/new location.

The documented procedures for recovery should be clear and recorded in a logical sequence. Responsibility for each required step should be clearly designated.

The procedures should typically cover:

- Notifying internal and external business partners associated with the system
- Obtaining necessary supplies and work space
- Obtaining and installing necessary hardware components
- Obtaining and loading backup media
- Restoring critical operating system and application software
- Restoring system data
- Testing system functionality
- Connecting system to network or other external systems
- Operating alternate equipment successfully.

7. RECOVERY STRATEGIES

Recovery strategies cover the actions to be undertaken to return affected ICT systems to a satisfactory operational state following a failure or disruption. The strategies employed should provide a way to restore basic ICT operations to support mission critical functions, quickly and effectively, after a disruption.

The strategies will need to be based on the anticipated effect of a disruption and the resulting requirements to restore the ICT service towards continuity of operations. The adopted strategy should enable the NDO to return to a level of normal operations in a timely manner, as dictated by the agreed RTO.

7.1 Recovery Plans

A Recovery Plan should include provision for the following:

- *A backup strategy*. The availability of backups will dictate how the recovery is undertaken.

- *Protection of backups*. A backup tape full of data in a local tape drive will be of little use if the office burns to the ground. A second copy of the backup needs to be in a different physical location.

- *Recovery of core operations from the backup*. If the office is completely flooded, there should be enough data in a protected location to continue NDO operations.

- *Redundant or alternate resources* . This could be for equipment e.g. server, for a site (which can include a remote option in another country) and for communications e.g. wireless and wired local networking, multiple phone / network / internet service providers, redundant communications links, backup satellite communications.

    - *Alternate Sites*. The plan should include a strategy to recover and perform system operations at an alternate facility for a period of time. These can range from an office/room with no technical equipment to one with all the technology required already setup.
    - *Remote Sites* – equipped alternative locations with systems or storage devices to which the NDOs can connect remotely for both backups and recovery purposes.
    - *Mobile Solutions*. Self-contained portable configurations of equipment that can be set up in any fixed or mobile space. Typically includes:

        - Laptop
        - Travel Router
        - Travel Printer
        - Portable Satellite Broadband Terminal (e.g. Inmarsat BGAN)
        - External Hard Drive with USB connector

- *Contractual arrangements and agreements* to cover:

    - Replacement equipment
    - Emergency support
    - Access to alternate locations
    - Off-site storage of resources
    - Priority recovery of services

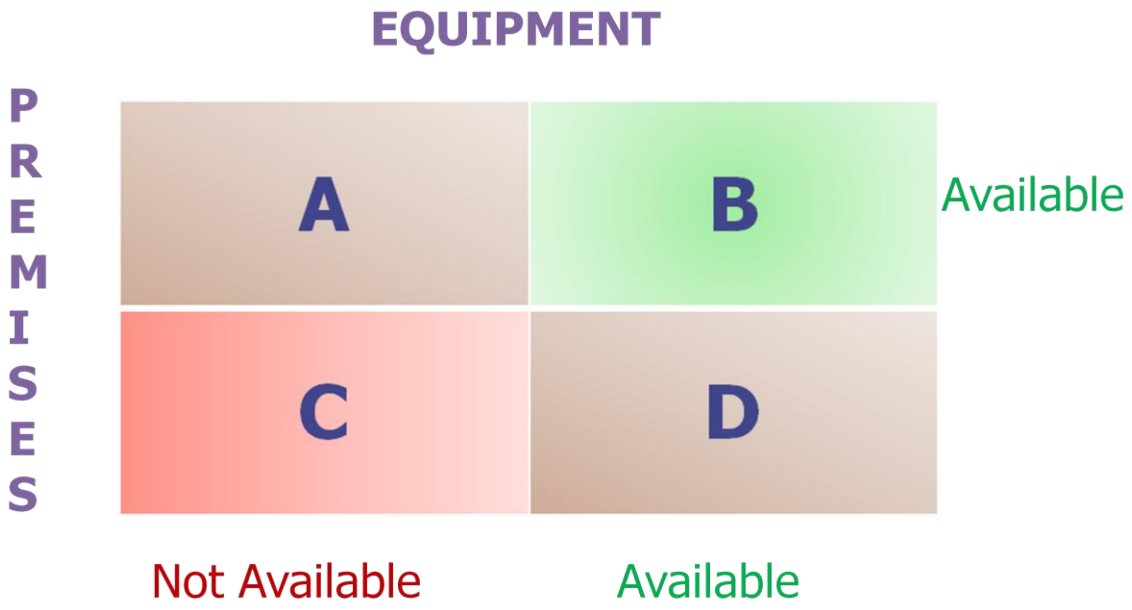
- *Recovery Time Objective (RTO).* The recovery process should function within a given timeframe to enable the NDO to get back to its emergency response or normal activities quickly. Suggested RTOs are shown in Section 5.3

- *Recovery Point Objective (RPO).* The data recovery process should enable the NDO to recover data to the point in time, before the event, that will ensure that their operations are not compromised.

The specific methods used to achieve the following plan's objectives will be dependant upon the NDO's level of ICT capability.

7.2 Recovery Scenarios – Complete Failures

Suggested recovery strategies can be developed by considering the "worst-case" anticipated effect – a combination of *loss of equipment* and *loss of premises*. Possible combinations arising are illustrated in the matrix below. The resulting scenarios are used to guide the recommended recovery steps explained below.



SCENARIO A	**Premises are Available; Equipment is Unavailable**
Objective	**Re-establish the ICT platform**
Actions	• Bring in alternate equipment facilitated either by : o An off-site redundant system o Arrangements with hardware support Or o Activate a mobile solution • Restore the critical systems and data using the most up to date backups • Achieve operational status and move to emergency response activities

SCENARIO B	**Premises are Available; Equipment is Available (Best Case)**
Objective	**Continue Emergency Response Operations**
Actions	• Continue operations • Move to emergency response activities

SCENARIO C	**Premises are Unavailable; Equipment is Unavailable (Worst Case)**
Objective	**Establish alternative premises and re-establish the ICT platform**
Actions	• Identify an alternative location by: o Finding a new location o Going to a pre-arranged alternative location o Activating a remote location if available (Level 3) • Bring in alternate equipment facilitated either by : o An off-site redundant system o Arrangements with hardware support Or o Activate a mobile solution • Restore the critical systems and data using the most up to date backups • Achieve operational status and move to emergency response activities

SCENARIO D	Premises are Unavailable; Equipment is Available
Objective	**Relocate the equipment and re-establish the ICT platform**
Actions	• Identify an alternative location by: o Finding a new location o Going to a pre-arranged alternative location o Activating a remote location if available (Level 3) • Relocate the main current equipment or activate a mobile solution • Verify the operational status of relocated equipment • Achieve operational status and move to emergency response activities

7.3 Partial Failures

Section 7.2 presents the extremes – where systems or facilities are completely disabled or destroyed. Disruptive events may also result in partial damage to the premises and /or failure of specific pieces of equipment. The principles underlying the actions for scenarios A- D above would still be applicable, however. The required actions for "partial failure" scenarios are outlined below:

<u>Partial damage to premises</u>

In that scenario, the NDO will have the following ***options*** for recovery, depending on the nature of the event, the extent of the damage, the ***Recovery Time Objective*** (RTO) and the availability of alternatives:

- Relocate any critical ICT resources (still operational) to an alternative area of the office and continue emergency operations
- Activate the mobile solution in an alternative area of the office and continue emergency operations
- Activate a remote location

<u>Partial damage to equipment</u>

For partial equipment failure, the recovery steps associated with that particular resource will need to be completed. The steps outlined for equipment failure in scenarios A and C can be applied to the specific pieces of equipment that are damaged or destroyed. For example, is a server is destroyed or disabled but the rest of the equipment is functional, the following approach can be used:

- Use backups to recreate the server on a pre-identified alternative machine
- Activate hardware vendor and/or technical support arrangements to provide a replacement server

- Reassign the storage volume from the failed server to another device, if a NAS virtualisation infrastructure is in place

7.4 Communication Failures

Communication failures are one of the most likely types of destruction and therefore require special attention. In the event of failure of the Public Telecommunications Network use the following:

Service	**Backup Solution**
Voice	HF & VHF Radio and Satellite
Data	Satellite Internet and Radio based Data Communications (e.g. PACTOR)

8. PLAN TESTING, TRAINING AND MAINTENANCE

Testing, training and maintenance are essential activities that should be carried out after the completion of the Contingency Plan.

8.1 Testing

It is important that the plan be thoroughly tested, in all its aspects. This will enable the identification and correction of deficiencies and allow the NDO to assess staff ability regarding effective implementation. It is generally recommended that there is a structured and comprehensive testing schedule covering at least the following areas:

- **System recovery -** involves ensuring that the backup media can be located, that they are adequate to restore systems to a functioning state, and that if alternate hardware has been specified it is available and functioning. To summarise, the ability to get critical systems up and running within the required timeframe should be satisfactorily demonstrated.
- **Co-ordination of responsible parties.** Testing should demonstrate that responsible teams and individuals understand and can carry out their assigned roles in an emergency.
- **Notification procedures**. The communication elements of the plan are easy to overlook but are in fact critical. Testing should ensure that communication procedures are viable and effective, and able to function properly under emergency conditions.

Commonly used methods for testing are:

- Procedural walkthroughs i.e. Walk through the procedures without carrying out any recovery operations

- Simulations

8.2 Training

Training is essential to ensure that staff members are aware of the plan, its possible impact on them and their role within it. Some form of training is therefore necessary for everybody – not just those with assigned responsibilities for recovery.

Training usually consists of a combination of classroom and practical exercises designed to imitate real life scenarios as convincingly as reasonably possible. Practical exercises should ideally involve simulations of anticipated disruptions.

8.3 Maintenance

A contingency plan is only as good as it is current but maintenance of the plan is often overlooked. In a dynamic environment and especially in the fast-changing area of IT, frequent reappraisal and review are necessary. The plan should be maintained to accurately reflect system requirements, procedures, organizational structure, and policies. IT systems change frequently due to changing business needs, technology upgrades, or new policies. It is critical that new information is documented and, where required, contingency measures are revised. FEMA (the US Federal Emergency Management Agency) recommends that organisations review their plan, at least, annually.

Procedures should be in place to update constantly changing details such as contact information on an as-needed basis.

The plan itself should be subject to security procedures i.e its distribution should be appropriately controlled and backup copies should be stored offsite and at the alternate site (if available).

REFERENCES

National Institute of Standards and Technology (NIST) (2002) Contingency Planning for Information Technology Systems. Washington, DC: NIST.

National Institute of Standards and Technology (NIST) (2009) Contingency Planning Guide for Federal Information Systems (Draft). Washington, DC: NIST.

APPENDIX A: CONTINGENCY PLANNING CHECKLIST

Purpose

The purpose of this document is to provide a quick checklist to ensure that all appropriate activities related to Contingency Planning have been addressed.

Activities Checklist

This section provides a checklist of activities to ensure proper preparation, use, and post completion review and continued use of this template.

ITEM	CONFIRM
Have any related regulatory requirements previous plans and lessons learned been identified?	
Has a Risk Analysis been conducted?	
Have preventive controls and measures been identified and implemented?	
Has a recovery strategy been developed?	
Have contingency plan been developed?	
Has higher-level management reviewed and/or accepted the Risk Assessment findings and the contingency plan?	
Have contingency plans been tested?	
Are there mechanisms for capturing lessons learned?	
Have stakeholders and staff been trained in contingency plan procedures?	
Have system descriptions and architectures been documented and included as part of the contingency plan?	
Have key personnel responsible for executing the contingency/disaster recovery plan been identified?	
Have responsibilities been clearly defined and documented as they relate to actions that will be taken in response to a disruption?	
Have notification and activation measures been identified and documented within the contingency plan?	
Have emergency recovery procedures and actions been identified and documented within the contingency recovery plan?	
Have procedures to return to normal operations following a disruption been outlined and documented as part of the contingency/disaster recovery plan?	
Have specific milestones been identified that would trigger and deactivate the contingency procedures?	
Have required contacts been documented and a formal contact list created and distributed?	
Have vendors/service providers been informed of and trained to respond in accordance with the procedures outlined within the contingency plan?	
Have formal agreements been established with any organizations responsible for providing technical support during a disruption?	
Are there procedures for reviewing and updating the plan?	

APPENDIX B: GLOSSARY

Note that the glossary below is intended to provide simple explanations of key technical terms used in the report, to aid the understanding of readers. It is not intended to be an authoritative definition of the terms.

Backup: A copy of files and programs made to facilitate recovery if necessary.

Contingency Plan: Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of system failures, or disruptive events.

Disruption: An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

Mobile Solution: A self-contained, portable configuration of IT equipment and telecommunications necessary to provide full recovery capabilities upon notice of a significant disruption.

RTO: The period of time, after a disruptive event, in which the systems and data must be restored to the predetermined RPO (Recovery Point Objective).

RPO: The point in time (prior to the disruptive event) to which systems and data should be restored.

System: A generic term used for briefness to mean either a major application or a general support system.

APPENDIX C: ICT CONTINGENCY PLAN TEMPLATE FOR NDOS

ICT CONTINGENCY PLAN FOR

<ORGANISATION NAME>

Version *<1.0>*

<mm/dd/yyyy>

VERSION HISTORY		
Date	**Reason/Description of Changes**	**Comments**

Contents

1. INTRODUCTION

1.1 Applicability

The ICT Contingency Plan applies to the functions, operations, and resources necessary to restore and resume the {Organization name}'s critical ICT system operations as they are installed at the main location. The ICT Contingency Plan applies to {Organization name} and all other persons associated with the identified critical ICT systems as identified under Section 2.3, Responsibilities.

1.2 Assumptions

The following assumptions were used when developing the ICT Contingency Plan

- The systems are inoperable at the NDO and cannot be recovered within 48 hours.
- Key personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the Contingency Plan.
- Preventive controls (e.g., generators, UPS, fire extinguishers) are fully operational at the time of the disaster.
- Core equipment is maintained in a functional state at all times e.g. network server, backup server, ups, backup media technology (tape drive, removable disks), laptops
- Key computer equipment is connected to a UPS that provides 45 minutes to 1 hour of electricity during a power failure.
- Current backups of critical application software and data are intact and available at the offsite storage facility.
- The equipment, connections, and capabilities required to operate the identified critical systems can be made available at the alternate site. .
- Service agreements are maintained with hardware, software, and communications providers to support the emergency system recovery.

The ICT Contingency Plan does not apply to the following situations:

- **Overall recovery and continuity of operations.**
- **Emergency evacuation of personnel.**
- *{Any additional constraints should be added to this list}*.

2.0 RISK ASSESSMENT

Category	Detailed Description	Risk	Impact
Physical			
Data			
Electrical Disruption			
Loss of Connectivity			
Human Action			
Hardware			
Software			

3.0 BACKUP & RESTORE STRATEGY

3.1Backup Schedule

Name/ID	File(s)/System(s)	Level	Frequency	Schedule	Responsible (Individual or Organisation)
<< Name or identifier associated with the backup procedure >>	<< Name(s) of the file(s)/ system(s) included in this backup >>	<< Such as "Full" or "Incremental" >>	<< Such as "Daily" or "Weekly" or "When modified" >>	<< Such as "Last Friday of the month" or "Monday" or "As required" >>	<< Organization or individual responsible for performing this backup procedure >>
E.G. *Working Documents*	*All files in C:\Documents\Current Documents*.**	*Full*	*Weekly*	*Monday*	*IT Support Officer*

3.1 Backup Log

Name/ID	*<< Name or identifier associated with this backup procedure >>*
Description /Purpose	*<< Description or purpose of this backup, such as "Daily incremental backup of modified emergency procedure documents" >>*
File System(s)	*<< Name(s) of the file system(s) included in this backup >>*
Level	*Circle/Tick one:* Full Incremental Other (*explain*):
Frequency (Cycle)	*Circle/Tick one:* Daily (Sunday through Saturday) Weekdays (Monday through Friday) Weekly Monthly Quarterly Annually When files are modified Other (*explain*):
Retention	*Circle one:* _____ backup cycles (*enter the number of cycles to retain*) Forever Other (*explain*):
Storage Location/ID	*Complete:* Onsite Location - Offsite Location Notes (*describe storage identifier, storage location, storage vendor*):
Backup Medium	*Circle/Tick:* Tape CD Flash Drive Portable External Drive Network Drive Other (*describe*):
Procedures	*<< Detailed steps for executing the backup procedure, including login, file locations, executables to run, parameters to use, expected messages or results, verification of backup results >>*

3.2 Schedule for Recovery/Restoration after a Major Outage

Restoration Timeframe	Restoration Sequence/ Priority	Recovery Procedure Name/ID	File System(s)	Responsible Individual/ Organization
<< Such as "Within 24 hours" or "Within 30 days" >>	<< Sequence or priority of this restoration >>	<< Name or identifier associated with the recovery procedure >>	<< Name(s) of the file system(s) included in this backup >>	<< Organization or individual responsible for performing this recovery procedure >>

3.3 Recovery Log

Name/ID	*<< Name or identifier associated with this recovery procedure >>*
Conditions for Use	*<< Description of the conditions or circumstances under which this recovery procedure should be used >>*
Purpose/Results	*<< Description of the purpose or expected results of using this recovery procedure >>*
File System(s)	*<< Name(s) of the file system(s) that will be restored >>*
Responsible Individual or Organization	*<< Name(s) and emergency contact information such as phone, pager, and cell phone >>*
Prerequisites/ Dependencies	*<< Description of any prerequisites that must be performed before this procedure is executed and/or any dependencies related to this procedure >>*
Associated Backup Procedure(s)	*<< Name(s) or identifier(s) of the procedure(s) that create the backup(s) that will be used by this recovery procedure >>*
ID(s) of Backup(s) Used	*<< Such as tape ID and storage vendor name associated with the backup tape used for this recovery >>*
Procedures	*<< Detailed steps for executing the recovery procedures, including login, file locations, executables to run, parameters to use, expected messages or results, verification of results >>*

4.0 OFF-SITE STORAGE FOR BACKUPS

LOCATION	CONTACT	REFERENCES e.g Account #, Code	ACCESS & INSTRUCTIONS e.g Phone Contact, Present contract, login & password	DATA STORED

- LOCATION – Details on the premises and the location of the data
- CONTACT – Main contact, with contact details, attached to location (is applicable)
- REFERENCES – Any relevant documents (agreement) or reference numbers
- ACCESS & Instructions– Information as to what is required to access the data e.g. phone call, password and any relevant technical instructions
- DATA – details of the data stored at the location e.g. Contingency Plan, Contact Lists,

5.0 KEY PROVIDERS SUPPORTING CONTRACTS, AGREEMENTS & SLA's

Add rows and types of contact as required:

Type Of Contact	Name, Title, Key Contact	Contact Option	Contact Number
Landlord / Property Manager			
	Name, Account Number, Key Contact		
		Work	
		Mobile	
		Home	
		Email Address	
Electricity			
	Name, Account Number, Key Contact	Work	
		Mobile	
		Home	
		Email Address	
Telecom Carriers	**1**		
	Name, Account Number, Key Contact	Work	
		Mobile	
		Fax	
		Home	
		Email Address	
	2		
	Name, Account Number, Key Contact	Work	
		Mobile	
		Home	
		Email Address	
Hardware Suppliers	**1**		
	Name, Account Number , Key Contact	Work	
		Mobile	
		Emergency Reporting	
		Email Address	

Type Of Contact	Name, Title, Key Contact	Contact Option	Contact Number
	2 - e.g. Server Supplier		
	Name, Account Number, Key Contact	Work	
		Mobile	
		Fax	
		Email Address	
	3 – e.g. Router Supplier		
	Name, Account Number, Key Contact	Work	
		Mobile	
		Home	
		Email Address	
Software Suppliers	**1**		
	Name, Account Number, Key Contact	Work	
		Mobile	
		Home	
		Email Address	
	2		
	Name, Account Number, Key Contact	Work	
		Mobile	
		Home	
		Email Address	
Office Supplies	**1**		
	Name, Account Number, Key Contact	Work	
		Mobile	
		Home	
		Email Address	
Insurance			
	Name, Account Number, Key Contact	Work	
		Mobile	
		Home	
		Email Address	

Type Of Contact	Name, Title, Key Contact	Contact Option	Contact Number
Security			
	Name, Account Number, Key Contact	Work	
		Mobile	
		Home	
		Email Address	
Off-Site Storage	**1**		
	Name, Account Number, Key Contact	Work	
		Mobile	
		Home	
		Email Address	
	2		
	Name, Account Number, Key Contact	User ID	
		Password	
		Home	
		Email Address	
HVAC			
	Name, Account Number, Key Contact	Work	
		Mobile	
		Home	
		Email Address	
Generator			
	Name, Account Number, Key Contact	Work	
		Mobile	
		Home	
		Email Address	
Other - Describe			
	Name, Account Number, Key Contact	Work	
		Mobile	
		Home	
		Email Address	

6.0 NOTIFICATION & ACTIVATION

Based on the assessment of the event, the plan may be activated by the {*Position Responsible}*

6.1 Notification

Contact information for key personnel is located in Appendix A. The notification sequence is listed below:

- The first responder is to notify the {*Position Responsible for Activation}.* All known information must be relayed to the {*Position Responsible for Activation}.*
- {*Insert further notification sequences specific to the organization and the system*.} Upon notification, the following procedures are to be performed by their respective teams:

6.2 Assessment

{Detailed procedures should be outlined to include activities to determine the cause of the disruption; potential for additional disruption or damage; affected physical area and status of physical infrastructure; status of IT equipment functionality and inventory, including items that will need to be replaced; and estimated time to repair services to normal operations.}

6.3 Activation

The Contingency Plan is to be activated if one or more of the following criteria are met:

1. {*System name}* will be unavailable for more than {*nn*} hours
2. Facility is damaged and will be unavailable for more than {*nn*} hours
3. *Other criteria*, *as appropriate*.

- The {*Position Responsible for Activation}* is to notify the off-site storage facility that a contingency event has been declared and that the necessary materials (backups/ replacement equipment etc) will be required.

- The {*Position Responsible for Activation}* is to notify the Alternate site that a contingency event has been declared and to prepare the facility for the {*Organization*}'s arrival

7.0 RECOVERY STRATEGY

This section provides procedures for recovering the application at an alternate site and/or to alternate equipment.
The following procedures are for recovering the *{System name}*. Each procedure should be executed in the sequence it is presented to maintain efficient operations.
Recovery Goal. - *State the first recovery objective. For personnel responsible for executing a function to meet this objective, state the names/positions and list their respective procedures.*

- *{Personnel Responsible}*
- *{Recovery Procedures}*
- *{Insert additional team names and procedures as necessary}*

Recovery Goal. – *State the remaining recovery objectives. For personnel responsible for executing a function to meet this objective, state the names/positions and list their respective procedures.*
{Personnel Responsible}
{Recovery Procedures}
{Insert additional team names and procedures as necessary}

7.1 ICT Resources

Refer to **Appendix B.** for *{Organisation Name}* resources

7.2 System Recovery Table

SYSTEM	RECOVERY INSTRUCTIONS
{Network Server}	**Appendix C**
{GIS}	**Appendix D**
{Inventory Management}	***etc***
{Communication Library}	
{Emergency Procedures}	
{Internet}	
{Insert Relevant Systems as Required}	

8.0 CONTINGENCY PLAN CHECKLIST

ITEM	CONFIRM
Have any related regulatory requirements previous plans and lessons learned been identified?	
Has a Risk Analysis been conducted?	
Have preventive controls and measures been identified and implemented?	
Has a recovery strategy been developed?	
Have contingency plan been developed?	
Has higher-level management reviewed and/or accepted the Risk Assessment findings and the contingency plan?	
Have contingency plans been tested?	
Are there mechanisms for capturing lessons learned?	
Have stakeholders and staff been trained in contingency plan procedures?	

Have system descriptions and architectures been documented and included as part of the contingency plan?	
Have key personnel responsible for executing the contingency/disaster recovery plan been identified?	
Have responsibilities been clearly defined and documented as they relate to actions that will be taken in response to a disruption?	
Have notification and activation measures been identified and documented within the contingency plan?	
Have emergency recovery procedures and actions been identified and documented within the contingency recovery plan?	
Have procedures to return to normal operations following a disruption been outlined and documented as part of the contingency/disaster recovery plan?	
Have specific milestones been identified that would trigger and deactivate the contingency procedures?	
Have required contacts been documented and a formal contact list created and distributed?	
Have vendors/service providers been informed of and trained to respond in accordance with the procedures outlined within the contingency plan?	
Have formal agreements been established with any organizations responsible for providing technical support during a disruption?	
Are there procedures for reviewing and updating the plan?	

APPENDIX A: KEY STAFF CONTACT LIST

Name	Title	Contingency Responsibility	Work #	Cell #	Home #	e-Mail(s)

APPENDIX B: ICT RESOURCES

Type/ Location	Description (including technical specifications where applicable)	Operational Status/Remarks

APPENDIX C: RECOVERY PLAN FOR {*Local Area Network (LAN)}*

SYSTEM	

OVERVIEW	
SERVER	Location: Server Model: Operating System: CPUs: Memory: Total Disk: System Handle: System Serial #: DNS Entry: IP Address: Other:
HOT SITE SERVER/ALTERNATE SERVER	*Provide details*
APPLICATIONS (Use bold for Hot Site)	
ASSOCIATED SERVERS	

KEY CONTACTS	
Hardware Vendor	*Provide details*
System Owners	*Provide details*
Database Owner	*Provide details*
Application Owners	*Provide details*
Software Vendors	*Provide details*
Offsite Storage	*Provide details*

BACKUP STRATEGY for SYSTEM TWO	
Daily	*Provide details*
Monthly	*Provide details*
Quarterly	*Provide details*

SYSTEM TWO **DISASTER RECOVERY PROCEDURE**	
Scenario 1 Total Loss of Data	*Provide details*
Scenario 2 Total Loss of HW	Provide *details*

ADDENDUM

CONTACTS	

File Systems <date>

File System as of <date> Minimal file systems to be created and restored from backup: <List>	**Filesystem kbytes Used Avail %used** **Mounted on** *<Provide details>*
Other critical files to modify	*<Provide details>*
Necessary directories to create	*<Provide details>*
Critical files to	*<Provide details>*

restore	
Secondary files to restore	*<Provide details>*
Other files to restore	*<Provide details>*

APPENDIX D: RECOVERY PLAN for *{GIS}*

SYSTEM	

OVERVIEW	
MAIN SERVER	Location: Server Model: Operating System: CPUs: Memory: Total Disk: System Handle: System Serial #: DNS Entry: IP Address: Other:
HOT SITE SERVER/ALTERNATE SERVER	*Provide details*
APPLICATIONS (Use bold for Hot Site)	
ASSOCIATED SERVERS	

KEY CONTACTS	
Hardware Vendor	*Provide details*
System Owners	*Provide details*
Database Owner	*Provide details*
Application Owners	*Provide details*
Software Vendors	*Provide details*
Offsite Storage	*Provide details*

BACKUP STRATEGY FOR SYSTEM ONE	
Daily	*Provide details*
Monthly	*Provide details*
Quarterly	*Provide details*

SYSTEM ONE ***DISASTER RECOVERY PROCEDURE***	
Scenario 1 Total Loss of Data	*Provide details*
Scenario 2 Total Loss of HW	*Provide details*

ADDENDUM

CONTACTS	

APPENDIX E: RECOVERY PLAN for {*System 3*}

Copy form from APPENDIX C and insert details for System 3