OKHAHLAMBA LOCAL MUNICIPALITY

I.T

DISASTER RECOVERY PLAN

2016/2017

TABLE OF CONTENTS

1. INTRODUCTION

The IT Department has been mandated to be the main custodian of the IT Systems Hardware and Software in the Municipality. It is charged with ensuring that the IT hardware and software, data, servers, firewalls and business applications are all functioning to optimal levels of efficiency, that the networking and telecommunications are available to users at all times.

1.1 PURPOSE

This Disaster Recovery Plan document is aimed at the IT Disaster Recovery Program for recovering IT systems operations after a disaster. The plan describes the preparation and actions required to effectively respond to a disaster, assign responsibilities and describe procedures for testing and maintaining the plan.

1.2 OBJECTIVES

The primary objective of Disaster Recovery Plan is to protect the organisation in the event that all or part of its operations or computer services is rendered unusable. Preparedness is the key.

The planning process should minimise the disruption of operations and ensure some level of organisational stability and an orderly recovery after a disaster.

Other objectives of the Disaster Recovery Plan included:

- Providing a sense of security
- Minimise risk of delays
- Guaranteeing the reliability of standby systems
- Providing a standard for testing the plan
- Minimise decision-making during a disaster

1.3 SCOPE

This Disaster Recovery Plan is focused only on the municipal-owned and managed IT systems.

This plan addresses all preparation and steps necessary to restore processing or those systems so that the participating applications can continue processing after a disaster has rendered any or all the systems inoperable.

1.4 DISASTER RECOVERY STRATEGY

Should the IT systems encounter a disaster that prevents them from functioning, the IT Department and IT service providers should be prepared to provide adequate computational, data storage and data communications services and facilities at an offsite disaster recovery resource for the participating applications.

The off-site disaster recovery resource is a fully operational DATA CENTRE that is prepared to host the Dolfin Financial Management Systems, VIP (Payroll System) and all other business applications as needed. (Referred to as the HOT SITE).

Traffic office (old municipal building) server should be the Municipality's first host-site, hence the need to fully secure and equip it.

The second option could be a reciprocal arrangement between Okhahlamba Local Municipality and SP (service provider) whereby a redundant spare server would be installed within their Data center or Cloud.

In the event that the main Okhahlamba server room becomes dysfunctional, the Traffic Server and/or the Data center Server would be used to offer network and application services to critical users.

The IT Officer, in conjunction with the Director of Corporate Services, shall assume the role of Disaster Recovery Coordinators and shall be responsible for:-

- Organising regularly scheduled, periodic tests of the disaster/data recovery procedures
- Maintaining and updating the Disaster Recovery Plan based on changes in user requirements, personnel, hardware and software configurations and the results of disaster recovery tests and plan reviews; and
- Orchestrating the execution of the Disaster Recovery Plan where a disaster has been declared.

The IT Officer and the Director of Corporate Services shall designate one user per department as the Disaster Recovery Technical Support Coordinator for each of the processing systems covered by this Disaster Recovery Program. The Disaster Recovery Technical Support Coordinator's responsibilities shall include:

- Assisting the participating application users in preparing for the disaster recovery test events;
- Serving as liaison for the participating application users during the disaster recovery tests(by assisting users in resolving errors in jobs, reporting communications problems to the test of the Disaster Recovery Team and answering disaster recovery testing questions in general); and
- Assisting the participating application users in preparing their applications to run successfully at the hot site in the event of a disaster.

Enhancement of disaster recovery capabilities is the responsibility of all Directors, HOD's and technical managers. This includes participating in the periodic Disaster Recovery Plan tests and communicating with the Disaster Recovery Coordinator regarding significant changes or developments in the applications.

1.5 **DISASTER DEFINITION**

For the purposes of this plan, a disaster is any event that prevents the IT systems from providing services needed by the participating applications for a period of 72 hours or longer.

Conditions that could be declared a disaster include, but not limited to extended electrical power outage to the computer server room, extensive fire, smoke, and water, floods, explosion damage and other environmental conditions to computing equipment.

2. **DISASTER RECOVERY ACTION PLAN**

Backup and off-site storage procedures for Dolfin Financial Management System, VIP, and Network shares shall be as follows:-

- A two week rotational backup strategy is being followed
- Daily back-ups are done from Monday to Thursday and these are kept in a safe and will be over written in the next two week cycle
- Weekly backups are done and will be overwritten in the following month
- Monthly back-ups are done in full and are only over-written in the next year
- Weekly and monthly backups are all stored off-site in the strong room or Data center
- Systems configuration information is backed up and stored off-site as well
- In a disaster, all backup tapes will be taken to the host site

2.1 **BACK UP SERVER**

The backup server is identical to the main server. Its purpose is to mirror the main server so that if the main server breaks down, the backup server takes over. Very little data and time will be lost in this instance.

2.2 **TRAFFIC SERVER**

The Traffic server (old main municipal building office) would not only provide the much needed load balancing, but it will definitely serve as a replication server for the Main building server.

When both the servers at the main building are down, the Traffic server (old main municipal building office) will work as the main server servicing users in both the buildings. It will also provide for internet connectivity to users at both the main building and also the Traffic/old main building. Data recovered will only be up to the last replication. Similar backup strategy will apply also at the Traffic/old main building to offer further redundancy.

2.3 **NETWORK SHARES**

Creation of network shares per department per user is an effort to save not only financial/ accounting data, but also business information that is critical to departments and users alike. In the event of hard drives crushing or in the event of theft, individual business files can be restored from the backup or the network share in question.

2.4 **OFF-SITE STORAGE SERVICES**

The IT Department can contract the Traffic section in the Municipality or SP's/ to provide secure off-site storage services. The Traffic section fire proof strong room must meet the acceptable standards for secure storage.

The Traffic section or SP's (service provider) is responsible for:-

- Delivery of backup tapes (both those stored off-site and those at the Main building or Traffic old main building) to the hot site upon request and as directed by the IT Disaster Recovery Technical Team (both for disaster recovery tests and for actual disaster); and
- Delivery of the backup tapes from the hot site back to the Traffic (old main municipal building office) or SP's strong room for storage.

2.5 OTHER IMPORTANT SECURITY POINTS OF CONCERN-RECOMMENDATIONS

FIREWALLS

- To be compliant with the organisation's current security policy and that they have been compliance-tested through regular penetration.
- Recognised standard of encryption for all critical communications is used internally and externally. This will go a long way to curb hacking and cyber-attacks.

FLASH DISKS

The usage of removable storage devices on desktops and laptops from outside the municipality is restricted and anti-virus deployed and no other removable storage devices will be used unless it has been scanned by the IT section to minimize the risk.

ANTI-VIRUS SOFTWARE

- Viral attacks on systems can render them inoperable.
- Hence, Antivirus Products are deployed at external network entry points, on mail server and on all desktops and laptops
- Antivirus products are automatically updated when released by vender and IT team ensures regular scans are carried out on users' machines
- Laptops are barred from connecting to the network unless they are authorized by IT security first.
- Vendor operating systems patches are reviewed for impact and relevance and tested before being applied

SITE-ACCESS CONTROL

Physical security of the systems server is critical. Theft of important servers may be disastrous and can cause loss of time and money to the Municipality.

For that reason; the following measures should be implemented to minimise risk

- The IT server rooms have separate physical access control
- The IT environment power supply to critical systems is protected with UPS and generators
- IT environment humidity, ventilation and air-conditioning are controlled
- IT environment (server rooms) is protected by fire detection and suppression
- IT environment is protected by water detection

DISASTER RESPONSE

In the event of a disaster, the Disaster Recovery Coordinator sets the following committees in motion.

Damage Assessment Team- Assess the damage to the IT Systems to determine if a disaster can be declared

Executive Team- makes a decision to formally declare a disaster

Executive Team- Establish a Disaster Command Post, if necessary, in another Municipal building with adequate communications and support equipment

Executive Team- Notify the off-site storage facility, the hot site, municipal top management and the IT service providers of the disaster declaration.

(Restoration Team, Operation Team, and Customer Support Team)- work with the hot site staff to restore municipal operating systems and applications at hot site and establish the communications link to the hot site in preparation for operations at hot site for duration of the emergency.

(salvage / reclamation team)- Reconstruct the servers at main office

(Operations Team, Restoration Team and Customer Support Team)- Conduct operation at the hot site until the computer centre is ready to resume operations.

(Operations Team and Restoration Team)- conduct preparations to leave hot site and to resume operations at the main server room

2.6 HOT SITE HARDWARE AND SOFTWARE CONFIGURATIONS

The standard IT hardware and software infrastructure at the hot site should include a mainframe system (server), Advanced Windows Server 2003/8 Network infrastructure for data communications and a work recovery centre.

The following are major hardware components of the standard mainframe configuration

- Dell processor with sufficient MIPS and memory capacity,
- Two logical partitions (LPARs)
- Sufficient quantity of tape drives
- Sufficient disk storage
- Sufficient Printer capacity

At the hot sit, the functions of the multiple servers are consolidated in one machine.

The following are provided to support data communications to the hot site:

- Network Control Centre for communication support to mainframe/server and workstations
- Dedicated T1 line with appropriate routers, switches, and firewalls for IP communication between main office, hot site main frame and all workstations
- Alternative web services, for Internet connectivity to provide alternative connectivity the T1 line be inoperable

2.7 RESUMING NORMAL OPERATIONS

While recovery operations are on-going at the hot site the Salvage/ Reclamation Team will be managing the restoration or rebuilding of the main server and network infrastructure in the main building.

2.8 SECURITY

While operating at the hot site, information security will be assured by firewall restrictions and the security controls on the hot site host systems which will be configured in accordance with the policies and procedures governing IT systems in the Municipality. As processing continuous at the hot site, the hot site hosts systems will be closely monitored to ensure systems are not compromised.

3 FUNCTIONAL TEAMS AND RESPONSIBILITIES

The following subsections describe each functional team's role as well as its responsibilities in preparing for and responding to a disaster. The responsibility for planning, coordinating, and managing this program is assigned to the Disaster Recovery Coordinator with assistance from technical advisors.

The appendices and attachments provide supplemental information and instructions to assist the teams in fulfilling their functions.

3.1 DAMAGE ASSESSMENT TEAM

The Damage Assessment Team assesses the extent of the damage to the Data Center, reports to the Executive Team, and makes a recommendation on declaring a disaster.

The major pre-disaster responsibility is to determine appropriate considerations/criteria for identifying the extent of the damage and the estimated duration of the outage.

The disaster responsibilities and actions are:

- Receive the first alert regarding the disaster.
- Ensure that the Protection Services departments (traffic, security and fire) have been notified.
- Coordinate with the security personnel and/or fire department to provide for safety, security, and access to the damaged facility.
- Assess the damage to each area of the computer facility.
- Brief the MM or alternate, communicating the recommendation(s).

3.2 EXECUTIVE TEAM

The Executive Team officially declares that a disaster has occurred, authorizes the execution of the Disaster Recovery Plan, and oversees the execution of the plan during the emergency.

The pre-disaster responsibilities are:

- Approve IT Disaster Recovery Plan and all major or material modifications to the plan.
- Establish primary and alternate disaster command posts, ensuring that the posts are adequately prepared for a disaster.

The disaster responsibilities and actions are:

- Notify the hot site and the off-site storage facility of a possible disaster.
- Review the report of the Damage Assessment Team.
- Declare a disaster:

a) Establish the command post and communications,

b) Activate the Functional Teams,

c) Inform the hot site of the disaster declaration, and

d) Initiate the shipment of the backup materials to the hot site.

- Notify the Key Executives.
- Monitor the performance of the Disaster Recovery Teams and the execution and effectiveness of the Disaster Recovery Plan.
- Keep all senior managers and the designated Information Officer/alternate informed of material/sensitive matters.

3.3 RESTORATION TEAM

The Restoration Team brings the hot site municipal email systems to operational mode by managing the relocation of services to the hot site email processing site, initiating and managing the recovery procedures at the hot site, and responding to operational problems at the hot site. The Restoration Team also manages the relocation of services back to the Data Center.

The pre-disaster responsibilities are:

- Establish and maintain the recovery procedures for the hot site/email systems.
- Manage and maintain the backup procedures.
- Establish and maintain the disaster recovery data communications link to the hot site.
- Plan and conduct regular hot site/email recovery tests.

The disaster responsibilities and actions are:

- Coordinate recovery procedures with hot site personnel.
- Restore the operating systems environments on the hot site/alternate email processing site host systems.
- Establish the data communications link to the hot site.
- Verify the operating systems and all other system and communication software are working properly.
- Restore the application/mailbox files.
- Support the operations at the hot site by resolving problems and monitoring and maintaining the data communications link to the hot site.
- Support operations at the alternate email processing site by resolving problems.
- Manage the backup tapes that were sent to the hot site.
- Ensure all required backups of the entire system are completed in preparation for leaving the hot site.
- Coordinate the return of the backup/storage media to the Data Center.
- Install all municipal system/messaging software at the Data Center.

3.4 OPERATIONS TEAM

The Operations Team assists in the recovery operations and manages the operations of the computer systems at the hot site.

The pre-disaster responsibilities are:

- Ensure that appropriate backups are made on the prescribed, rotating basis and are ready to be taken off-site.
- Maintain current, up-to-date systems operations documentation, ensuring that this documentation is suitably stored off-site.

The disaster responsibilities and actions are:

- Provide assistance to the Restoration Team in the restoration of the system software and customer files, as required.
- Run system and operation jobs, as required.
- Implement and maintain a problem log.
- Provide information to the Customer Support Team regarding the status of the system, operations, and the customer jobs.
- Effect the transfer of media and print output from the hot site to suitable customer pickup location(s).
- Coordinate the shutdown of the hot site operations and the transfer back to the Data Center.

3.5 CUSTOMER SUPPORT TEAM

The Customer Support team provides assistance to customers during the disaster from the time the disaster is declared until operations resume at the Data Centre.

The pre-disaster responsibilities are:

- Advise and consult with application customers regarding their disaster recovery requirements.
- Assist application customers during disaster recovery tests.
- The disaster responsibilities and actions are:
- Notify participating application customers that a disaster has been declared.
- Advise customers of the disaster recovery system status, availability, and accessibility.
- Provide problem diagnosis and resolution guidance/assistance to application owners and their customers.

3.6 SALVAGE/RECLAMATION TEAM

The Salvage/Reclamation Team manages the restoration or rebuilding of the Data Center.

The major pre-disaster responsibility is to maintain current copies of equipment inventory lists, physical plant layout/diagrams (floor plans), and other pertinent documentation describing IT production hardware configuration in a suitable off-site location.

The disaster responsibilities and actions are:

- After the Restoration Team has implemented recovery operations at the hot site, assess the damage to the Data Center and report the damage, with recommendations, to the Executive Team.
- Organize the recovery of salvageable equipment, supplies and the physical plant.
- Initiate, coordinate, and expedite construction and work requests to prepare the municipal facility to receive equipment, supplies, tools, machinery, and utilities (electrical power, telephones, network connectivity, air conditioning, plumbing, water, gas).
- Order and expedite replacements for unusable IT equipment.
- Monitor the construction of the new/repaired facility, and the installation of all utilities and other essentials.
- Monitor the installation of computers, peripherals, and other IT equipment.
- Advise the Executive Team regarding status, progress, and schedules, and any problems associated with the construction/reconstruction and installation.
- Inform the Executive Team when the new/restored facility is ready for use by the participating applications and by other customers.

3.7 ADMINISTRATIVE SUPPORT TEAM

The Administrative Support Team provides logistical and organizational support for all the other teams.

The major pre-disaster responsibility is to prepare up-to-date property management lists, inventory lists, and other pertinent documentation on the physical assets of the Data Center; ensuring current copies of this documentation are suitably stored off-site.

The disaster responsibilities and actions are:

- Prepare travel orders and other documents to facilitate the Restore Team activities.
- Provide general administrative support to the Executive Team and to all other Disaster Recovery Teams as necessary.

4 TESTING THE DISASTER RECOVERY PLAN

Testing and exercising the Disaster Recovery Plan helps to verify that the recovery procedures work as intended and that the supporting documentation is accurate and current. Testing also provides an opportunity to identify any omissions in recovery procedures or documentation and to determine whether personnel are adequately prepared to perform their assigned duties. Therefore, IT regularly schedules exercises of its Disaster Recovery Plan at the vendor hot site, referred to as hot site tests (HSTs).

4.1 HOT SITE TEST PROCEDURES

IT schedules two hot site tests per year with sufficient time to test the operating system and customer application recovery procedures. The initial hours are dedicated to exercising the system recovery procedures and establishing the communications link. The remaining hours are dedicated to testing the recovery of participating applications. The hot site tests are managed and conducted by members of the Restoration Team, the Operations Team, and the Customer Support Team, referred to collectively as the HST Team.

Prior to the HSTs, the HST Team determines which backup tapes will be used for the tests; establishes a test plan which outlines the HST Team goals and activities for the given test; conducts the necessary preparations for the test; and assists customers in their preparations for the HST. (Customers set their own HST objectives.) During the tests, in addition to providing customer assistance, the HST Team participants maintain a running log of the test activities to assist in the post-test review.

After every test, the HST Team participants meet to discuss the tests in order to improve the recovery procedures and the plan documentation. The HST Team also schedules a meeting with the customers to gain their input and suggestions for improvements.

4.2 HOT SITE TEST PLANNING

To ensure a successful hot site test, the HST team will:

- Confirm with the hot site vendor that the hot site mainframe, Unix computer, and data communications configurations will meet the HST needs, and that the hot site will be ready for the test. (Two to three months prior to the scheduled test)
- Set the HST Team objectives for the test and establish action items for the team in preparation for the test. (At least two months prior to the scheduled test)
- Disseminate information to the user community regarding the test. (Six to eight weeks prior to the scheduled test)
- Confirm that preparatory tasks are being completed and review the schedule of events for the days of the HST. (Four to six weeks prior to the scheduled test)
- Discuss the final test preparations with the hot site vendor to confirm the hot site configurations, to obtain the information required for the mainframe backups, and to reconfirm the hot site will be ready. (Two to three days before the scheduled backups for the test will be taken)
- Send the backup tapes and tape lists to the hot site. (One week prior to the scheduled test)

4.3 APLICATION TESTING SUPPORT

The HST Team offers user support during a hot site test to assist the application owners/participants in successfully running their applications at the alternate site. The assistance includes help with test preparations, on-call support during the duration of the test, resolving reported problems, and serving as the liaison between the user and the HST Team.

Test preparation support includes:

- Ensuring the users have made all appropriate preparations for their data to be available for the HST,
- Ensuring the users are ready for the HST and have no further questions, and
- Ensuring users have the necessary contact phone numbers for user support during the HST.

Hot site test support includes:

- Notifying those users who have not logged on that the disaster system is up and ready for user testing,
- Responding to general user questions and to user problem reports, ensuring they are resolved, and

- Recording all problem reports and general notes to a system status database that is made available to users to read.

4.4 POST-TEST WRAP-UP

Two debriefings are schedule on the days immediately following the hot site test. One is for the HST Team participants to assess the systems software recovery procedures. The second is for the user community who participated in the HST.

These meetings are general discussions to address:

- Areas where the exercise was successful,
- Problems that were encountered, and
- Suggestions for improvements.

Based on the conclusions, an action list of improvements to be made prior to the next test is developed and responsibility for implementing them is assigned.

4.5 HOT SITE TEST SCHEDULE

The bi-yearly tests are scheduled approximately six months apart beginning 6 months after approval of this DRP.

4.6 TRAINING

In addition to regular training, team members and managers receive annual refresher training regarding the emergency alert procedures.

5 MAINTAINING THE PLAN

The Disaster Recovery Coordinator of the Data Center is responsible for the maintenance of this document. The plan is updated as needed:

- in response to events such as office moves, telephone number changes, new personnel joining the Municipality, retirements, duty changes, and additions or deletions of participating applications;
- after each hot site test to reflect the recommendations resulting from the post-test wrap-up debriefings; and
- After a periodic review of the plan.

All changes to the DRP will have to be noted and attached to this document.

As sections of the plan are updated, the revised sections are posted to the municipal intranet to ensure the most current information is available to DR team members. DR participants are notified of the changes and are encouraged to produce printouts for their copies of the disaster recovery plan.

Additionally, the plan will be updated in the event an actual disaster occurs. The plan will be reviewed and updated at a convenient point after the initial responses to the disaster have been completed.

DATE ADOPTED BY COUNCIL: …26…/…06……/…2013….