FETAKGOMO TUBATSE
LOCAL MUNICIPALITY

INFORMATION TECHNOLOGY Disaster Recovery Plan

Council Resolution NR: OC148/2018

In the event of plan invocation, go immediately to "DRP Invocation actions" Section 8 and perform actions as listed

Table of Contents

ABBREVIATIONS AND DEFINITIONS

Abbreviation/ Definition	Description
Backup	The procedure for making extra copies of data in case the original is lost or damaged.
Business Continuity (BC)	Business Continuity means maintaining the uninterrupted availability of all key business resources required to support essential business activities.
Business Continuity Management (BCM)	Business Continuity Management is defined by the Business Continuity Institute as a holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.
Business Impact Analysis (BIA)	A Business Impact Analysis identifies the functions, which are most critical to the organisation and which, if not recovered timeously after a disaster will have major financial and operational impacts on the organisation.
BU	This refers to a specific Business Unit within Fetakgomo Tubatse Local Municipality IT Unit
COBIT	Control Objectives for Information and Related Technology is a framework created by ISACA for information technology management and IT governance. It is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.
Disaster	A disaster is any event that can cause a significant disruption in the business processes for a period of time and effects the operation of the organisation. Potential threats/disasters, which could impact upon the divisional site and ultimately also on the Group. These are divided into two categories, namely threats requiring relocation and those that do not require relocation.
Information Technology Service Continuity Plan	The IT Service Continuity Plan constitutes one of the elements, which makes up Business Continuity Management. It focuses on the Information Technology processes in response to a disaster, as contained within the Business Continuity Management Process.
IM	Information Management is the collection and management of information from one or more sources and the distribution of that information to one or more audiences
IT	Information Technology refers to anything related to computing technology, such as networking, hardware, software, the Internet, or the people that work with these technologies.
ITSC	Information Technology Service Continuity is a subset of business continuity planning and encompasses IT disaster recovery planning and wider IT resilience planning. It is the process of assessing and managing risks associated with information technology (IT) departments. It involves the evaluation of values, threats, risks, vulnerabilities and development of countermeasures to ensure continuation in the event of an IT services disruption.

Abbreviation/ Definition	Description
Mitigated	The act of reducing the severity or seriousness of a disaster
Policy	A policy is a set of rules and principles that must be adhered to and is approved by the executive committee as directed by Approval and Signing Authority Manual (ASAM). The purpose of a policy is to establish accountability, roles and responsibilities, to direct the management of IM and formalise the requirements and standards for implementing security measures in a consistent and cost effective manner. If an exception is required, the committee that approved the policy must be requested to authorise the exception.
Process	A process is a collection of procedures influenced by the municipality's policies and procedures that takes inputs from a number of sources, including other processes, manipulates the inputs, and produces outputs, including other processes. Processes have clear business reasons for existing accountable owners, clear roles and responsibilities around the execution of the process, and the means to measure performance (Cobit).
Risk Appetite	An aggregated account of the board's willingness (to allow management) to take risks in the pursuit of strategic objectives
Risks	Is an uncertain future event that could influence the achievement of a company's objectives.
RTO	The recovery time objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.
SLA	Service Level Agreement is an agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers (ITIL).
Standard	A Standard is a set of mandatory practices that must be followed in achieving compliance to predetermined standards criteria (COBIT and ITIL). An IM standard is used to support a policy or a number of policies within the policy framework.
DRP BCP	Disaster Recovery Plan Business Continuity Plan
FTLM	Fetakgomo – Tubatse Local Municipality

1. Purpose

This document is a disaster recovery plan for IT and describes the actions that must be taken to recover critical systems at an alternate site (FTLM Regional Office) within stipulated Recovery Time Objectives (RTOs) and to stipulated Recovery Point Objectives (RPOs) in order for the Fetakgomo – Tubatse Local Municipality (FTLM) to recovery their Mission Critical Activities (MCAs) within their required RTOs after an incident affecting business operations.

2. Scope

This document is a subset of the IT Governance Framework and IT Strategy for FTLM.

This document is used in conjunction with the Common Data document, which contains associated data common to all of the plans.

A full copy of the disaster recovery plan is kept by the FTLM's IT Manager or Business Continuity Coordinator (BCC).

3. Authority

Invocation of this plan is governed by the Crisis Management Team through the IT Manager or BCC.

4. Escalation

Crisis Management Team in Common Data document.

5. Assumptions

This plan is to be used during an incident that affects normal business processes that have been interrupted or affected by:

1. Loss of people (staff)
2. Denial of access to normal work area (premises)
3. Loss of critical technology (IT systems, applications, networks, etc.)
4. Interruption of supply chain
5. Other

This plan also assumes that Occupational Health and Safety procedures are in place and tested.

This plan assumes that the agreed recovery strategy for the relocation of staff, prepared command centres and supporting teams has been implemented and that team members are trained and aware of their roles and responsibilities.

6. Disaster Recovery Plans (DRPs) Introduction and Schematic

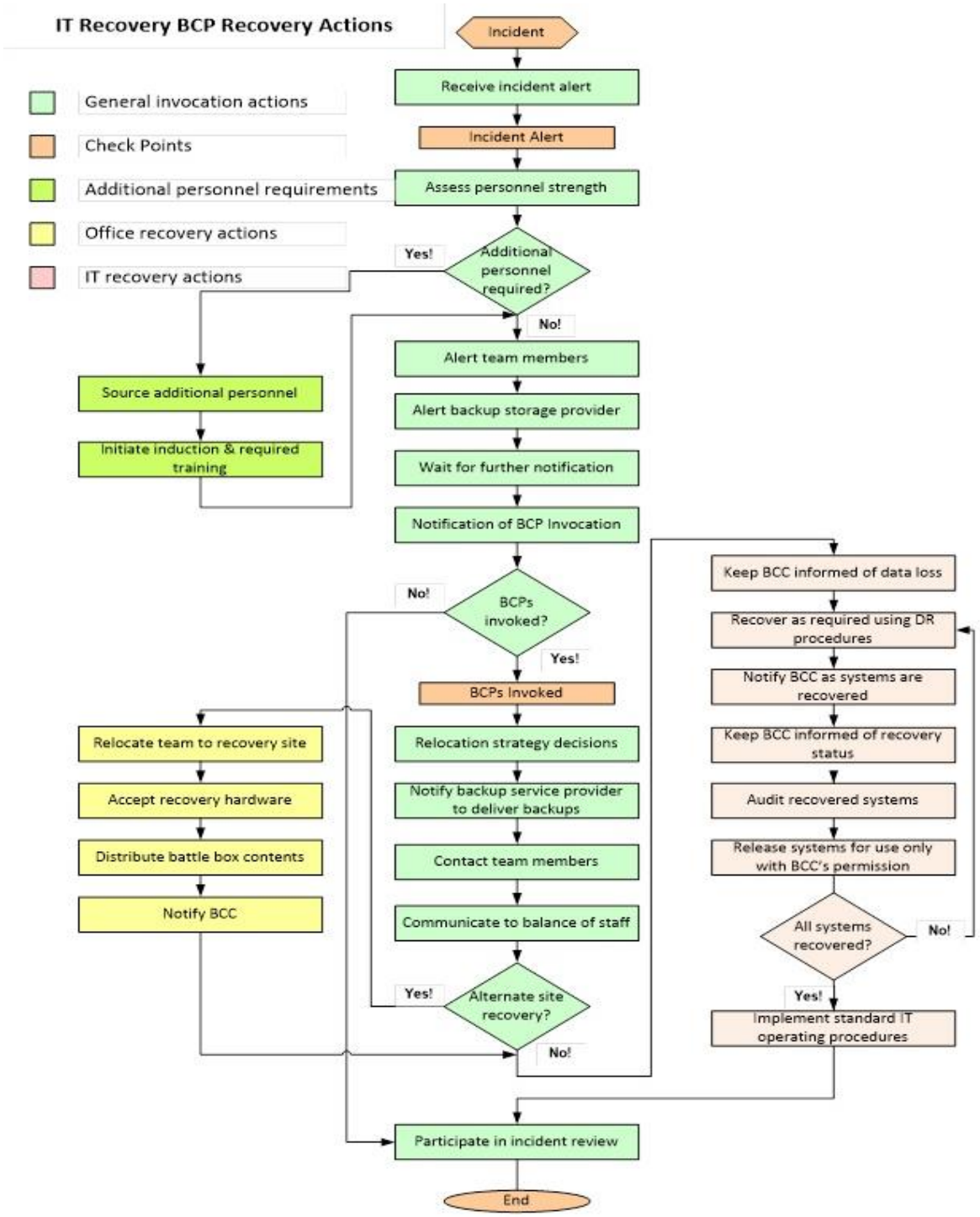
This DRP contains a set of procedures to enable the IT Recovery team to recover critical systems at an alternate site (FTLM – Regional Office) within stipulated Recovery Time Objectives (RTOs) and to stipulated Recovery Point Objectives (RPOs) in order for the Fetakgomo Tubatse Local Municipality (FTLM) to recovery their Mission Critical Activities (MCAs) within their required RTOs, and to identify and recover lost data and lists the resources required to enable the above.

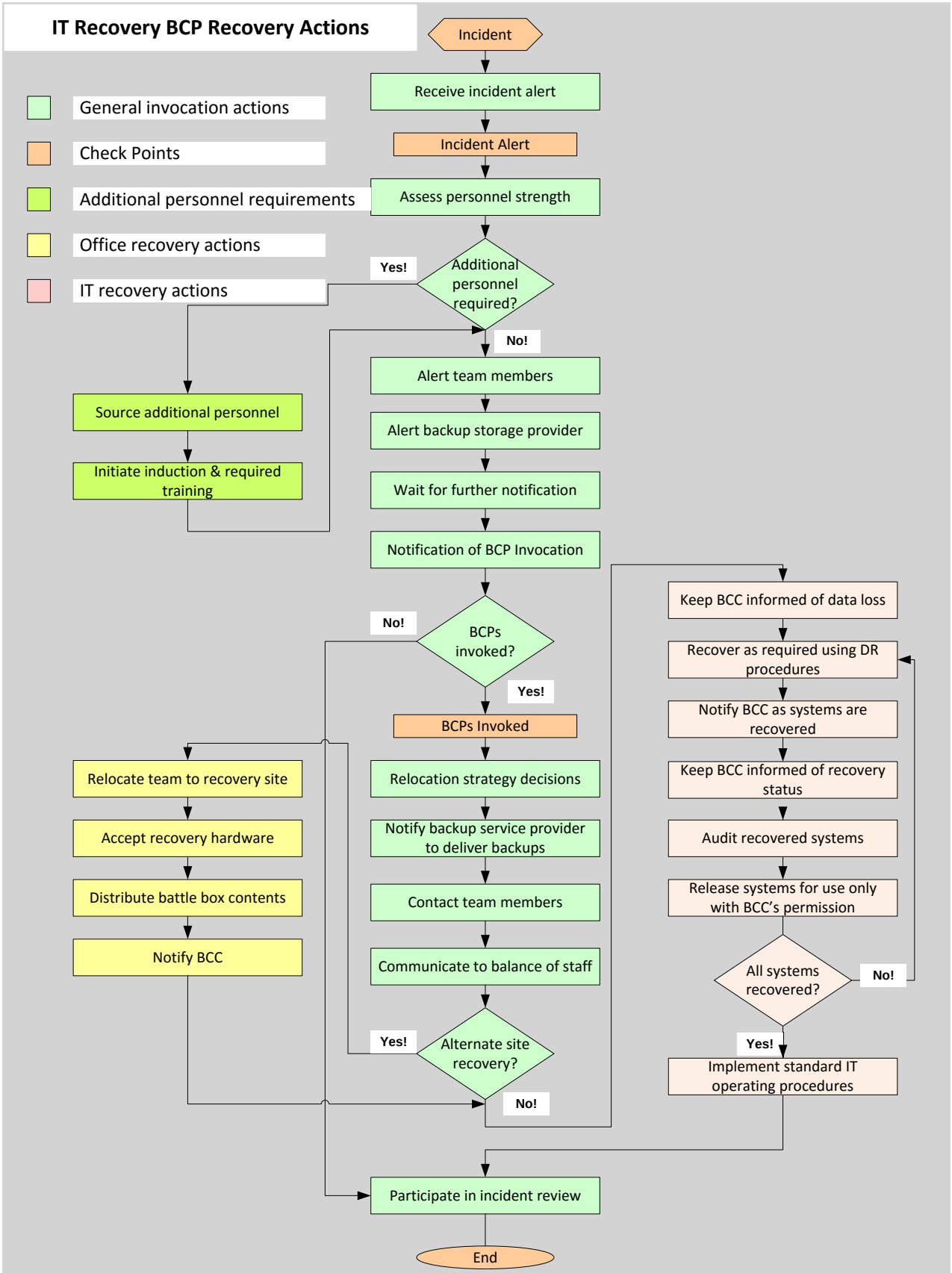
This document is used in conjunction with the Common Data document, which contains associated data common to all of the plans.

A full copy of the DRP is kept by the IT Manager or Business Continuity Coordinator (BCC).

Refer to Section1 of the common data document for the full schematic which identifies all components that constitute the Fetakgomo Tubatse Local Municipality (FTLM) Disaster Recovery Plans.

7. DRP Invocation Actions Flowchart





8. DRP Invocation Actions

No.	Actions	Status/Notes
ITR 010	Note: Actions below make allowance for one of the following possible scenarios: • Additional Personnel Requirements • Office Relocation • IT Recovery	
ITR 020	RECEIVE INCIDENT ALERT Receive notification from the IT Manager/BCC of an incident affecting FTLM's functionality. Ensure the extent of the incident and what is expected of the team is understood.	
ITR 030	CHECKPOINT ONE - Incident Alert.	
ITR 040	ASSESS PERSONNEL AVAILABILITY Assess what personnel and skills are available and if no additional personnel or skills are required go to ITR 080 or continue with Action ITR 050.	
ITR 050	**Additional Personnel Requirements**	
ITR 060	SOURCE ADDITIONAL PERSONNEL Source additional personnel require**d** to perform recovery procedures.	
ITR 070	INITIATE INDUCTION AND ADDITIONAL TRAINING Initiate any induction or additional training that might be required to assist the additional sourced team members to perform the required processes.	
ITR 080	OPTIONAL - ALERT TEAM MEMBERS If required at this stage contact team members to place them on alert. Explain what has happened and course of action. *(For contact details refer to Sections 2 & 3 of the Common Data document)* Reinforce the media communications policy. *(For communications procedures refer to Section 4.3 of the Common Data document)*	
BCC 085	WARN BACKUP STORAGE SUPPLIER If required warn backup storage supplier of possible backup delivery requirements. (*For contact details refer to Section 5.2*)	
ITR 090	WAIT FOR FURTHER NOTIFICATION Wait for further notification from the IT Manager/BCC with regard to decisions made by the Management team.	

No.	Actions	Status/Notes
ITR 100	NOTIFICATION OF DRP INVOCATION Receive notification from the IT Manager / BCC that the DRPs have been invoked. Ensure course of action is understood and agree on reporting intervals with the IT Manager / BCC.	
ITR 110	NOTE: If DRPs have not been invoked go to ITR 320 otherwise continue with ITR 120.	
ITR 120	CHECKPOINT TWO - DRPs invoked.	
ITR 130	RELOCATIONS STRATEGY DECISIONS If alternate site recovery is required, decide which IT team members must relocate to the recovery site?	
ITR 135	NOTIFY BACKUP STORAGE SUPPLIER Notify the backup storage supplier of the decision taken by management not to invoke the DRPs. (*For contact details refer to Section 5.2*)	
ITR 140	CONTACT TEAM MEMBERS Contact team members and inform them of the situation and what is expected of them. *(For contact details refer to Sections 2 & 3 of the Common Data document)* Reinforce the media communications policy. *(For communications procedures refer to Section 4.3 of the Common Data document)*	
ITR 150	COMMUNICATE TO BALANCE OF STAFF Contact balance of staff and inform them of the situation and what is expected of them. *(For contact details refer to Sections 2 & 3 of the Common Data document)* Reinforce the media communications policy. *(For communications procedures refer to Section 4.3 of the Common Data document)*	
ITR 160	Note: If recovery site **not** required for recovery go to Action ITR 230 otherwise continue with Action ITR 170.	
ITR 170	**Recovery Site Relocation**	
ITR 180	RELOCATE TEAM TO RECOVERY SITE Designated team members (decided on in Action ITR130) to relocate to the recovery site. *(For recovery site maps refer to Section 5 of the Common Data document)*	
ITR 190	DISTRIBUTE BATTLE BOX CONTENTS Distribute the contents of the Battle Box. *(For Battle Box details refer to Section **5.1.**)*	
ITR 200	ACCEPT RECOVERY HARDWARE Accept recovery hardware from DR site manager.	
ITR 220	KEEP IT Manager / BCC INFORMED Keep the IT Manager / BCC apprised of the recovery status at intervals previously agreed to in Action ITR100.	

No.	Actions	Status/Notes
ITR 230	IT Recovery	
ITR 240	INFORM IT Manager / BCC OF DATA LOSS Keep the BCC apprised of what backups are being used and the extent of the data loss, if any, per system.	
ITR 250	PERFORM REQUIRED RECOVERY Perform recovery of required systems/applications as per IT Recovery Strategy. *(For details regarding IT Recovery Strategy refer to Section 4.3.)*	
ITR 260	NOTIFY IT Manager / BCC Notify BCC as systems are recovered.	
ITR 270	KEEP BCC INFORMED Keep BCC informed of recovery status.	
ITR 280	AUDIT RECOVERED SYSTEMS Audit recovered systems to ensure the systems have been recovered correctly and are ready for use. (*For details regarding the auditing procedure refer to Section 4.4*)	
ITR 290	RELEASE SYSTEMS FOR USE Release the recovered systems for use only with permission from the IT Manager / BCC.	
ITR 300	**Note:** This could be a reiterative process for each application as they are recovered. If all required systems have been recovered continue with Action ITR 310 otherwise go the Action ITR 240 for each system that required recovery.	
ITR 310	IMPLEMENT OPERATING PROCEDURES Implement standard IT operating procedures (SOP) at the recovered site.	
ITR 320	**General Actions**	
ITR 340	PARTICIPATE IN INCIDENT REVIEW Participate in an incident review meeting that will be called by the IT Manager/BCC for team leaders in order to address any shortcomings in the plans and update DRPs where necessary.	

9. Procedures

9.1 Source Additional Team Personnel

The FTLM has an HR department that is responsible for staff recruitment amongst its many responsibilities.

This means should there be a need for an additional resource the recruitment process will be faster.

Please refer to FTLM procedure on recruitment

9.2 Initiate Induction And Additional Training

Please refer to FTLM procedure on recruitment

9.3 IT Recovery Strategy

This refers to FTLM's IT Disaster Recovery Plan and location of where it is stored at the off-site recovery facility).

9.4 Server Recovery Sequence

System owners will audit the recovered systems to ensure compliance to FTLM's RPO's.

Number	Hostname	Application	Inter-server Dependencies	Critical (Y/N)	Recovery Priority
1	GTM-SRV-DC01	Active Directory, DHCP, DNS	Primary Domain Controller	Y	1
2	GTM-SRV-DC02	Active Directory, DHCP, DNS	Is dependent on the Primary Domain Controller. If the Primary DC is up, then the second does not have to come on during the DR period	Y	2
3	GTM-SRV-MAN01	File/Application Server	Requires a host to run from –	Y	3

4		Venus	Requires a host to run from –	Y	3
5		Payday	Requires a host to run from –	Y	3
6	GTM-SRV-EXC02	Primary Exchange Server	Requires a host to run from –.	Y	3
7		SQL Server	Requires a host to run from –	Y	4

9.5. Auditing of Recovered Systems

System owners will audit the recovered systems to ensure compliance to FTLM's RPO's.

10. Resources

10.1 Battle Box Details

Item Description	Quantity
IT Disaster recovery plan	1
IT002 IT Back-ups and Restoration Procedure	1
Usernames and passwords envelope	1
Server software installation keys envelope	1
Change control forms envelope	2
Other IT forms envelopes	3

10.2 Third Party Contact Details

Company	Solution/system	Contact details

		Name	Tel	Cell
VIP	VIP Payroll, ESS			
Mashcorp2008	PBX/ Telephone/ Teleconferencing	Mr. Brian Chiyaka	013 231 1000	083 285 8244
	Website			
	Internet Link / Data Line			
Telkom	ISDN			
Mashcorp2008	Disaster Recovery	Mr. Brian Chiyaka Mr. Chris Kleynhans	013 231 1000 012 433 6480	083 285 8244 073 907 8062
Payday				
Venus				
Fujitsu	Thin Client			

11. Plan Preparation and Maintenance Actions

No	Actions	Resp.	Start	End
DEP 390	BATTLE BOX INVENTORY AND MAINTENANCE Develop a comprehensive Battle Box requirements list, ensure the Battle Box is populated and maintained with the off-site needs of the team.	IT Manager	Start of every quarter	Start of every quarter
DEP 400	PLAN MAINTENANCE Ensure that the plan is kept up-to-date with the team's requirements by participating in reviews and walkthroughs as required.	IT Manager	Start of every quarter	Start of every quarter

12. Disaster Recovery Plan Review

a. This Recovery Plan shall be reviewed 36 months after the day of council approval.

13. Version Control

Document Creation or Maintenance Revision Control		
Revision Number	**Change Effected**	**Date of Issue**
1.0	Plan developed and first issue to Team Leader	