Molemole Municipality BUSINESS

CONTINUITY PLAN

Revision: Version 1.0

Effective date: 31 May 2022

Molemole Municipality

1. Introduction

A business continuity plan (BCP) is a plan to help ensure that business processes can continue during a time of emergency or disaster. Such emergencies or disasters might include a fire or any other case where business is not able to occur under normal conditions. Businesses need to look at all such potential threats and devise BCPs to ensure continued operations should the threat become a reality.

A business continuity plan involves the following:

1. Analysis of organizational threats
2. A list of the primary tasks required to keep the organization operations flowing
3. Easily located management contact information
4. Explanation of where personnel should go if there is a disastrous event
5. Information on data backups and organization site backup
6. Collaboration among all facets of the organization
7. Buy-in from everyone in the organization

The recovery time objective for this activity is < 4 hours.

Recovery Manager, i.e. person responsible for the recovery of this activity is ICT Manager

The activity will recover in the following way:

a) Recovery of the activity at an alternative site – relocating all resources or activities to an alternative site. Molemole has established an alternate site at SITA in Polokwane.

2. Performing key tasks and obligations

The activity must perform the following tasks and obligations:

Name of resource	Description	Amount	When the resource is necessary
People:			
Manyelo Maphuti	ICT: Manager		
Rapetswa Manakedi	IT Officers		
Applications / databases:			
Venus	Finance		Replicated
Exchange	Emails		Replicated
Itron	Prepaid Electricity		Replicated
GIS	Graphical Information System		Replicated
Case ware	AFS system		Replicated
Payday	Payroll System		Replicated
File Server	Data storage		Replicated
Data stored in electronic form:			

User Data	All user data for the above production systems		Replicated
Data stored on paper:			
Standard Operations Procedures	Procedures are in place		Stored at alternate site
IT and communications equipment:			
All critical IT infrastructures will be replicated at alternate site.	Critical ICT hardware and systems		Replicated at alternate site
Communication channels:			
Email	These facilities will be provided at alternate site		
Telephone			
Internet			
Fax			
Other equipment:			
Facilities and infrastructure:			
Server Room	All of these will be provided for at alternate site		
Air Conditioning			
UPS			
Generator			
Environmental Control Systems			
External services:			
All contracted (SLA) service providers (Applications hardware software support etc.)	Contracts will be extended to alternate site as well.		
All contracted (SLA) service providers (Applications hardware software support etc.)	Contracts will be extended to alternate site as well.		

Resource recovery for this activity will be executed in the following way:

- Hardware and other ICT equipment will recover in the following way: a) advance purchase and installation of equipment at an alternative site, the recovery time objective is short, the equipment is complex and it will be installed in advance, regardless of the occurrence of a possible incident. This process has already started.

- Human resources will recover in the following way: a) detailed documenting of procedures for activities enabling other persons to implement them; b) providing training for employees, c) sharing key knowledge and skills with several persons in order to disperse risk;

d) Using external suppliers for certain operations in case the organisations own employees are unavailable; e) substitution planning in case certain employees are unavailable – the substitutes may be persons within the same organisational unit or persons located nearer to the alternative site; or f) managing knowledge of existing and former employees, suppliers and outsourcing partners, and documenting such knowledge in various knowledge bases

Note: the recovery strategy for applications/databases and external services will be specified in the

General part of the Strategy.

4. Backup procedure

Backup copies of data used by this activity must be made at the following intervals:

Name of application, database, folder, document:	***Frequency of making backup copies***	***Backup procedure***
		[a) applications/databases - automated server-based backup procedure; b) electronic documents - storing in intranet folders for which backup copies are created automatically; c) paper documents - receiving all fax documents by electronic means, or scanning the documents, or copying them and storing at two separate locations]

Note: the frequency of making backup copies of data shared by other activities is defined in the general part of the Strategy.

Appendix 5 - Preparation Plan for Business Continuity

In order to implement the Business Continuity Strategy, it is necessary to carry out the following preparations to meet conditions for a successful resumption of business operations after a disruptive incident:

Description of preparation	*Item in Strategy*	*Necessary financial and other resources*	*Responsible person*	*Start and completion deadlines*	*Method for evaluation of results*
Complete Business Continuity Policy	1		Manager: ICT	Completed	Approved BCP
Complete IT Recovery Strategy	2		Manager: ICT	Completed	Approved ITRS
Complete IT Recovery Plan	3		Manager: ICT	Completed	Approved ITRP
Plan Installation for backup Site and Test	4	Included in the SLA	Manager: ICT	Completed	Backup Server
Application/database installation, preparation of installation media	5		Manager: ICT	Completed	
Creating backup copies	6		Manager: ICT	Completed	
Implement single point of failure avoidance strategies	7		Manager: ICT	Completed	
Complete Recovery Strategy for each Business Unit	8		Manager: ICT	Completed	
Complete Recovery Plan for each Business Unit	9		Manager: ICT	Completed	
Prepare the members of the Crisis Management Team and if necessary the Crisis Management Support Team for their role in handling disruptive incident.	10		Appointed Service provider	Completed	
Complete Business Continuity Plan	11		Manager: ICT	Completed	
Prepare employees in Molemole to handle incidents related to IT and communications technology	12		Manager: ICT	Completed	

Prepare employees in Molemole for handling other incidents	13		Manager: ICT	Completed	
Create all necessary conditions for cooperation with the Police	14		Senior Manager: Community Services	Completed	
Create all necessary conditions for cooperation with the Ambulance	15		Senior Manager: Community Services	Completed	
Create all necessary conditions for cooperation with the Fire Service	16		Senior Manager: Community Services	Completed	
Create all necessary conditions for cooperation with [list other authorities]	17		Senior Manager: Corporate Services	Completed	
...	18			Completed	
Write and maintain evacuation plans in the case of fire	19		Senior Manager: Corporate Services	Completed	
Purchase/prepare and if necessary maintain means of communication	20		Municipal Manager	Completed	
Prepare all means of transport	20		Senior Manager: Corporate Services	Completed	
Prepare persons responsible for communication during disruptive incident	21		Municipal Manager	Completed	
Prepare templates for media statements	22		Municipal Manager	Completed	
Manage relationships with suppliers and outsourcing partners	23		Senior Manager: Corporate Services	Completed	
Make all necessary arrangements for provision of financial resources	24		CFO	Completed	
Write recovery plans for individual activities	25		Manager: ICT	Completed	

Prepare resources for individual activities	26		Manager: ICT	Completed	

Change history

Date	Version	Created by	Description of change

Table of contents

1. Purpose, scope and users

The purpose of the Recovery Plan is to define precisely how Molemole will recover this activity within set deadlines, in the case of a disaster or other disruptive incident. The objective of this Plan is to complete the recovery of this activity within the set recovery time objective. This Plan includes all resources and processes necessary for the recovery of this activity. Users of this document are members of the Crisis Management Team and employee's necessary for the recovery of this activity.

2. General

Recovery time objective:	Less Than 4 hours
Person responsible for recovery plan activation / means of activation:	Manager: ICT (oral and written)
People who must be notified about plan activation / who is responsible:	Notify SMT (Strategic Management Team) 1. Senior Manager: Corporate Services 2. Senior Manager: Community Services 3. Senior Manager: Technical Services 4. Senior Manager: LED 5. CFO 6 Municipal Manager
Person responsible for deactivation of recovery plan / means of deactivation / criteria:	Manager: ICT (oral and written)
Key tasks/obligations and respective deadlines:	Manager: ICT oral and written
Minimum acceptable amount of work immediately after the disaster (MBCO – minimum business continuity objective):	Manager: ICT oral and written
Period after which the normal operational level must be resumed:	Manager: ICT oral and written
Instructions for manual work if ICT resources are unavailable:	Manager: ICT oral and written

3. Roles and contact information

No.	*Role in recovery*	*Name*	*Job title / organizational unit*	*Mobile phone*	*Landline phone*	*E-mail*	*Home address*	*No. of substitute*
1.	Recovery Manager	Manyelo Maphuti	Manager: ICT	0723566789	015 501 2354	Manyelomf@molemole.gov.za	7452 Lizard street Serala view	
2.	Substitute	Rapetswa Manakedi	IT Officer	-	015 501 2354	manakedi@molemole.gov.za	Botlokwa	

External contacts Suppliers, outsourcing partners, state authorities etc.

No.	*Name of organization*	*Name*	*Job title / organization l unit*	*Mobile phone*	*Landline phone*	*E-mail*	*No. of substitute*	*No. of substitute*
1.	Payday							
2.	Venus							
3.	ITRON							
4.	Case Ware							

4. Authorisations in a crisis

Role in recovery / job title	*Authorisations*
Municipal Manager	Authorised to take all steps specified in the Business Continuity Plan and this Recovery Plan in order to recover the activity
Municipal Manager	Authorised for urgent purchases of equipment/services up to [amount]
Municipal Manager	Authorised to communicate with clients
Municipal Manager	Authorised to communicate with [name of state authority]
Municipal Manager	Authorised to cooperate with [name of supplier/outsourcing partner]
Other authorisations Needed	

The following resources will be used for the recovery of this activity:

Name of resource	*Description of where resources are located*	*Amount*	*When the resource is necessary*	*Person responsible for obtaining the resource*
People:				

All ICT Staff	Molemole Offices		Disaster is Declared	Manager: ICT
Applications / databases:				
Venus	Molemole Offices		Disaster is Declared	Manager: ICT
Exchange	Molemole Offices		Disaster is Declared	Manager: ICT
Itron	Molemole Offices		Disaster is Declared	Manager: ICT
GIS	Molemole Offices		Disaster is Declared	Manager: ICT
All user Data	Molemole Offices		Disaster is Declared	Manager: ICT
IT and communications equipment:				
List when Acquired				
Facilities and infrastructure:				
External services				

6. Recovery steps for the activity [Staff have been moved to Recovery site and this is the start of the recovery plan]

This activity should be recovered in the following way: **TO BE COMPLETED WHEN ALTERNATIVE SITE IS Established and Operating**

Recovery procedures (main steps / individual tasks)	*Persons responsible for implementation*	*Communication (content, to whom)*	*Implementation record (date / time)*
1. Arrive at alternate site	**Manager: ICT**	**Municipal Manager**	
a. Gathering of the team at the alternative site	**Manager: ICT**	**Crisis Management Team**	
b. Checking and recovering basic infrastructure and furniture	**Manager: ICT**	**Users**	
2. Checking and recovering ICT equipment and links	**Manager: ICT**	**Users**	
a. Checking and recovering applications	**Manager: ICT**	**Vendor & Users**	

7. Managing records kept on the basis of this document

Record name	*Storage location*	*Person responsible for storage*	*Controls for record protection*	*Retention time*
Record of recovery step implementation (record in paper form)	Archive BCP Coordinator	SITA	Records are stored in a locked cabinet	3 years

Only BCP Coordinator can grant other employees access to the records.

8. Validity and document management

This document is valid as of 01/07/2015

This document, together with all additional documents, is stored in the following way:

- the paper form of the document is stored at the following locations: Command Centre, Registry and DR Site
- the electronic form of the document is stored in the following way: File Server and mail server

The owner of this document is Municipal Manager, who must check and if necessary update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- number of corrective actions based on conducted exercises
- number of corrective actions based on implementation of the plan in a crisis
- in the case of a crisis, whether the recovery was completed within the recovery time objective

9. Additional documents

- [technical documentation for ICT systems]
- [detailed recovery plans for individual ICT systems]
- [working instructions]

Municipal Manager

_____

Signature

Change History

Date	Version	Created by	Description of change

TABLE OF CONTENTS

1. Purpose, scope and users

The purpose of this Plan is to ensure the protection of health and safety of people in the case of disaster or other incident, and to contain the incident. The objective is to reduce damage to the business to the smallest possible extent.

This Plan is applied to all major incidents threatening to disrupt any critical activity within the Business Continuity Management Systems (BCMS) scope for a period longer than the recovery point objective for each individual activity (further in text: disruptive incidents).

Users of this document are all employees of the Molemole Municipality.

2. Authorisations and responsibilities in incident response

Role in recovery / job title	*Authorisations and responsibilities*
Any employee	Notifying the responsible organisational unit about the incident
Manager: ICT	All steps necessary to resolve incidents related to ICT and communications technology
Manager: ICT	All steps necessary to resolve all other incidents
Manager: ICT	Activation of recovery plans for activities
Senior Manager: Community Services and Manager Communication's	Communication with public media - this person has exclusive authorisation for communication with the public media
Director Corporate Services	Psychological help for employees

3. Communication

(This section should be expanded with procedures regarding national or regional threat advisory systems were they exist)

The following table lists responsibilities for communication (sending as well as receiving information and responding to information requests) with various types of interested parties:

	[Telephone]	*[Meetings]*	*[E-mail]*	*[Press conferences]*	*[Media]*
[Employees]					
[Owners / shareholders]					
[Employees' relatives]					
[Clients]					
[Public media]					
[Associations]					
[Emergency services]					
[various state authorities]					
[Owners / shareholders]					

The communication procedure is as follows:

1. Any employee who receives a communication request or wants to initiate communication towards interested parties must forward such request to the responsible person as indicated in the table above.

2. Director Strategic and Social Development must agree

Municipal Manager on the content of the communication.

3. If the communication with external parties includes significant risks and impacts, the decision about such communication must be documented and formally approved by Municipal Manager before such information is released.

4. After getting appropriate approval, Director Strategic and Social Development provide information to interested party. Director Strategic and Social Development is responsible for documenting each communication with any interested party.

4. Procedures for disruptive incidents (Include here all incidents identified as most probable during risk assessment)

4.1. Managing a disruptive incident

4.1.1. Obligation of every employee to report incidents

Every employee is obliged to report any disruptive incident in the following way:

- all incidents related to IT and communications technology are reported by telephone or if not urgent via e-mail to IT Manager or IT Department
- All other incidents are reported by telephone to Crisis Manager.

Any other event or system vulnerability that has not yet developed into a disruptive incident must be reported in the same way.

If an incident requires intervention of the police, ambulance or fire service, the first available person must call Crisis Manager.

In case an incident occurs, employees can freely communicate only with their relatives and the police, ambulance, or fire service, while all other communication is left to the Crisis Management Team.

4.1.2. Disruptive incident handling

The person who received information about the incident must assess whether the incident/potential incident is real or false, and if it is determined to be real, immediately activate this plan by taking the following steps:

- Start containing and eradicating the incident as described in the following sections of this document notify all responsible persons about the occurrence of the incident within their area of responsibility
- Notify Crisis Manager, who must consider whether any of the interested parties need to be alerted
- Monitor the status of an incident and, as necessary, inform the incident reporter and other employees involved in the incident about the progress of incident handling. In case a person is unable to contain and/or eradicate the incident, he/she must inform the Crisis Manager. The information that is forwarded to the Crisis Manager must include the nature and extent of a disruptive incident and its potential impact. The person responsible for eradicating the incident must record all the actions taken into the Incident Log.

4.1.3. Crisis Manager

The Crisis Manager must monitor the progress of incident handling and the period of disruption of individual activities, and assess the time needed to solve the incident.

If the required time to solve the incident is longer than the recovery time objective of a particular activity, the recovery plan for disrupted activity must be activated. In that case the Crisis Manager must notify all recovery managers who will have to activate their recovery plans.

4.2. Containing and eradicating an incident

4.2.1. Evacuation of the building (regardless of incident type)

The building is evacuated to assembly points specified in the List of Business Continuity Sites, appended to the Business Continuity Plan.

Crisis Manager	• In case people's lives or health are threatened, issue an evacuation order • If Assembly Point 1 is unavailable, send someone to mark the location of Assembly Point 2 (paper sign, pointing arrows, flags, vehicle signs, etc.) • In case of a malicious threat (e.g. bomb threat), make a decision about the new assembly point location (Assembly Point 3) and notify the person responsible for executing evacuation
Persons responsible	• Direct evacuation towards the assembly point

for executing evacuation	• Check that all rooms are empty after evacuation, leave the rooms and lock the doors • In case someone was unable to leave the building, inform the [telephone number of emergency service]
All employees	• Evacuate in accordance with evacuation plans for your building • Follow the instructions provided by persons responsible for directing evacuation • Do not use mobile phones during evacuation • When evacuating, take only your handbag and wallet, do not take any other items with you • Assist others in evacuation if they need help
Crisis Management Support Team	• When people have gathered at the assembly point, keep record of all present and missing persons

4.2.2. Fire

The building is evacuated in accordance with the building evacuation plan.

Crisis Manager	• In case people's lives or health are threatened, Crisis Manager issues an evacuation order • He/she selects measures to reduce damage or save property, unless this represents a risk for the people

4.2.3. Interruption of power supply

Crisis Management Support Team	• Establish the cause of interruption - is it caused by the wiring or by the electricity distributor
Manager: Electricity	• Solve the problem together with the electricity distributor
All employees	• In line with the recovery plans, proceed with alternative ways of executing activities, without the use of electricity
Employees in [IT department]	• Monitor UPS devices and execute information system shutdown as necessary

4.2.4. Earthquake

The building is evacuated in accordance with the building evacuation plan.

All employees	• Find shelter under a door frame, close to an inside bearing wall or under a desk • Do not use lifts • Do not run outside the building until the end of earthquake • When the earthquake is over, try to save people's lives unless this inflicts even more damage to the injured • In case evacuation is ordered, proceed according to the evacuation plan
Crisis Manager	• In case people's lives or health are threatened, order evacuation of the building when the earthquake is over
Crisis Management Support Team	• Shut down all utilities - gas, electricity, heating, ventilation, water supply • Secure the building and other property

4.2.5. Threat letter

All employees	• If you receive a suspicious letter , do not open it, hold it only at its outer edges • Put it in an empty envelope • Notify [job title] • Proceed according to instructions by [job title]
Senior Manager: Corporate Services	• Notify the police on [telephone number] • Notify the superior of the employee who reported about the letter • Execute measures as instructed by police

4.2.6. Threat call / bomb threat

All employees	• If you receive a threat call, write down the exact time and the caller's telephone number • Write down the caller's exact words • Allow the caller to say as much as possible, without interruptions: - try to make him/her talk - repeat your questions, say you didn't understand what they were saying - if your phone is equipped with a speaker, put the call on speaker and ask someone to take notes - repeat each request made by the caller • In the case of a bomb threat, ask the caller the following questions: - Will the bomb go off? When? - Can it be deactivated? How? - Where is it located?

	- What does it look like? - Why is it placed - what are the requests? - Who is calling? Can you introduce yourself? • Open office doors only if you are sure that they are not wired to the bomb • Do not search the building looking for the bomb! This is the job of the police • Do not touch any unknown objects • If evacuation is ordered, proceed according to the evacuation plan
Crisis Manager	• Notify the responsible person in the organizational unit targeted by the threat • Do not use standard assembly points - select a new assembly point • If you assess that the bomb could really go off, order evacuation; assembly point should be at least 300 metres away • Notify persons responsible for evacuation and the Crisis Management Support Team about the new assembly point location • In case of an explosion, make a decision to get the injured away from the affected area as soon as possible

4.2.7. Telecommunications failure

Employee in [IT department]	• Any employee receives information about the failure • As needed, he/she coordinates the process with IT service providers
Employees - users of communications services	• Use alternative means of communication

4.2.8. Information system failure

Employee in [IT department]	• Any employee receives information about the incident • As necessary, he/she coordinates the process with IT service providers • Take necessary measures to prevent or contain the information system incident
Crisis Manager	• Consultation with all relevant services, assessment of incident severity
All employees	• If possible, proceed to alternative ways of carrying out activities

4.2.9. Malicious code attack

Employee in [IT department]	• Any employee receives information about the incident • If dealing with an unknown type of malicious code, [name of organization responsible for information security] should be notified • Notify the producer of antivirus software • If the external source of malicious code has been identified, contact the person responsible for IT in that organization • Coordinate notification of other employees, particularly those who exchanged messages with the infected system • As needed, coordinate the process with IT service providers
All employees	• Physically disconnect any infected PC from the network; disable wireless networks, Bluetooth, etc. • do not shut down the network devices and servers - this is the job of people from [IT department]
Employees	• If the computer is still not disconnected from the network, assess whether to disconnect it to prevent further infection • Disable all wireless connections on the computer • Close your software (including the operating system) - for servers, assess whether system users should be notified first • Find information about the type of malicious code and necessary steps for its eradication (from the Internet, from the suppliers) • Proceed according to received instructions
	•

4.2.10. Violation of internal or external rules

Manager: Legal Services	• The procedure is carried out as required by the labour laws regulating disciplinary procedures and the organization's own disciplinary procedures

5. Managing records kept on the basis of this document

Record name	*Storage location*	*Person responsible for storage*	*Controls for record protection*	*Retention time*
Incident log	Shared folder on the intranet	Director Corporate services	only Manager: ICT has the right to edit the list	3 years

6. Validity and document management

This document is valid as of [date]

This document, together with all additional materials, is stored in the following way:

- The paper form of the document is stored at the following locations: Command Centre, and all alternative sites for activities
- The electronic form of the document is stored in the following way: [provide intranet folder name] and access is allowed to only those authorised to use it.

The owner of this document is Municipal Manager, who must check and if necessary update the document at least once a year. When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- number of incidents not covered by this document
- whether steps described in this document are feasible in real situations
- incident response time

Municipal Manager

BUSINESS CONTINUITY PLAN

Code:	
Version:	
Date of version:	
Created by:	
Approved by:	
Confidentiality level:	

Table of contents

1. Purpose, scope and users

The purpose of the Business Continuity Plan is to define precisely how Molemole will manage incidents in the case of a disaster or other disruptive incident, and how it will recover its activities within set deadlines. The objective of this plan is to keep the damage of a disruptive incident at an acceptable level.

This plan is applied to all critical activities inside the scope of the Business Continuity Management System (BCMS).

Users of this document are all staff members, both inside and outside the organization, who have a role in business continuity.

2. Reference documents

- ISO 22301 standard, clause 8.4
- ISO/IEC 27001 standard, clause A.14.1.3
- BS 25999-2 standard, clause 4.3
- List of statutory, regulatory, contractual and other requirements
- Business Continuity Policy
- Business Impact Analysis questionnaires
- Business Continuity Strategy

3. Business Continuity Plan

3.1. Plan content

This Business Continuity Plan consists of two major parts:

- Incident Response Plan - Appendix 1 - a plan that defines direct response to the occurrence of various types of incidents
- Recovery plans for individual activities - these are prepared separately for each activity - Appendix 6 and on - plans dealing with the recovery of necessary resources for each activity

Each of these plans defines its activation procedure.

3.2. Assumptions

For this plan to be effective, all the resources and arrangements specified in the Business Continuity Strategy need to be prepared.

3.3. Appointments and authorities

The following bodies are formed when a disruptive incident occurs:

Crisis Management Team		
Members:	Substitutes:	Role:
Senior Manager: Corporate Services		
Senior Manager: Technical Services		
CFO		
Senior Manager: Community Services		
Senior Manager: LEDP		
Crisis Management Support Team		
Members:	Substitutes:	Role
Manager: ICT		
Manager: Administration		
Manager: Electricity		
Manager: LED		
Manager: Budget, Expenditure and Revenue		

The purpose of the Crisis Management Team is to make all key decisions and coordinate actions during the disruptive incident; the purpose of the Crisis Management Support Team is to relieve the Crisis Management Team from administrative and other operational activities, in order to focus on managing the disruptive incident. Members of the Crisis Management Support Team are directly responsible to the Crisis Management Team.

Recovery managers for individual activities are appointed in the recovery plans for the said activities.

Authorisations for action during disruptive incident are the following

Type of decision	***Who is authorised***
How small incidents related to IT and communications technology are resolved	Employees in ICT Business Unit
How all other small incidents are resolved	Employees in Disaster Management Unit
Making a decision about invoking recovery plans	Crisis Manager
Making a decision about the selection of alternative site (use of close or remote alternative site)	Crisis Manager
Informing employees about the invocation of recovery plans	Crisis Manager; if he/she is unable to do it, then recovery manager for individual activity
Implementing all tasks necessary for the recovery of individual activities	Recovery Manager for individual activity
Content of the communication for different interested parties	Crisis Manager
Selecting information to be provided to the public media during disruptive incident	Municipal Manager
Purchases during disruptive incident - over [amount]	Municipal Manager

Purchases during disruptive incident - up to [amount]	Municipal Manager

3.4. Plan activation; plan deactivation

The Incident Response Plan is activated automatically in case an incident occurs, or a potential incident is threatening its activities. The Incident Response Plan is deactivated after an incident has been contained or eradicated.

Recovery plans for particular activities are activated exclusively by the Crisis Manager's decision, if he/she assesses that a particular activity will be interrupted for a period longer than the recovery time objective for that activity. The decision of the Crisis Manager may be written or oral.

Recovery plans may be deactivated by recovery managers for individual activities when they establish that all conditions for the resumption of business activities have been met. Recovery plans are deactivated by resuming normal business activities.

3.5. Communication

The following means will be used for communication between the Crisis Management Team and activities, and between activities themselves - they are ordered according to priority (the first one from the list is to be used first; in case it is not available, the next one is used):

1. Mobile phones (business and private)
2. Telephones (business and private)
3. E-mail (sent from business or private computers)
4. [Messaging services - e.g. Skype]
5. Couriers (employees of the organisation or specialised services)
6. [Hand held stations - state where they are stored and who has the right to use them]
7. [Amateur radio stations - state where they are stored and who has the right to use them]
8. [Satellite phones - state where they are stored and who has a right to use them]

Director Strategic and Social Development in the Crisis Management Team is responsible for coordinating communication with all activities.

Responsibilities for communicating with particular interested parties are specified in the Incident Response Plan.

3.6. Sites and transportation

ICT Manager is responsible for ensuring access to each provided alternative site.

Responsibilities for transportation to alternative sites are specified in Appendix 4 - Transportation Plan.

3.7. Order of recovery for activities

Activities must be recovered in the following order: COMPLETED ONCE ALTERNATE SITE IS ESTABLISHED

No.	*Name of activity*	*Recovery time objective*

3.8. Interdependencies and interactions

The dependencies and interactions between activities, as well as with suppliers and external parties, are detailed in the Incident Response Plan and individual recovery plans for activities.

3.9. Required resources

Resources that are required for the recovery of the activities are listed in their recovery plans.

The Command Centre, which serves the Crisis Management Team and Crisis Management Support Team, is equipped as follows: TO COMLETED ONCE ALTERNATE SITE IS ESTABLISHED.

Name of resource	*Description*	*Amount*	*When the resource is necessary*	*Person responsible for obtaining the resource*
Applications / databases:				
Venus	Financial System		Yes	CFO
Exchange	Emails		Yes	ICT Manager
Itron	Electricity		Yes	Manager Electricity
GIS	Geographic Information System		yes	Town Planning Manager
Data in electronic form:				
Data in paper form:				
IT and communications equipment:				
Mail Server				
Telephones				
Internet				

Communication channels:				
Mail Server				
Telephones				
Internet				
Other equipment:				
Facilities and infrastructure:				
External services:				

4. Restoring and resuming business activities from temporary measures

The purpose of restoration and resuming the business activities from temporary measures is to bring the business operations back to business-as-usual – to the normal state as it was prior to the disruptive incident.

The steps described in this section are not time critical – they are to be performed in proportion with the impact of the disruptive incident and in accordance with available resources. The decision to activate each of the following steps is made by the Crisis Manager.

The following steps need to be performed, in this order:

1. Preservation of the damaged assets and evaluation of damage

2. Assessment of the situation and determining options and responsibilities

3. Developing an action plan – determining the steps needed to return activities to normal state

4.1. Preservation of damaged assets and evaluation of damage

Municipal Manager will nominate the team for preserving the damaged assets – the focus of this team is to prevent the damage from spreading.

Municipal Manager will nominate the team for evaluation of damage. The evaluation must consist of the following: name of the asset, location of the asset, type of damage, and cost of damage.

4.2. Assessment of the situation & determining options and responsibilities

Depending on the extent of the damage, the Crisis Manager needs to decide the following: (1) whether to move back to the primary location or look for a new location, (2) whether to purchase

new equipment or repair the existing, (3) when and where the operations of activities that do not support key products and services (activities with lower priority) will be recovered/resumed, and (4) whether there are enough human resources to support normal operations, etc.

Based on these decisions the Crisis Manager must nominate responsible persons for the following:

a) Making claims against insurance policies

b) Restoring facilities

c) Acquiring new facilities

d) Logistics for moving to other locations

e) Repairing the equipment

f) Purchasing new equipment

g) Hiring new personnel

h) Recovering lower priority activities

4.3. Developing action plans

Each responsible person must develop an action plan for his/her area of responsibility, which will – amongst other information – contain the following: (1) steps to be taken, (2) required human resources, (3) required financial resources, and (4) deadlines.

The Crisis Manager must define (1) how to provide necessary funding, (2) procurement process and authorizations, (3) which reports will be sent to the Crisis Management Team, and (4) who will perform the review of the steps once they are completed.

5. Validity and document management

This document is valid as of [date]

This document is stored in the following way:

- the paper form of the document is stored at the following locations: Command Centre, [list locations]
- the electronic form of the document is stored in the following way: [provide location on the intranet]

The owner of this document is Municipal Manager, who must check and if necessary update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Did activities recover within required time?
- Are recovery plans and Incident Response Plan synchronised?
- Did exercising and testing achieve objectives?

6. Appendices

- Appendix 1 - Incident Response Plan
- Appendix 2 - Incident Log

- Appendix 3 - Transportation Plan
- Appendix 4 - Key Contacts
- Appendix 5 - Activity Recovery Plan for ICT Business Unit

Municipal Manager

_____

Code:	
Version:	
Date of version:	
Created by:	
Approved by:	
Confidentiality level:	

Change history

Date	Version	Created by	Description of change

Table of contents

1. Purpose, scope and users

The purpose of this document is to define how Molemole will ensure that all conditions for the resumption of business activities in the case of disaster or other disruptive incident are met. It forms the basis for preparing the Business Continuity Plan and recovery plans.

This document is applied to the entire BCMS scope as defined in the Business Continuity Management Policy.

Users of this document are members of top management and persons implementing the business continuity management project.

2. Reference documents

- ISO 22301 standard, clauses 8.3 and 8.4.2
- BS 25999-2 standard, clauses 4.1.1 and 4.2
- Business Continuity Management Policy
- Business Impact Analysis questionnaires
- Risk Assessment Report
- Business Continuity Plan containing the Incident Response Plan and recovery plans.

3. Recovery Strategy

3.1. Strategy input

This Strategy is written based on Business Impact Analysis results and results of risk assessment and risk treatment.

3.2. Business Impact Analysis

The Business Impact Analysis established that activities listed in Appendix 1 support key products and services - please see Appendix 1 for a list of such activities.

The maximum tolerable period of disruption (maximum acceptable outage) for each activity has been determined in the Business Impact Analysis Questionnaire - please see Appendix 2.

Appendix 3 determines recovery time objectives for each activity, taking into account dependencies on other activities.

3.3. Risk management

Assessment of risks which could affect business continuity is described in [Risk Assessment Report]. The highest risks which could lead to a disruptive incident, i.e., business disruption identified during risk assessment are the following:

For all mentioned risks / incidents it is necessary:

- To apply preventive action to reduce the probability of such incidents - the actions are described in [name of document]
- To apply preventive action in order to minimise possible consequences of such incidents - these actions are also described in [name of document]
- To prepare event scenarios which describe how such incidents could affect the organization's operations; scenarios are provided in Appendix 4 of this Strategy, and must be used at a later point for testing plans
- To define in the Incident Response Plan the appropriate way to respond to each of the incidents

3.4. Detailed Strategy

Together with the business' requirement for high uptime and high availability of critical services, as defined by The Municipality, were key criteria in selecting the appropriate platform.

3.4.1. Deployment Architecture

It is recommended that Molemole solution is architected around two separate interconnected data centres, in order to offer high availability and minimal downtime. The current data room will house the primary production servers. For disaster recovery, a secondary data room will house the recovery servers, where data will either be mirrored in real time or near real time depending on the business requirements, as defined by the Business Impact Analyses and Risk Assessment.

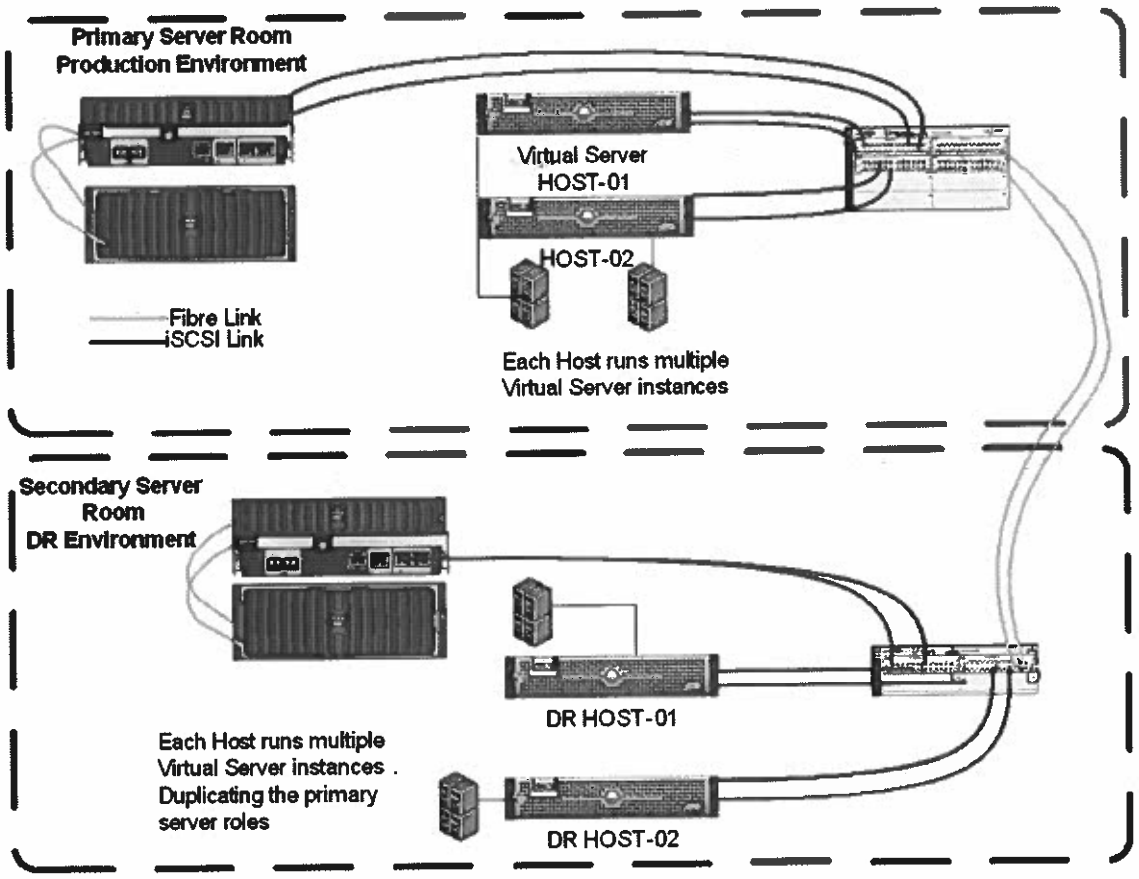
A dual data room approach has been adopted to cater for a Level 3: Main Server Room disaster / off-line. In the event of a Level 3 disaster, the primary time delay factor, contributing to brining the IT services back online, is the provisioning of suitable hardware to recover the systems upon. Without a failover site that has the necessary redundancy, the IT department cannot access the offline data backups. With this in mind, the IT systems that have a high priority and zero downtime at critical times to the business require a fully redundant and duplicated platform design.

The technology platform is based on server virtualization and utilizing a Storage Area Network (SAN) backend as the primary storage mechanism. Application servers will connect to the SAN on which all

operating systems and data will reside. The primary systems will be run on new server hardware, which is based on Intel's latest-generation micro architecture.

Hardware consolidation is achieved by running servers as Virtual Machines. This allows multiple Windows Server instances to be run on a single physical server. Existing server hardware acquired within the last 24 months, which are still under warranty, and supports virtualisation technology will be incorporated. Server virtualization is the masking of server resources, including the number and identity of individual physical servers, processors, and operating systems, from server users. The server administrator uses a software application to divide one physical server into multiple isolated virtual server environments. The virtual server environments are referred to as guest server instances.

Basic diagrammatic representation of the solution:



3.4.2. Why Virtualisation?

Server virtualization conserves space through consolidation. With the traditional approach to server deployment in the past, it was common practice to dedicate each server to a single application. If several applications only use a small amount of processing power, the network administrator can consolidate several machines into one server running multiple virtual environments. As the business requirements for services and hence server hardware to support it, the need for physical space can decrease significantly.

Server virtualization provides a way for companies to practice redundancy without purchasing additional hardware. Redundancy refers to running the same application on multiple servers. It's a safety measure, if a server fails for any reason, another server running the same application can take its place. This minimizes any interruption in service. It wouldn't make sense to build two virtual servers performing the same application on the same physical server. If the physical server were to crash, both virtual servers would also fail. The design incorporates redundant virtual servers on different physical machines, as well as different data centres.

Virtual servers offer the internal IT department isolated, independent systems in which they can test new applications or operating systems. Rather than buying a dedicated physical machine, the network administrator can create a virtual server on an existing machine. Because each virtual server is independent in relation to all the other servers, IT can run tests on new software without worrying about affecting other applications and possibly causing unintentional interruption to business.

Server hardware will eventually become obsolete, and switching from one system to another can be difficult. In order to continue offering the services provided by these outdated systems, sometimes referred to as legacy systems, a network administrator could create a virtual version of the hardware on modern servers. From an application perspective, nothing has changed. The programs perform as if they were still running on the old hardware. This can give the company time to transition to new processes without worrying about hardware failures, particularly if the company that produced the legacy hardware no longer exists and can't fix broken equipment.

3.4.3. Why Utilize a Storage Area Network (SAN)?

A SAN backend with virtualisation offers the following advantages:

1. Better disk utilization

The number one benefit from installing a SAN is better disk utilization. When all your storage is tied together through a centralized storage network, you gain the ability to manage everything as a single entity. This gives you the ability to slice up the central pool of storage resources at the network level and assign that storage more intelligently to the servers that need it. The approach to disk management without a SAN is to buy large numbers of disks and utilize them in large expensive servers so that you can grow into them. All the disk space that's not currently being used is wasted until you need that space.

2. Better hardware utilization

There will be less physical server hardware, resulting in better resource utilisation. Power consumption will be lower due to fewer servers and the use of more efficient blade servers. Additional power savings will be made subsequent to the lower cooling requirements. This supports an initiative to moving to towards "Green IT" as well as lowering the cost of electricity utilisation.

3. DR solution for multiple applications

With many critical servers in the data centre running applications that simply can't go down as well as the need to be recovered quickly if a disaster strikes, the best solution is a SAN. Although the upfront costs for implementing a SAN-based disaster recovery solution are higher than the traditional approach of local storage, the benefits can be realized in just a single hour if a disaster happens. The cost of downtime is critical to business. A SAN-based disaster recovery (DR) solution is like having a good insurance policy on your business.

4. Better availability for your applications

Storage arrays in storage networks are built from the ground up to be as reliable and redundant as possible with the aim to never go down. They use pre-failure notification technology like email home, where the storage array itself sends a notification to the manufacturer to report that one of its components might fail. Equipment that you find in a SAN is built to highly robust standards. Applications fail because of data becoming corrupted by things going wrong with the disks that those applications use. The storage arrays in a SAN use very good data protection algorithms to make sure that your data stays consistent. The best thing that can happen to you is that you forget that your SAN is even there. It just works, like the dial tone on your phone.

5. Backup windows are taking too long

Decreasing the time needed to back up large volumes of data is also one of the major benefits of installing a SAN. With the use of Snapshot Technology that SAN's offer, they enable making hardware-based, exact duplicates of your data almost instantly. The duplicates can be used as both the backup of your data and as a source for backing up that data to a tape library connected to your SAN. This is known as a disk to disk to tape topology that is the ideal method of backup.

The secondary data room as part of the implementation houses a secondary SAN which will provide full redundancy in the event of a disaster. It will contain near live mirror images of the application servers in the primary production environment. It will be located in a separate data room to support a level 3 disaster.

4. Incident response structure

4.1. Crisis Management Team and Crisis Management Support Team

4.1.1. Crisis Management Team

If business continuity plans are activated, a working body called Crisis Management Team is formed which is authorised to make any decisions to resolve the situation. Members of the Crisis Management Team are:

1. Municipal Manager

2. Senior Manager: Corporate Services

3. Senior Manager: Technical Services

4. Senior Manager: Community Services

5. Senior Manager: Local Economic Development and Planning

6. Manager: ICT

The Crisis Management Team is managed by the Crisis Manager. Municipal Manager perform the function of Crisis Manager, and in the case of his/her absence the function will be performed by Acting Municipal Manager

The Crisis Management Team manages the disruptive incident from a facility called the Command Centre, the location of which is specified in item 5.1 of this Strategy.

4.1.2. Crisis Management Support Team

The Crisis Management Support Team has the function of relieving the Crisis Management Team from administrative and other operational activities, in order to focus on managing the disruptive incident.

Members of the Crisis Management Support Team are:

- [secretaries]
- [couriers]
- [security personnel]
- [personnel for non-ICT equipment repairs]
- [other support staff]

The Crisis Management Support Team shall work on locations specified by the Crisis Management Team.

4.1.3. Command Centre Equipment

To serve the Crisis Management Team and Crisis Management Support Team the Command Centre must be equipped as follows: To BE Established

Name of resource	Description	Amount	When the resource is necessary
Applications / databases:			
Venus			
Exchange			
Itron			
GIS			
Data stored in electronic form:			
Business Continuity Strategy and plans for all activities			[within 2 hours]
Data stored on paper:			
Business Continuity Strategy and plans for all activities			immediately
IT and communications equipment:			
Workstations	[within 2 hours]	Workstations	[within 2 hours]
Telephones	immediately	Telephones	immediately
Mobile phones	immediately	Mobile phones	immediately
Printer	[within 2 hours]	Printer	[within 2 hours]
Fax machine	immediately	Fax machine	immediately
Communication channels:			
Telephone land lines			immediately

Internet access			[within 2 hours]
Other equipment:			
TV set	immediately	TV set	immediately
Radio	immediately	Radio	immediately
Facilities and infrastructure:			
Computer network	[within 2 hours]	Computer network	[within 2 hours]
Furniture	immediately	Furniture	immediately
External services:			
Electricity			immediately

Municipal Manager is responsible for preparing the Crisis Management Team and the Crisis Management Support Team for their role during a disruptive incident. Manager: ICT is responsible for equipping the Command Centre.

4.2. Reporting and decision making

Incidents are reported in the following way:

- all incidents related to IT and communications technology are reported to Manager: ICT
- all other incidents are reported to Crisis Manager

If the persons mentioned are unable to resolve the incident, they must inform the Crisis Manager who decides whether to activate recovery plans.

Authorisations for making decisions are the following:

Type of decision	***Who is authorised***
How small incidents related to IT and communications technology are resolved	Manager: ICT
How all other small incidents are resolved	Municipal Manager
Making a decision about activating recovery plans	Municipal Manager
Implementing all tasks necessary for the recovery of individual activities	Municipal Manager
Selecting information to be provided to the public media during disruptive incident	Municipal Manager
Purchases during disruptive incident - over [amount]	Municipal Manager
Purchases during disruptive incident - up to [amount]	Municipal Manager

ICT Manager is responsible for preparing employees in ICT Business Unit to recognise and react to incidents related to IT and communications technology. Municipal Manager is responsible for preparing employees in Molemole to handle other incidents.

4.3. Cooperation with authorities

The following persons are in charge of coordination with state authorities and emergency services:

Authority	*Who is in charge*
Police	Municipal Manager
Ambulance	Municipal Manager
Fire service	Municipal Manager
Any others	Municipal Manager

The mentioned persons must implement all preliminary activities to ensure interoperability with authorities during disruptive incident is at a satisfactory level. Preliminary activities may include obtaining instruction from authorities regarding the type of information required in the case of disruptive incident and how the organization is expected to react.

4.4. Building evacuation and assembly points

Each building is evacuated as specified in the building evacuation plan in the case of fire.

After evacuating the building employees must gather at the following assembly points:

	Assembly Point 1	*Assembly Point 2*
[address of location no. 1]		
[address of location no. 2]		
[address of location no. 3]		
[address of location no. 4]		

Note: if Assembly Point 1 is unavailable, employees must gather at Assembly Point 2.

Manager: HRM is responsible for preparing and maintaining evacuation plans in the case of fire.

4.5. Means of communication

The following means of communication will be used in the case of disruptive incident – those at the top of the list are to be used first, those near the bottom are used only if the former are out of order:

1. Mobile phones (business and private)
2. Telephones (business and private)
3. E-mail (sent from business or private computers)
4. [Messaging services - e.g. Skype]
5. Couriers (employees of the organisation or specialised services)
6. [Hand held stations - state where they are stored and who has the right to use them]

7. [Amateur radio stations - state where they are stored and who has the right to use them]

8. [Satellite phones - state where they are stored and who has a right to use them]

Senior Manager: Corporate Services and ICT Manager are responsible for acquiring/preparing and when necessary maintaining the mentioned means of communication to ensure they are available during a disruptive incident.

4.6. Transportation to alternative sites

Employees of the organisation will be transported from the primary to the alternative site in the following ways: Activity Means of transport

Crisis Management Team and Crisis Management Support Team by business car; by business transport [activity]

Senior Manager: Corporate Services is responsible for providing for all means of transportation.

4.7. Communicating with interested parties

Senior Manager: Strategic and Social Development will handle relations with interested parties by designating persons to communicate with them in the case of disruptive incident by the following means of communication:

	[Telephone]	*[Meetings]*	*[E-mail]*	*[Press conferences]*	*[Public media]*		
[Employees]							
[Owners / shareholders]							
[Employees' relatives]							
[Clients]							
[Public media]							
[Associations]							
[Emergency services]							
[various state authorities]							

Municipal Manager is responsible for preparing all the above-mentioned persons for communicating during disruptive incident.

Senior Manager: Strategic and Social Development is responsible for preparing templates for the media statements, which would cover all disruptive incidents related to the above-mentioned highest risks.

5. Resource Strategy

5.1. Sites and infrastructure

Recovery sites of Molemole are the following:

Name	*Primary site*	*Alternative Site Strategy*	*Min. number of workplaces*	Equipment*	*Alternative site – close*	*Alternative site – remote*

*Terms used in this column have the following meaning:

a) Cold – a site with no infrastructure or equipment

b) Warm – a site with pre-installed basic infrastructure (network, etc.), links and equipment for which the procurement periods are long

c) Hot – a site with pre-installed infrastructure, all equipment, links and software

D) Mirrored – a site with previously installed infrastructure, all equipment, links and software, and real time data

ICT Manager is responsible for making all necessary arrangements concerning the alternative site and is responsible for equipping alternative sites.

5.2. Suppliers and outsourcing partners

Relations with suppliers and outsourcing partners must be managed in the following way:

Name of supplier / outsourcing partner	*Strategy*
	a) encouraging, or forcing suppliers/outsourcing partners to raise their level of business continuity capability (this reduces the risk of an incident, and also reduces consequences) b) obliging the suppliers/outsourcing partners by contract to deliver the product or service regardless of the disruptive incident, and define penalties (in this way suppliers/outsourcing partners are obliged to introduce business continuity, and transferring a part of the financial risk to them)

Name of supplier / outsourcing partner Strategy

a) Encouraging, or forcing suppliers/outsourcing partners to raise their level of business continuity capability (this reduces the risk of an incident, and also reduces consequences)

b) Obliging the suppliers/outsourcing partners by contract to deliver the product or service regardless of the disruptive incident, and define penalties (in this way suppliers/outsourcing partners are obliged to introduce business continuity, and transferring a part of the financial risk to them)

ICT Manager is responsible for managing relations with suppliers and outsourcing partners to ensure interoperability during disruptive incident is at a satisfactory level.

5.3. Applications/databases

All the necessary applications and databases will be installed at the alternative site if they are required within 24 hours from disruptive incident; for those applications and databases which are not required within 24 hours, the installation media will be stored at the alternative site.

ICT Manager is responsible for application/database installation and/or for the preparation of installation media.

5.4. Data

Backup copies of data shared by several activities must be made at following intervals:

Name of application, database, folder, document:	***Frequency of creating backup copies***	***Backup procedure***
		[a) applications/databases - automated server-based backup procedure; b) electronic documents - storage in intranet folders for which backup copies are created automatically; c) paper documents - receiving all fax documents by electronic means, or scanning the documents, or copying them and storing at two separate locations]

Note: the frequency for creating backup copies of data used only by a single activity is defined in the strategy for the said activity.

ICT Manager is responsible for creating backup copies of the above-mentioned data.

5.5. Avoiding a single point of failure

The following strategies are used to avoid a single point of failure which can cause a disruption of an activity: Single point of failure Activity where it occurs Avoidance Strategy

ICT Manager is responsible for implementing the single point of failure avoidance strategy.

5.6. Providing Financial Resources

Molemole requires [amount in local currency] for working capital for all activities, plus [amount in local currency] for urgent purchases in case a disruptive incident occurs.

In case of a disruptive incident, financial resources will be provided in the following way: (a) an organization will continuously maintain the required level of liquidity in money; (b) a stand-by arrangement with [name of the financial institution] will be negotiated; (c) [name of the person] will provide private loan; or (d) [names of suppliers and outsourcing partners] will extend the payment terms.

Municipal Manager is responsible for making all necessary arrangements concerning provision of financial resources.

6. Recovery Strategy for Individual Activities

The recovery strategy for individual activities is defined in Appendices 6 to this Strategy.

The person specified as Recovery Manager for an individual activity is responsible for writing Recovery Plans for this activity. Municipal Manager is responsible for preparing all resources necessary for individual activities.

7. Implementing all necessary preparations

Appendix 5 lists all necessary preparations for the implementation of this Strategy. Municipal manager must define necessary financial and other resources, and set deadlines for the implementation of each preparation; Business Unit Director is in charge of monitoring coordination and execution of all preparatory actions, as well as of reporting about their implementation.

8. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
Preparation Plan for Business Continuity (in electronic form)	Computer of [job title responsible for monitoring execution]	[job title responsible for monitoring execution]	Only [job title] has the right to make entries and changes to Plan data.	The Plan is stored for the period of 3 years

9. Validity and document management

This document is valid as of [date].

The owner of this document is [job title], who must check and if necessary update the document at least twice a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- whether the organization succeeded in recovering activities within the recovery time objective
- whether all necessary preparations for business continuity have been implemented

This policy shall be reviewed after a period of three(3) years from the date of approval or should a need arise.

10. Appendices

- Appendix 1 - List of Activities
- Appendix 2 - Recovery Priorities for Activities
- Appendix 3 - Recovery Time Objectives for Activities
- Appendix 4 - Examples of Disruptive Incident Scenarios
- Appendix 5 - Preparation Plan for Business Continuity
- Appendix 6 - Activity Recovery Strategy for each Business Unit

Approved/ disapproved

Signature	
Initial and Surname	Cllr. M.E Paya
Designation	Mayor