SWELLENDAM MUNICIPALITY

BUSINESS CONTINUITY MANAGEMENT POLICY FRAMEWORK, 2019

APPROVED BY COUNCIL ON PER ITEM A83 ON 25 JULY 2019

SWELLENDAM MUNICIPALITY

BUSINESS CONTINUITY POLICY FRAMEWORK INDEX:

PART 1: Business Continuity Management Committee

1.1 Introduction

Business Continuity Management (BCM) requires a governance structure often in the form of a committee that will ensure senior management commitment and define senior managements‘ roles and responsibilities.

The BCM senior management committee is responsible for the oversight, initiation, planning, approval, testing and audit of the Business Continuity Plan (BCP). It also implements the BCP, coordinates activities, approves the Business Impact Analysis (BIA) survey, oversees the creation of continuity plans and reviews the results of quality assurance activities.

1.2 Responsibilities

A BCM Committee should:

- approve the governance structure;
- clarify their roles, and those of participants in the program;
- oversee the creation of a list of appropriate committees, working groups and teams to develop and execute the plan;
- provide strategic direction and communicate essential messages;
- approve the results of the BIA;
- review the critical services that have been identified;
- approve the continuity plans and arrangement;
- monitor quality assurance activities;
- resolve conflicting interests and priorities; and
- meet at least annually to review the business continuity plan.

1.3 Composition

The BCM Committee is comprised of the following members:

- Executive sponsor: Director: Corporate Services

The executive sponsor has overall responsibility for the BCP committee; elicits senior management's support and direction; and ensures that adequate funding is available for the BCP program.

The executive sponsor is also the chairperson of the BCM Committee.

- BCM Coordinator: Chief Risk Officer

The BCM Coordinator secures senior management's support; estimates funding requirements; develops BCM policy; coordinates and oversees the BIA process.

Ensures effective participant input; coordinates and oversees the development of plans and arrangements for business continuity; establishes working groups and teams and defines their responsibilities; coordinates appropriate training; and provides for regular review, testing and audit of the BCP.

The BCM Coordinator is also a co-chair of the BCM Committee.

- Security Officer: Chief: Traffic & Law Enforcement

The Security Officer works with the coordinator to ensure that all aspects of the BCP meet the Security, Disaster and Emergency requirements of the Municipality.

- Occupational Health and Safety (OHS) Officer: Senior Human Resource Practitioner: Labour Relations; OHS & Employee Wellness

The OHS Officer is responsible to coordinate all related OHS prescripts according to National legislation and guidelines in the event of the activation of the Business Continuity Plan and processes. Close working group between OHS and Security Officer.

- Chief Information Officer (CIO): Manager: Information Communication Technology (ICT)

The CIO cooperates closely with the BCM coordinator and IT specialists to plan for effective and harmonised continuity.

- Communication Officer: Senior Media & Communication Officer

The Communication Officer formalises communication structures, handles internal and external communication and ensure everyone is aware of the communication policy.

- Business unit representatives

Business unit representatives provide input and assist in performing and analysing the results of the business impact analysis.

1.4 Review and Approval

This Business Continuity Framework must be reviewed by the BCM committee annually and per recommendation of the Fraud & Risk Management Committee (FARMCO) and be approved by Council as and when material amendments are required.

PART 2: Business Impact Analysis (BIA)

2.1 Introduction

The purpose of the BIA is to identify the Municipality's mandate and critical services; rank the order of priority of services for continuous delivery or rapid recovery; and identify internal and external impacts of disruptions.

2.2 Steps for a BIA

2.2.1 Identify the mandate and critical aspects of the Municipality

This step determines what services must be delivered. Information can be obtained from the IDP Strategy of the Municipality and legal requirements for delivering specific services.
The following critical services have been identified by the BCM Committee:

Focus Area	Critical Services/ Functions	Sub-Services/ Functions
Infrastructure and Community Services	Water supply	Extraction / sourcing Treatment Distribution Maintenance of water supply infrastructure
	Electricity supply	Purchase of electricity Distribution of electricity Electrical support services
	Sewerage removal	Removal Treatment Maintenance of waste water infrastructure
	Solid waste removal	Collection Processing Disposal Maintenance of solid waste infrastructure
	Roads & storm water maintenance	Repair of roads Maintenance of roads Maintenance of sidewalks Repair of storm water systems Maintenance of storm water systems
Support Services	Finance	Payroll Asset management Insurance Supply chain management Revenue management Budgeting Accounting
	Information and Communication Technology (ICT)	ICT Support Services Disaster Recovery: Access to Key Business Systems for Updates/Queries Infrastructure: - Access to/Redeployment of computers - Servers - Server Room (Disaster Recovery Server) - Recovery Tape Repository - Network Infrastructure - Telephone Communications - Internet Capability - Email Capability
	Human Resources (HR)	Employee administration Recruitment and appointment

		Occupational health and safety Labour relations
	Legal Services	Legal representation Legal advice
Administrative services	Support buildings & structures	Offices Workshops Work sites Archives Inventory stores Parking lots
	Communication	Public relations Media relations Advice on statements and answers prepared by municipal officials or political office bearers
Oversight and Strategic Services	Council	Executive Mayor Executive Deputy Mayor Speaker Ward Councillors Proportional Councillors Mayoral Committee Portfolio Committees
	Top Management	Municipal Manager Directors
	Assurance Providers	Internal Audit
		Audit- & Performance Audit Committee

2.2.2 Identify risks to business continuity

Risks are identified in the BIA or in a full risk assessment. Mitigating risk is an ongoing process and should be performed even when the BCP is not activated.
For example, if the municipality requires electricity for service delivery, the risk of a short-term power outage can be mitigated by installing stand-by generators.
Another example would be if municipality relies on internal and external telecommunications to function effectively. Communications failures can be minimised by using alternate communications networks or installing redundant systems.
The following BIA (Risk Assessment) was conducted by the BCM Committee:

Business Impact Analysis (Risk Assessment)						
Scores above **8 - 10** should be classified as **critical** and requires an immediate **improvement of Internal Controls** Scores of **11 - 12** should be classified as **catastrophic** and requires immediate **Strategic Action Plans**		**Score:** **4. Very Likely** **3. Likely** **2. Unlikely** **1. Rare**	**Score:** **4. Monthly/weekly** **3. Every 1 - 2 years** **2. Every 2 - 5 years** **1. Every 5 - 10 years**	**Score:** **4. Major** **3. Serious** **2. Minor** **1. Negligible**		
Rank	**Threat**	**Probability**	**Frequency**	**Impact**	**Total Score**	
1	Ageing, Alien & Insufficient infrastructure	3	2	4	9	Critical

2	Vandalism / Protest Actions	4	3	3	10	Critical
3	Interruption of electricity supply	3	2	3	8	Critical
4	Ageing fleet	4	4	4	12	Catastrophic
5	No internet / network connectivity & Cyber Security	4	4	4	12	Catastrophic
6	Security of buildings and personnel	3	1	3	7	
7	Drought	3	2	3	8	Critical
8	Key personnel	3	4	3	10	Critical
9	Floods (seasonal)	1	1	4	6	
10	Fire (seasonal)	3	4	4	11	Catastrophic
11	Gale Winds	3	3	3	9	Critical

2.2.3 Prioritise Critical Services

Once the critical services are identified, they must be prioritised based on minimum acceptable delivery levels and the maximum period of time the service can be down before severe damage to the Municipality results.

To determine the ranking of critical services, information is required to determine impact of a disruption to service delivery, loss of revenue, additional expenses and intangible losses.

3. Business Continuity Plan Quality Assurance

Review of the BCP should assess the plan's accuracy, relevance and effectiveness. The review should also uncover which aspects of the BCP needs improvement.

Continuous evaluation of the BCP is essential to maintain its effectiveness. The evaluation can be performed by internal assurance providers (such as risk management or/and internal audit functions) or by an external assurance provider.

The BCP must be reviewed on the following occasions:

- Scheduled review

The BCP must be reviewed at least 365 days after the last review or changes.

- Changes in risks

The disruptions covered in the BCP are based on the risks identified in the BIA.

- Changes in critical services

The critical services identified during the BIA changes. Recovery operations in the BCP only exist for the critical services identified in the BIA.

- ❖ Changes in personnel or contact details

The BCP must be updated to include up to date personnel and contact details.

- ❖ Changes to the Municipality's organisational structure or operations

Changes to the Municipality's structure (e.g. directorates and departments) or operations (e.g. replacement of people with machinery) can make the BCP outdated and inadequate for business continuity purposes.

- ❖ After exercises and tests

The results of business continuity exercises and tests must be incorporated into the BCP if applicable.

3.1 Risk Management function

Risk management function should play an oversight role, as it is strategically located to challenge the reliability and how realistic is the business continuity framework of the municipality among other things.

3.2 Internal Audit Function

Internal audit function has to provide assurance on the accuracy and reliability of the information contained in the components of business continuity framework.

3.3 Assurance Coverage

Assurance concerns all aspects of the framework; it tests processes to ensure that information is complete, accurate and valid. It can be provided by either internal audit function, risk management function or/and external assurance providers.

PART 3:
Business Continuity Plan

1 Introduction

The purpose of this business continuity plan (BCP) is to prepare the Municipality in the event of extended service outages caused by factors beyond our control (e.g. natural disasters, man-made events) and to restore services to the widest extent possible in a minimum time frame. All Municipal departments are expected to implement preventive measures whenever possible to minimise operational failure and to recover as rapidly as possible when a failure occurs.

The plan identifies vulnerabilities and recommends necessary measures to prevent extended service outages. It is a plan that encompasses all Municipal systems, Departments and operation facilities.

2 Business Continuity Plan Objectives

- Serves as a guide for the Municipal recovery teams.
- References and points to the location of any information/plans that reside outside this document.
- Provides procedures and resources needed to assist in recovery.
- Identifies vendors and customers that must be notified in the event of a disaster.
- Assists in avoiding confusion experienced during a crisis by documenting, testing and reviewing recovery procedures.
- Identifies alternate sources for supplies, resources and locations.
- Documents storage, safeguarding and retrieval procedures for vital records.
- Key people (Team Leaders or Alternates) will be available following a disaster.
- This document and all vital records are stored in a secure offsite location to survive a disaster and be accessible immediately following the disaster.
- Each support organisation will have its own plan consisting of unique recovery procedures, critical resource information and procedures
- Apocalyptic disasters such as a nuclear war are beyond the scope of this plan.

3 Mitigating risks

Risks are identified in the business impact analysis (BIA) or in an enterprise risk assessment. Moderating risk is an ongoing process, and should be performed even when the BCP is not activated.

For example, if the Municipality requires electricity for ICT, the risk of a short term power outage can be mitigated by installing stand-by generators.

Risk	Cause of risk	Critical Services Impacted	Reason for mitigation	Mitigation strategy	Mitigating actions
Drought	Lack of rain Evaporation	Water supply	Ensure adequate water resources for continuous water supply.	Treatment	Water restrictions Boreholes Increase dams' capacity. Decrease rate of evaporation of dam water.
Ageing & Insufficient infrastructure	Inadequate maintenance Lack of funding.	Water supply Sewerage removal	Ensure continuous water supply and sewerage removal.	Treatment	Maintenance Apply for infrastructure grants. Replacement of infrastructure.
Interruption of electricity supply	Eskom's inability to meet demand. Ageing infrastructure	Electricity supply Water supply Sewerage removal Support services Oversight and strategic services	Ensure service delivery during blackouts.	Treatment	Electricity generators for office buildings. Reservoir levels kept high enough to provide water during periods of blackouts. Backup generators for sewerage pumps at locations prone to sewerage spills.
No internet/ network connectivity & Cyber Security	Limited internet connectivity options available due to Swellendam's location.	Technical/Community services Support services Oversight and strategic services	Ensure service delivery	Exploit Treatment Transfer	Use current internet connectivity more productively. Explore unconventional internet connectivity options. Appoint service provider to provide the required internet connectivity.
Security of buildings and personnel	Inadequate access control. Deterioration of buildings due to inadequate maintenance.	All municipal services delivered from the affected buildings.	Protect property, assets and personnel required for the delivery of municipal services.	Treatment Transfer	Access controls Security guards (municipal employees or private security) Alarms Maintenance Renovations
Key personnel	Scarce skills. No replacements available to take over from key personnel.	All municipal services dependent on key personnel.	Ensure service delivery can continue when key personnel are unavailable.	Treatment Transfer	Identify delegates and complete the process to approve delegations and the authority of delegates. Scarce skills retention measures. Career development of skilled employees. Insurance against death of key personnel.

Risk	Cause of risk	Critical Services Impacted	Reason for mitigation	Mitigation strategy	Mitigating actions
Ageing fleet	Old vehicles Inadequate maintenance	All municipal services dependent on old vehicles	Ensure service delivery can continue when vehicles are out of service.	Treatment	Maintenance Replacement plan for old vehicles.
Vandalism / Protest Actions	Inadequate security Sabotage Politics	All municipal services.	Protect municipal property and personnel required for service delivery.	Treatment Transfer	Security guards (municipal employees or private security) Community participation in municipal decision-making. Grievance channels Zero tolerance approach to damage to municipal property or attacks on municipal employees during protests.
Fire (Seasonal)	Lightning Arson Negligence	All municipal services dependent on infrastructure or assets that can be destroyed by a fire.	Ensure service delivery is not affected by fires or can resume within a day after a fire has been extinguished.	Exploit Treatment Transfer	Fire safety training Fire extinguishers Reliable and fast communication line with ODM Fire Department. Veld Fire Plan Fire and waterproof safes Safe storage of flammable materials. Use of fire retardant materials where possible. Insurance against fire damage.
Floods (Seasonal)	Heavy rain Inadequate maintenance of storm water system. Burst water pipes	All municipal services delivered from areas prone to flooding.	Ensure service delivery is not affected by flooding or can resume immediately after a flood subsided.	Treatment Transfer	Waterproof safes Electric equipment stored on top of elevated platforms (e.g. desks). Critical equipment stored on 2nd floors of buildings. Maintenance of storm water systems. Replacement of deteriorating water pipes. Installation of water management systems that can identify leaks. Flood barriers Insurance against water and flood damage.

4 Event Response

4.1 Background

Each risk event stemming from the risks identified in the BIA is addressed in the continuity plans contained in the BCP, in terms of the disruptions it causes to the Municipality's service delivery and business operations.
One risk event can be the cause of another risk event, for example a fire can destroy power lines, resulting in an interruption of the electricity supply.
Many risk events can also have the same impact, for example a flood, fire, protest action and vandalism can all result in damage to or destruction of assets.
Due to the abovementioned interrelatedness of risk events and risk event impacts, the continuity plans are designed for responses to a specific disruption event, for example destruction of water pumps, and not for responses to the impacts of a specific risk event, for example water pumps destroyed by fire.

4.2 Drought

The response to a drought requires long term planning, with the impact stretching over months or even years.
Normally only events with immediate disruptive impacts are covered by the BCP, but the drought impacts on the available water supply, which will eventually have an immediate effect of water the one day, no water the next day.

4.3 Infrastructure breakdowns due to old age

Ageing infrastructure and resulting breakdowns is a long term problem and not specifically covered by the BCP. Technical services' continuity plans cover any type of breakdown of infrastructure and not age related breakdowns.

4.4 Interruption of electricity supply

Interruptions in the electricity supply can either be caused by a lack of supply from Eskom, technical faults or external events affecting the distribution network. See the continuity plans for responses to interruptions in electricity supply.

4.5 Lack of internet / network connectivity

Due to Swellendam's rural location, fixed line internet connectivity options are limited, slow and unreliable.
Finding reliable, fast internet connectivity options are the responsibility of the ICT department and addressed in the ICT continuity plans.
A loss of internet connectivity affects all critical services and is addressed in the universal / general continuity plans.

4.6 Security compromises of buildings and personnel

Security compromises can consist of unauthorised entry to premises, buildings or rooms and crimes committed inside buildings like theft and robbery.
Security comprises of personnel include damage to or theft of personnel's personal belongings while on municipal premises or offsite while performing their municipal jobs,

assault on personnel while performing their municipal jobs or for being a municipal official and threats made against personnel, stemming from their work done as municipal officials.

Detailed security plans for the protection of buildings and personnel fall outside the scope of a BCP. It is the responsibility of municipal law enforcement and building administrators to develop and implement security measures to ensure the security of buildings and the personnel inside.

The protection of personnel while working outside municipal premises is the responsibility of municipal law enforcement and outside the scope of the BCP. Municipal law enforcement must, if necessary, implement security measures to protect personnel while performing their municipal jobs.

The South African Police Service (SAPS) has the responsibility to enforce the law, consisting of apprehending criminals and crime prevention, which should include the protection of municipal buildings and personnel from known criminals and planned attacks.
The consequences of security compromises of buildings, for example damage to, theft or destruction of assets, are covered by the BCP.

Security compromises of personnel results in personnel either being injured or killed in attacks or resigning due to the unsafe work environment. The loss of key personnel through injury, death or resignation is covered by the BCP.

4.7 Vehicle breakdowns due to old fleet

Ageing fleet and resulting breakdowns is a long term problem and not specifically covered by the BCP.
Breakdowns of any kind of technical services' vehicles are covered by the BCP.

4.8 Vandalism / Protest actions

It is the responsibility of the South African Police Service (SAPS) to enforce the law, which includes preventing vandalism, apprehending vandals, stopping unlawful protest actions and apprehending protestors who damaged property or attacked people during the protest.
Vandalism and protest actions result in damage or destruction of infrastructure, buildings, vehicles and other assets. The damage and destruction are covered by the continuity plans.
Detailed plans for the prevention of vandalism and control of protest actions fall outside the scope of the BCP. It is the responsibility of the SAPS and municipal officials to create plans to address vandalism and protest actions, including the protection of municipal property.

4.9 Fires

Each department has the responsibility for basic fire prevention and firefighting measures, like fire extinguishers and not storing flammable materials near ignition sources.
The basic fire prevention and firefighting measures will be assessed by the Occupational Health and Safety inspector and/or an inspector from the Fire Department.
Detailed and complex fire prevention and firefighting plans and measures are the responsibility of the Fire Department and Disaster Management, which will form part of their fire plans and are beyond the scope of the BCP.

Evacuation plans are the responsibility of each department's/building's safety officer. Evacuation plans should already be displayed and known by every municipal official, thus it will not be included in the BCP.
In the continuity plans, the disruptions caused by fires are dealt with as part of general groupings of disruptions (e.g. damage to / destruction of infrastructure) and individually (e.g. inaccessible roads due to fires).

4.10 Floods

Detailed and complex flood mitigation plans are the responsibility of Disaster Management and beyond the scope of the BCP.
In the continuity plans, the disruptions caused by floods are dealt with as part of general groupings of disruptions (e.g. damage to / destruction of infrastructure) and individually (e.g. flooding of sewerage system).

5 Universal / General continuity plans

Universal or general continuity plans cover disruptions related to the risks identified in the BIA that require the same type of response, regardless of the critical service impacted.
The universal or general continuity plans contain condensed responses and it is the responsibility of each department to create detailed plans and standard operating procedures to implement the responses contained in these continuity plans.
General responses to disruptions can be supplemented by additional or more detailed responses in the service specific continuity plans and should thus be read in conjunction with the responses listed in the service specific plans.

6 Business Continuity Teams

Proper response to a disruption for the Municipality requires teams to lead and support business continuity operations. Team members should be selected from trained and experienced personnel who are knowledgeable about their responsibilities.

The duties and responsibilities for each team must be defined, including the team members and authority structure, the specific team tasks, members' roles and responsibilities, creation of contact lists and identifying alternate members.

The business continuity teams consist of the following:

1) Emergency Management Team
2) Response & Recovery Co-ordinator
3) Business Continuity Teams

- Technical / Community Services Team
  - Water
  - Electricity
  - Sewerage
  - Solid Waste
  - Roads
  - Storm Water Systems
- Finance Team
- Information and Communication Technology Team
- Communication Team
- Occupational Health and Safety Team

- Disaster Management Team
- Fire & Rescue
- Disaster Management
- Traffic

6.1 Emergency Management Team (EMT)

The EMT is responsible for overall coordination of the business continuity effort, determining whether the BCP should be activated and communications with senior management.
The EMT's other responsibilities include:

- Evaluate which BCP actions should be invoked and activate the corresponding teams.
- Evaluate and assess damage assessment findings.
- Set restoration priority based on the damage assessment reports.
- Provide senior management with ongoing status information.
- Act as a communication channel to teams and major stakeholders.
- Work with suppliers and business continuity teams to develop a rebuild/repair schedule.

6.2 Response & Recovery Co-ordinator

The Response & Recovery Co-ordinator is responsible for the overall coordination of the recovery effort, establishment of the command centre and communications with the EMT.

The Response & Recovery Co-ordinator's other responsibilities include:

- Notify the business continuity teams.
- Gather damage assessment information and report it to EMT.
- Determine recovery needs.
- Establish command centre and related operations.
- Notify all Team Leaders and advise them to activate their plan(s) if applicable, based upon the disruption situation.
- If the BCP is not activated, take appropriate action to return to normal operation using regular staff.
- Determine whether suppliers or other teams are needed to assist with detailed damage assessments.
- Prepare post-disruption debriefing report.

6.3 Technical / Community Services Team

The Technical / Community Services Team is responsible for the response and recovery of services delivered to the community. The services are interdependent on one another to a certain extent and therefore a combined team will be best suited to restore the services as soon as possible.
The responsibilities of the Technical / Community Services team include the following:

1) Water

- Repair / Reconstruction of water infrastructure;
- Monitor water levels of reservoirs and coordinate refilling of reservoirs that are empty or nearly empty;
- Dispatch and coordinate water tankers to residents who are or will be without water for more than 24 hours;
- Ensure maintenance of water infrastructure;
- Ensure the fleet of water service vehicles are maintained;

- Review the controls in place to protect water infrastructure against vandalism and theft and ensure improvements are implemented where necessary;
- Ensure a fast and effective reporting mechanism for burst or leaking water pipes exist;
- Monitor water levels of dams and boreholes supplying Swellendam Municipality;
- Identify possible borehole sites for establishing boreholes during a water crisis;
- Identify key personnel in the water department and ensure continuity plans address key personnel adequately;
- Inform the Communication team about the timeframes for the restoration of water supply and the timetables of water tankers;

2) Electricity
- Repair / Reconstruction of electricity infrastructure;
- Review the controls in place to protect electricity infrastructure against vandalism and theft and ensure improvements are implemented where necessary;
- Ensure maintenance of electricity infrastructure;
- Ensure maintenance of electricity generators;
- Maintain a 7 day fuel supply for electricity generators;
- Procure electricity generators for infrastructure identified in the BCP;
- Dispatch and coordinate mobile electricity generators to infrastructure;
- Explore possible alternative electricity suppliers and self-generation;
- Inform the Communication Team about the timeframes for the restoration of electricity supply;

3) Sewerage
- Repair / Reconstruction of sewerage infrastructure;
- Ensure maintenance of sewerage infrastructure;
- Review the controls in place to protect sewerage infrastructure against vandalism and theft and ensure improvements are implemented where necessary;
- Monitoring of sewerage levels;
- Dispatch and coordinate sewerage tankers to drain areas that will spill;
- Clean-up of sewerage spills;
- Ensure a fast and effective reporting mechanism for burst or leaking sewerage pipes exist;

4) Solid Waste
- Ensure maintenance of fleet;
- Identify alternative routes and collection spots when usual routes are inaccessible;
- Create new collection schedules to suit the circumstances;
- Inform the Communication Team about alternative collection spots and adjusted collection schedules;

5) Roads
- Repair / Reconstruction of roads;
- Ensure maintenance of roads;
- Ensure an effective reporting mechanism for damaged roads exist;
- Monitor bitumen supply to proactively manage possible shortages;

6) Storm Water
- Repair / Reconstruction of storm water systems;
- Ensure maintenance of storm water systems;
- Ensure a fast and effective reporting mechanism for blocked or damaged storm water systems exist;

6.4 Finance Team

The Finance Team is responsible for recovery of the finance function and supporting business continuity.

The Finance Team's responsibilities regarding recovery of the finance function include:

- Ensure municipal employees are paid no later than 2 days after their payment date stipulated in their employment contracts;
- Ensure suppliers are paid no later than 2 days after the due date;
- Liaise with SARS if taxes and/or levies will not be paid over on time and arrange for extension of the payment date;
- Implement controls to prevent fraudulent transactions during downtime;
- Recovery of financial data and information in cooperation with the ICT Team;
- Ensure financial transactions are recorded in an appropriate and standardised system while the mSCOA portal is inaccessible;

The Finance Team's responsibilities regarding business continuity of the Municipality include:

- Help departments and directorates establish the necessary emergency procurement procedures in advance;
- Handle requests for emergency procurement;
- Perform cost-benefit analysis and probability calculations to determine which insurable events identified in the BIA should be covered by insurance;
- Continuously monitor the BIA and insurance policy to ensure adequate coverage;
- Calculate the costs mentioned in the BIA;

6.5 Information and Communication Technology Team (ICT Team)

The ICT Team is essential to the business continuity and recovery efforts. Their responsibilities' include:

- Backup of all important electronic data;
- Safekeeping of backups;
- Restore data after a disruption;
- Ensure the security of the Municipality's network against cyber intrusions and attacks;
- Restoration of network capabilities;
- Recover email system and functionality;
- Restore telephone functionality;
- Restoration of internet connectivity;
- Equip alternative sites with the necessary ICT infrastructure;

6.6 Communication Team

The Communication Team is responsible for communication to the Municipality's stakeholders the effects of the disruption on the Municipality's operations, the current recovery operations in progress, additional planned recovery operations, the estimated time before services are resumed at minimum levels and the estimated time before normal operations are resumed.

The Communication Team's responsibilities include:

- Communicating to employees if there wages/salaries will not be paid on time and the estimated pay date;
- Communicating to suppliers if they will not be paid on time and the estimated pay date;

- Informing the public when service delivery will be resumed;
- Media relations, including handling all media queries, forwarding questions to the appropriate municipal officials, reviewing answers to media questions from municipal officials before sending it, releasing continuous updates on the state and progress of recovery efforts and communicating information from other response and recovery teams to the public;

6.7 Occupational Health & Safety Team (OHS Team)

The OHS Team is responsible to oversee the safety of all municipal employees while they are performing municipal work and/or while they are at municipal premises.

The OHS Team's responsibilities for business continuity include:
- Inspect damaged buildings, vehicles and equipment for contraventions of the Occupational Health and Safety Act, Act 85 of 1993 (OHS Act), and unsafe conditions;
- Declare whether repaired buildings, vehicles and equipment are safe and meet the requirements of the OHS Act before municipal personnel move back in;
- Ensure alternative premises fulfil the requirements of the OHS Act;
- Ensure complete medical records are kept of all personnel and that backup copies are made of medical records;
- Assist municipal departments to create safe working environments and fulfil all requirements of the OHS Act;

6.8 Disaster Management Team

The Disaster Management Team's role is to prevent disasters from occurring where possible, decrease the likelihood and impact of unpreventable disasters and managing the fallout of disasters to enable the other business continuity teams to focus on returning the Municipality's operations to normal.

The Disaster Management Team's responsibilities for business continuity include:

1) Fire & Rescue
- Extinguish fires on municipal property;
- Evacuate municipal employees from burning or flooded buildings;
- Assist municipal departments to acquire adequate firefighting equipment and reduce fire risks;
- Salvage data, records and equipment from buildings, if it is safe to do so;

2) Disaster Management
- Perform disaster risk assessments on potential disasters, determining its potential impact and likelihood on the Municipality's services;
- Inform the BCP Committee of changes in the risk profile of disasters, to enable them to evaluate whether the business continuity plan addresses all relevant disaster scenarios;
- Assist departments with the creation of mitigation strategies for disasters;
- Ensure disaster relief funds received specifically for components of the business continuity plan, are allocated to the specific components;
- Include business continuity funding requirements in applications for disaster relief funds;
- Warn the EMT of approaching fires that could disrupt the operations of the Municipality and advise them on steps to take to prevent or mitigate a disaster;
- Warn the EMT of impending or current flooding that could disrupt the operations of the Municipality and advise them on steps to take to prevent or mitigate a disaster.

- Warn the EMT of any other known approaching event that can have disastrous consequences and advise them on steps to take to prevent or mitigate a disaster.

3) Traffic
- Regulate traffic to enable municipal service vehicles to get to their destinations to deliver or restore services;
- Regulate traffic to enable municipal officials to get to work at the main sites or at alternative sites;
- Regulate traffic to enable suppliers or couriers to deliver equipment and materials required to restore services;

7. General team member responsibilities

- Each team member must designate a team alternate backup.
- All team members must keep an updated calling list of their team members' work, home and cell phone numbers.
- All team members must keep the BCP for reference at home in case the disruption happens after normal work hours.
- All team members must familiarise themselves with the contents of the BCP.

8. Alternative Sites

Alternative sites must be identified where municipal services can be delivered from in case the primary sites are unavailable.

8.1 Identify the amount of alternative sites

Each function, department, directorate, the whole municipality or a combination of the aforementioned can have an alternative site.
The amount of alternative sites will be determined by cost and practicality considerations. Functions, departments and directorates whose operations overlap can share an alternative site. Functions or departments that have unique operations can have their own alternative sites.
To keep capital costs to a minimum, one alternative site for the whole municipality can be used.

8.2 Location of alternative sites

Alternative sites should be situated in areas where it will not simultaneously be affected by the same disruption as the primary site.
The location must also be accessible by municipal officials during disruptions.
For example, if the primary site is in a low lying area prone to flooding and surrounded by veld that can burn, the alternative site should be on top of a barren hill to prevent floodwater and fires from reaching it, but it must also be accessible by a road that cannot be flooded or surrounded by veld fire.

8.3 Requirements of alternative sites

The requirements of alternative sites will differ, depending on the function, department or directorate operating from the alternative site. The assets and materials at the alternative site must enable the function, department, directorate or municipality to resume critical services and start the process to return to normal operations.

The minimum requirements of alternative sites are the following:

- Access control to ensure the physical security of the site and staff.
- Backup electricity supply that can support the operations at the site for a one week period.
- Office furniture and supplies, including:
- Desks
- Chairs
- One week's supply of stationary.
- One week's supply of printing paper.
- One week's supply of printing ink.
- Information communication technology infrastructure, including:
- Power points
- Network points
- Wi-Fi
- Network hub and network infrastructure
- Landlines (telephone/facsimile)
- ISDN lines
- ADSL lines
- Satellite communications
- Radios
- Computers
- Computer Screens
- Printers
- Projectors
- Conference facilities, including conference calls and webcams
- One week's supply of portable water stored on site.
- Ablution facilities
- Sewerage storage for a period of one week.
- Refuse storage capacity for one week's accumulation.
- One week's supply of food stored on site.
- Kitchen
- Lounge/Relaxation area