A21/2011

121

# Information Communication Technology Disaster Management and Business Resumption Policy

## Purpose

The purpose of this policy is to ensure that Information Communication Technology(ICT) resources of Council are managed and protected against and during service interruptions, natural disasters, accidents and intentional acts.

This policy describes four levels of service availability and steps to resume business processes in the event of disasters and other incidents.

## Scope

This policy is subject to the Computer User Policy of Council and covers computer services and system managed by the Information Communication Technology department.

## Disaster Management Process

1. Identify that a disaster or event has taken place
2. Save data
3. Save hardware, software and facilities
4. Resume original state and restore data

## Definitions

For the purpose of this policy the following definitions will be used:

- *Natural disaster:*
  - Earthquake
  - Tornado
  - Flooding
  - Landslide
  - Volcanic eruption
  - Lightning
  - Smoke, dirt, dust
  - Sandstorm or blowing dust
  - Windstorm
  - Snow/ice storm

*Accidents:*

- Disclosure of confidential information
- Electrical disturbance
- Electrical interruption
- Spill of toxic chemical

*System failure:*

- Hardware failure
- Operator/user error
- Software error
- Telecommunications interruption

*Intentional acts:*

- Alteration of data
- Alteration of software
- Computer virus
- Bomb threat
- Disclosure of confidential information
- Employee sabotage
- External sabotage
- Terrorist activity
- Fraud
- Riot/civil disturbance
- Strike
- Theft
- Unauthorized use
- Vandalism

**Risk assessment of disasters, accidents, acts and failures**

The Information Communication Technology department will continuously monitor the current and future risks to the delivery of service and systems.

In the event of a perceived immanent disaster, accident, act or failure the Information Communication Technology department will implement the necessary steps to stop; or limit the impact of; such an event.

**Information Communication Technology services and systems that can be affected by a disaster or event:**

- Hardware availability
- Operating systems
- Local Area Network and Wide Area Network services
- Financial Applications
- Human Resource Applications
- In-house developed applications
- E-mail and Internet Service
- Firewall Service
- Office Application Service
- Website and Intranet Service
- Library system
- Back-up and restore service
- Printing service
- Databases
- Geographical Information Systems

**Levels of availability per service or system**

**Level One:**

- All services are available during operational business hours.
- Maintenance on the system is done after hours.

  I.e. a few users have unrelated issues that are dealt with individually

**Level Two:**

- All services are available during operational hours but limited intermittent unavailability exists.
- Maintenance, reconfiguration on the system is done in operational hours and can require the Information Communication Technology department to bring the system/service offline for limited period of time.

  I.e. groups of users have related issues that are dealt with globally

**Level Three:**

- Not all services are available and long periods of unavailability exist.

- Maintenance, procurement, reconfiguring on system will be done as a priority and can require the Information Communication Technology department to bring down the system for long periods of time.

  I.e. A whole department cannot work and infrastructure relevant to that department can be unavailable, functional activities for that department have stopped. Procurement of equipment might be needed.

Level Four:

- No services are available and unavailability will exist for extended period of time.

- Maintenance, procurement, reconfiguration and recovery will be done as a priority without handling any other situations.

  I.e. All departments cannot work; total infrastructure can be destroyed or unavailable. Procurement of equipment might be needed

## Determining availability levels

Availability levels will be determined and affected by the Information Communication Technology department as the disaster or event investigation unfolds.

## Backup and restore procedures

The restoring of data will be done in accordance with the backup and restoration procedure in Council.

## Escalation procedure for resolving unavailability

In the case of level one availability the relevant user will be informed of the problem and the problem will be dealt with operationally.

In the case of level two availability the group of people without a service will be informed of the problem and the problem will be dealt with operationally.

In the case of level three availability the affected departmental head will be informed of the problem and the problem will be dealt with at management level.

In the case of level four availability the Municipal Manager will be informed and all the departmental heads of the problem and the problem will be dealt with at executive management level.

## Storage of backup data and system configuration

The backup data and a complete system configuration manual are stored off-site in a fire proof safe.

The configuration manual and backup data will allow for a complete rebuild of the total system by an outside company in the event that the Information Communication Technology department and staff destroyed.

# Information Communication Technology Disaster Management and Business Resumption Policy

## Purpose

The purpose of this policy is to ensure that Information Communication Technology(ICT) resources of Council are managed and protected against and during service interruptions, natural disasters, accidents and intentional acts.

This policy describes four levels of service availability and steps to resume business processes in the event of disasters and other incidents.

## Scope

This policy is subject to the Computer User Policy of Council and covers computer services and system managed by the Information Communication Technology department.

## Disaster Management Process

1. Identify that a disaster or event has taken place
2. Save data
3. Save hardware, software and facilities
4. Resume original state and restore data

## Definitions

For the purpose of this policy the following definitions will be used:

- *Natural disaster:*
    - Earthquake
    - Tornado
    - Flooding
    - Landslide
    - Volcanic eruption
    - Lightning
    - Smoke, dirt, dust
    - Sandstorm or blowing dust
    - Windstorm
    - Snow/ice storm

*Accidents:*

- Disclosure of confidential information
- Electrical disturbance
- Electrical interruption
- Spill of toxic chemical

*System failure:*

- Hardware failure
- Operator/user error
- Software error
- Telecommunications interruption

*Intentional acts:*

- Alteration of data
- Alteration of software
- Computer virus
- Bomb threat
- Disclosure of confidential information
- Employee sabotage
- External sabotage
- Terrorist activity
- Fraud
- Riot/civil disturbance
- Strike
- Theft
- Unauthorized use
- Vandalism

**Risk assessment of disasters, accidents, acts and failures**

The Information Communication Technology department will continuously monitor the current and future risks to the delivery of service and systems.

In the event of a perceived immanent disaster, accident, act or failure the Information Communication Technology department will implement the necessary steps to stop; or limit the impact of; such an event.

**Information Communication Technology services and systems that can be affected by a disaster or event:**

- Hardware availability
- Operating systems
- Local Area Network and Wide Area Network services
- Financial Applications
- Human Resource Applications
- In-house developed applications
- E-mail and Internet Service
- Firewall Service
- Office Application Service
- Website and Intranet Service
- Library system
- Back-up and restore service
- Printing service
- Databases
- Geographical Information Systems

**Levels of availability per service or system**

**Level One:**

- All services are available during operational business hours.
- Maintenance on the system is done after hours.

I.e. a few users have unrelated issues that are dealt with individually

**Level Two:**

- All services are available during operational hours but limited intermittent unavailability exists.
- Maintenance, reconfiguration on the system is done in operational hours and can require the Information Communication Technology department to bring the system/service offline for limited period of time.

I.e. groups of users have related issues that are dealt with globally

**Level Three:**

- Not all services are available and long periods of unavailability exist.

- Maintenance, procurement, reconfiguring on system will be done as a priority and can require the Information Communication Technology department to bring down the system for long periods of time.

I.e. A whole department cannot work and infrastructure relevant to that department can be unavailable, functional activities for that department have stopped. Procurement of equipment might be needed.

**Level Four:**

- No services are available and unavailability will exist for extended period of time.
- Maintenance, procurement, reconfiguration and recovery will be done as a priority without handling any other situations.

I.e. All departments cannot work; total infrastructure can be destroyed or unavailable. Procurement of equipment might be needed

**Determining availability levels**

Availability levels will be determined and affected by the Information Communication Technology department as the disaster or event investigation unfolds.

**Backup and restore procedures**

The restoring of data will be done in accordance with the backup and restoration procedure in Council.

**Escalation procedure for resolving unavailability**

In the case of level one availability the relevant user will be informed of the problem and the problem will be dealt with operationally.

In the case of level two availability the group of people without a service will be informed of the problem and the problem will be dealt with operationally.

In the case of level three availability the affected departmental head will be informed of the problem and the problem will be dealt with at management level.

In the case of level four availability the Municipal Manager will be informed and all the departmental heads of the problem and the problem will be dealt with at executive management level.

**Storage of backup data and system configuration**

The backup data and a complete system configuration manual are stored off-site in a fire proof safe.

The configuration manual and backup data will allow for a complete rebuild of the total system by an outside company in the event that the Information Communication Technology department and staff destroyed.

# ABENG LOCAL MUNICIPALITY

MC78/2007

APPLICATION SYSTEMS ACQUISITION AND DEVELOPMENT AND MAINTENANCE POLICY (2/4) (AMICT) (P 23: ANNEXURES P 136 – 143)

1. PURPOSE

To submit to the Mayoral Committee the proposed Software Development Acquisition and Maintenance Policy.

IT WAS RESOLVED BY THE EXECUTIVE MAYOR (15 AUGUST 2007)

That the policy BE NOTED BUT SHOULD BE PROPERLY crafted to conform to standards requirements for drafting of policies.

TOGETHER SISONKE TESAME

# ATJHABENG LOCAL MUNICIPALITY'S APPLICATION SYSTEMS ACQUISION AND DEVELOPMENT POLICY

## Introduction

New application systems could be developed or acquired without due consideration of the associated information security risks, or the security controls required. As a consequence, the required controls could be implemented at a later stage, with a higher cost and amplified effort.

Matjhabeng ICT Department have recognised this threat and have therefore formulated this Application Systems, Acquisition, Development and Maintenance Policy in order to address the risks attached to this threat.

## 1 Scope

### 1.1 Purpose

The purpose of this policy is to ensure adequate security controls are built into new application systems or present in acquired systems.

Lack of a security policy to govern system development or maintenance activity could lead to new application systems being developed or acquired and eventually put into production without appropriate security controls. This could lead to a breach in confidentiality, reliability or availability of information and/or application systems.

### 1.2 Applicability

This policy applies to all Matjhabeng Local Municipality employees, including temporary staff, contractors, service providers, and consultants utilising the Municipality's information resources. It covers all system software that are stored in Matjhabeng Local Municipality's Data Networks, servers, personal computers and other storage devices, where these systems are under the jurisdiction and/or ownership of the Council.

## 2 Normative references

The following documents contain provisions that, through reference in the text, constitute requirements of this policy. At the time of publication, the editions indicated were valid. All standards and specifications are subject to revision, and parties to agreements based on this policy are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

| | | |
|---|---|---|
| Reference | : | Matjhabeng Local Municipality Information Security Policy |
| Reference | : | Change Control Policy |
| Reference | : | Logical Access Control Policy |
| Reference | : | Information Classification Policy (under development) |

## 3 Definitions and abbreviations

### 3.1 Definitions

#### 3.1.1 System

An application system is an ICT implementation of a business system or process.

#### 3.1.2 Production environment

The live environment that should not be updated.

#### 3.1.3 Development environment

A fixed area which is set aside for the development of software to avoid/minimise the possibility of conflict between an existing program and a new version.

#### 3.1.4 Test environment

A fixed area that is set aside for testing of software prior to moving the software into the production environment.

#### 3.1.5 Information resources

Information resources entails all data, information, software, application systems, hardware, people and processes involved with the storage, processing and output of information. This includes data networks, servers, PCs, storage media, printers, photo copiers, fax machines, telecommunication equipment, supporting equipment (projectors etc), back-up media and storage area networks.

## 4 Policy

**4.1 A system development methodology shall be adopted and used for any new application systems being developed, in accordance with the Application Systems, Acquisition, Development and Maintenance Policy.**

The system development methodology shall be used whenever new application systems are developed in house or when the development has been outsourced to contractors.

**4.2 The systems development process shall include a security risk analysis and specification of security requirements and controls.**

When developing a new application system, modifying an existing application system, or acquiring an application system, possible security risks and the corresponding controls required; shall be identified.

The security requirement analysis and specification should as a minimum:

- be carried out at an early stage of the system development process, in compliance with formal standards / procedures for risk analysis and using formal risk analysis methodologies,
- be reviewed at key stages of the system development process
- involve representatives of key areas, such as the 'owners' of the system under development, the project manager, an IT specialist, Information Security specialist, key user representatives and, for critical systems, an expert in risk analysis
- determine business risk (taking into account the criticality of the installation, the business impact of a loss of confidentiality, integrity or availability, key threats and vulnerabilities)
- take into account the full range of controls needed to keep risks within acceptable limits.

The results of the risk analysis should include a clear indication of key risks, an assessment of their potential business impact and recommendations for the actions required to reduce risk to an acceptable level.

The results (including any residual risk) should be documented, reviewed and agreed by the person in charge of the system under development, and communicated to the 'owners' of business processes supported by the system under development. Agreed actions should be implemented and a process established to ensure that this is done effectively.

Identified information security requirements for the system under development should be clearly defined in terms of scope, resources (including timing and costs) and roles / responsibilities. They should be documented and supported by an agreed process for handling changes to requirements. The specification should include requirements for:

- application system capacity, availability, continuity, flexibility, connectivity and compatibility;
- information processing, storage and transmission (including requirements for protecting integrity and confidentiality);
- arrangements needed to support the application system in the live environment;
- compliance with contractual, legal and regulatory obligations;
- access control arrangements, such as access by system users; and
- segregation of duties.

**4.3 Documentation pertaining to Systems, Acquisition, Development and maintenance security controls shall be retained.**

System documentation shall contain all security controls required by the application system, or environment in which the system is to be used.

**4.4 Information shall be protected in accordance with Reference : Information Classification policy.**

An assessment of security risks shall be carried out to determine whether data encryption is required for sensitive information (Reference Information Classification Policy)

**4.5 The production, test and development environment shall be segregated.**

In the event that the system or application under development has flaws, these may negatively effect the production environment if they are not segregated. A segregation of these environments shall aid in maintaining control over the confidentiality, integrity and availability of the production environment.

**4.6 The acquisition process of application systems from third parties shall take into account the security requirements and controls as per clause 4.2**

The acquisition process shall include the testing of acquired software.

**4.7 Security requirements and controls, as identified in 4.2, shall be tested as part of the system development-testing phase.**

Formal test scripts shall be drawn up based on the requirements analysis. A formal security-testing plan should be formulated and testing activities monitored against the plan. Testing results should be properly documented and decisions to go live on changes will be based on the success of those tests.

**4.8 Post-implementation reviews shall be conducted for new or significantly changed application systems**

Post-implementation reviews should cover:

- fulfilment of information security requirements;
- efficiency, effectiveness and cost of controls;
- scope for improvements of controls; and
- Review of security incidents.

**4.9 Data used for testing purposes shall be protected and controlled in accordance with the Information Classification policy.**

Operational data that is simulated for the purposes of testing shall be subject to normal access control procedures. Simulation of this data shall only be permitted with appropriate authorisation and the use of this information shall be logged. Test data shall be removed when no longer required.

**4.10 Access to program source libraries shall be controlled in accordance with Reference: Logical Access Control Policy.**

**4.11 Access to the development and test environment shall be controlled in accordance Reference : Logical Access Control Policy.**

**4.12 Any changes to application systems shall be in accordance with the Municipality's Reference: Change Control Policy.**

**4.13 End user computing**

**4.13.1 Critical end-user developed applications e.g. spreadsheets, databases and ad-hoc reports, in accordance with Reference: Physical Asset Classification and Control Policy, developed for use in an operational environment, shall adhere to the following Information Security requirements:**

- Confidentiality – i.e. ensuring that information is accessible only to those authorised to have access.
- Integrity – i.e. safeguarding the accuracy and completeness of information and its associated processing methods.
- Availability – i.e. ensuring that authorised users will have access to information and associated processing systems when required.

Examples of controls are:

- All databases and ad-hoc reports shall be labelled to show name, author, date and time of creation, location of file, and an indication of the reliance that can be placed on the contents.
- All databases and ad-hoc reports shall be designed to include controls to assist integrity checking.
- All databases and ad-hoc reports shall be independently tested (e.g. tested by someone other than the author).
- Audit and test programs designed for this purpose shall be used to assist the testing process.
- Access to databases and ad-hoc reports shall be in accordance with Reference: Logical Access Control policy.

- Databases and ad-hoc reports that are used on a regular basis shall be held in a protected and controlled library where accidental and malicious changes cannot be made. (Reference Change Control Policy)
- The purpose, source of information and explanations of complex calculations in databases and ad-hoc reports shall be documented.
- Documentation shall include the purpose of the output, source of information, and explanations of complex calculations. Documentation should be to a level that is easy for a non-programmer to understand.

## 5 Roles and Responsibilities

| ROLE | FUNCTIONAL RESPONSIBILITIES |
|---|---|
| Director | • The Director shall ensure that the necessary information security controls are implemented and complied with as per this corporate policy. |
| Manager | • Establish and revise the corporate information security strategy, and policy for Systems, Acquisition, Development and maintenance with input from all stakeholders.<br>• Establish Systems, Acquisition, Development and maintenance process between the Municipality, and the service providers.<br>• Evaluate systems for development or change, and potential risks to the Municipality and introduce counter measures to address these risks.<br>• Report and evaluate changes to Systems, Acquisition, Development and maintenance policies and standards.<br>• Co-ordinate the overall communication and awareness strategy for Systems, Acquisition, Development and maintenance.<br>• Establish, implement, maintain and update the group strategy, architecture, standards and procedures for Systems, Acquisition, Development and maintenance with input from all stakeholders.<br>• Approve and authorise Systems, Acquisition, Development and maintenance measures on behalf of the group.<br>• Co-ordinate the overall communication and awareness strategy for Systems, Acquisition, Development and maintenance.<br>• Reviewing the effectiveness of the Municipality's Systems, Acquisition, Development and maintenance strategy and implemented security controls. |

| | |
|---|---|
| | • Evaluate and recommend changes to Systems, Acquisition, Development and maintenance.<br>• Responsible for approving, authorising, monitoring and enforcing Systems, Acquisition, Development and maintenance security controls within a division.<br>• Approve and authorise Systems, Acquisition, Development and maintenance budgets and evaluations for a division, where this accountability has been allocated to divisions.<br>• Ensure that all computer users are aware of policies, standards, procedures and guidelines for Systems, Acquisition, Development and maintenance at divisional level.<br>• Ensure the compliance of this policy.<br>• Co-ordinate the overall communication and awareness strategy for Systems, Acquisition, Development and maintenance.<br>• Report and evaluate changes to Systems, Acquisition, Development and maintenance policies and standards.<br>• Co-ordinate the implementation of new or additional security controls for Systems, Acquisition, Development and maintenance.<br>• Co-ordinate technical issues with the service provider. |
| Chief Computer Systems | • Establish a software development and maintenance process between the Municipality, and the service providers.<br>• Establish and revise the corporate information systems architecture strategy, and policy for system development and maintenance with input from groups and subsidiaries.<br>• Facilitate and co-ordinate the necessary counter measures to software development and maintenance incidents with groups and the service provider;<br>• Report and evaluate changes to software development and maintenance policies and standards.<br>• Co-ordinate the overall communication and awareness strategy for software development and maintenance.<br>• Establish and co-ordinate an appropriate team to facilitate organisation-wide emergency response in the event of a software development and maintenance incident. |
| IT Service Provider/ System Analysts and Programmers | • Implement and maintain Systems, Acquisition, Development and maintenance for the |

| | |
|---|---|
| | Municipality as indicated in the corporate strategy, architecture, policy, procedures and standards. |
| Computer User | • Shall comply with all information security policies, standards and procedures for Systems, Acquisition, Development and maintenance. |