A21/2004

PROPOSED INFORMATION COMMUNICATION TECHNOLOGY DISASTER MANAGEMENT AND BUSINESS RESUMPTION POLICY (2/4) (MICT)

PURPOSE OF REPORT

To propose to Council the adoption of the abovementioned policy.

INTRODUCTION AND BACKGROUND

The acceptance that disasters or events can take place requires a managed approach. The risks involved in the operations of the ICT department must be investigated continuously and formally addressed. The proposed policy recognizes these risks and defines a procedure of risk assessment and escalation.

*** Attached please find proposed policy on page **16** to **20** of the annexures.

PROBLEM STATEMENT

No ICT *Disaster Management Policy* exists.

POLICY POSITION

None

COMMENTS: HEADS OF DEPARTMENTS

MUNICIPAL MANAGER

Policy in order

RECOMMENDATIONS:

It is **recommended** that:

1) the proposed policy be adopted.

THE MANAGEMENT COMMITTEE RESOLVED (1 DECEMBER 2003)

That the proposed policy **BE ADOPTED.**

IT WAS RESOLVED BY THE MAYORAL COMMITTEE TO RECOMMEND (18 FEBRUARY 2004)

[MICT] That the proposed policy **BE ADOPTED.**

FOR CONSIDERATION

IT WAS RESOLVED (24 FEBRUARY 2004)

[MICT]

1. That the proposed policy **BE ACCEPTED** as a draft and **BE CIRCULATED** for inputs and interrogation.
2. That the draft policy on Information Communication Technology Disaster Management and Business Resumption **BE TABLED** at the next Council meeting to be held on 30 March 2004 for **ADOPTION.**

FOR CONSIDERATION

A21/2004

PROPOSED INFORMATION COMMUNICATION TECHNOLOGY DISASTER MANAGEMENT AND BUSINESS RESUMPTION POLICY (2/4) (MICT) (P 4: ANNEXURES P 16 – 20)

IT WAS RESOLVED (6 APRIL 2004)

[MITC] That the proposed information communication technology disaster management and business resumption policy **BE ADOPTED.**

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.