EDEN

DISTRICT MUNICIPALITY
UMASIPALA WESITHILI
DISTRIKSMUNISIPALITEIT

ICT DISASTER RECOVERY MANAGEMENT POLICY

Council Approved: 05/12/2017

Council Resolution Nr: C.5

1. INTRODUCTION

The latest auditor-general report (on National Audit Outcomes) cited the lack of adequate IT systems across government as a key obstacle to service delivery.

Failings highlighted include:

- a lack of IT service continuity planning
- inadequate controls in terms of user-access management
- insufficient security management systems
- a general lack of IT governance compliance

The responsibility for ensuring ICT organizational disaster recovery resilience does not rest solely with executive or senior management. As recognized good management practice it is also the responsibility of every member of staff. It is therefore essential that all members of staff familiarize themselves with this policy and any resultant accountabilities, responsibilities and authorities relevant to their role via the organization's ICT Disaster Recovery Management Strategy and their own Disaster Recovery Plan (DRP).

2. SCOPE

The purpose of this policy document is to clearly define and document the ICT Disaster Recovery Management (DRM) Policy for Eden District Municipality.

2.1 Applicability

This policy is applicable to:

- All business divisions, support units, branch offices of Eden District Municipality
- All subsidiaries of Eden District Municipality

2.2 Policy Aim

The purpose of having a *ICT Disaster Recovery Policy* is to make sure that organisations are protected against service interruptions, including large scale disasters, by the development, implementation, and testing of disaster recovery/business resumption (DR/BR) plans.

The three main aims of such a policy is to:

- Save data, hardware, software and facilities
- Resume critical processes and restore data
- To provide Eden District Municipality with ICT operational disaster recovery resilience through an effective and efficient ICT Disaster Recovery Management Programme that is consistent with the ISO/IEC 27002 Certification Requirements.

2.3 Policy Objectives

In order to achieve the aim stated above, this policy must achieve the following objectives:

- To help the organisation identify the IT resources that are at risk.
- The safety of all municipality staff, customers, clients and contractors.
- The protection of the assets of Eden District Municipality.
- To minimize financial and non-financial impact and losses.
- To maintain high levels of customer/client service.
- To maximize the defence of the reputation and brand image of Eden District Municipality.
- To ensure that ICT Disaster Recovery Management is conducted on an end-to end product and/or service basis.
- To ensure that all business divisions, business areas/units and corporate services, implement appropriate levels of disaster recovery to allow Mission (Business) Critical Activities to continue following disruption, interruption or loss.
- To ensure that external and internal suppliers of products and services are able to continue to provide an agreed level of service and/or supply of products should they themselves suffer a crisis or disaster incident.
- To ensure that all ICT Disaster Recovery Plans, ICT Disaster Recovery Solutions and Teams are implemented, exercised, tested, rehearsed and proven 'fit for purpose' at a frequency commensurate to the risk and criticality of the business activities.
- To allow the Council and senior management of the municipality to discharge their accountabilities, responsibilities and satisfy their corporate governance, legal and regulatory obligations.
- To ensure that Disaster Recovery Management is standardised.

3. ICT DISASTER RECOVERY MANAGEMENT POLICY STATEMENT

It is corporate policy that Eden District Municipality will:

- Ensure that an effective fit-for-purpose and up-to-date ICT Disaster Recovery Management competence and capability exists that is consistent with ISO/IEC 27002 Certification Requirements.
- Ensure that external and/or internal suppliers providing critical services and/or products are required through contractual terms and conditions and service level agreement(s) to have a DRM capability that ensures a continuous level of service and/or supply of products that is acceptable to the municipality in the event of the supplier(s) suffering a disaster recovery disruption, interruption or loss.
- Retain the right via contract terms and conditions and/or service level agreements to audit via due diligence the Disaster Recovery capability of internal and external service and/or product providers.
- Comply with the ICT Disaster Recovery Management Strategy of Eden District Municipality. Ensure that the appropriate knowledge, skills, expertise and resources are made available to enable the effective and efficient implementation and maintenance of ICT Disaster Recovery Management.
- Ensure that any legal proceedings/actions/investigations/inquiries/ enquiries following a Disaster Recovery invocation are under the supervision of the Municipality's legal department.

- Ensure that all ICT DR plans and solutions are developed to a detail and scope appropriate to the findings of a formal Business Impact Analysis (BIA).
- Provide adequate resources (including finance) to enable and maintain an effective ICT DRM competence and capability.
- Ensure that any media or public relations enquiries/activities during or following a DR situation are under the direct supervision of the Executive Manager Support Services.
- Ensure that the change management process shall consider the implications of any business process or other change and its impact on DRM.
- Assist Manager Human Resources in providing ICT DRM awareness and training for all relevant staff.
- All implemented ICT DR Plans should be tested at least bi-annually.
- Maintenance on the documented plans and backup and recovery procedures must be done as and when any changes occur or are implemented within the primary ICT environment.
- All changes and amendments or implementations happening at the primary site, must be maintained accordingly at the DR site.

4. POLICY PRINCIPLES

- Information and Communications Disaster Recovery Management (ICT DRM) is an integral part of the corporate governance responsibilities of the Eden District Municipality and is undertaken as it adds value in addition to governance or regulatory considerations
- ICT DRM will be treated as a management owned and driven process
- ICT DRM activities will match and focus upon and directly support the business strategy and goals of the organisation
- ICT DRM will provide resilience within the municipality to protect and optimise product and service availability
- ICT DRM will be based on a holistic managed DRM programme approach rather than just DR Planning
- As a value based management process, ICT DRM will optimise cost efficiencies
- Each business division and site of Eden District Municipality is accountable and responsible for managing their own business risk. The management of the business risk should be based upon the individual risk appetite of that business unit of the organisation and clearly reflect the risk appetite of the organisation as a whole.
- Eden District Municipality and its business units shall recognise and acknowledge that the reputation, brand image, market share and shareholder value risk cannot be transferred or removed by internal and/or external sourcing.
- All ICT DR Strategies, plans and solutions will be based upon the Municipality's Business Critical Activities identified by a formal Business Impact Analysis (BIA).
- All Business Impact Analysis and Risk Assessments will be focused upon municipal products and services in an end-to-end production context.
- An approved policy, for ICT DR should be published and distributed throughout the organisation.

5. RESPONSIBILITY FOR COMPLIANCE

The ICT Manager is accountable for ensuring the governance, implementation and compliance monitoring and provision of management information concerning this policy.

6. ISO/IEC 27002 CERTIFICATION REQUIREMENTS

ISO/IEC 27002 specifies that Service Continuity requirements shall be:

- Identified on the basis of business plans, service level agreements and risk assessments
- Developed and reviewed at least annually
- Maintained to ensure that changes agreed by the business are reflected
- Verified and plans tested at every major change to the business environment
- Considered during the Change Management process by evaluating the impact of any change on the service continuity plans. (ICT Steering Committee minutes (if available or applicable) must reflect representation by Business and Service Continuity functions)
- ISO/IEC 27002 provides suggested good practice for ensuring that Service Continuity requirements are addressed properly.

ANNEX A: ABBREVIATIONS AND DEFINITIONS

A.1 Abbreviations

BCM	Business Continuity Management
BIA	Business Impact Analysis
ISO	International Organisation for Standardisation
IEC	International Electro technical commission
DRM	Disaster Recovery Management
DRP	Disaster Recovery Plan
ICT	Information and Communications Technology
MCA	Mission-Critical Activity
RA	Risk Assessment

A.2 Definitions

Term	Definition
Disaster Recovery Management (DRM)	A holistic management process incorporating processes, policies and procedures related to preparing for recovery or continuation of *technology infrastructure* critical to an organization after a natural or human-induced disaster. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication and reputation protection, and should refer to the disaster recovery plan (DRP) for IT related infrastructure recovery /continuity.
Business Situation	An incident or occurrence and/or perception which threatens the operations, staff, shareholder value, stakeholders, brand, reputation and/or strategic/business goals of an organisation.
Mission (Business) Critical Activity (MCA)	A critical operation and/or business support activity (ies) (either provided internally and/or outsourced) without which the organisation would quickly be unable to achieve its business objective(s) i.e. provision and/or supply of services and/or products.