|  |
| --- |
|  |
| Kareeberg Municipality |
| IT Disaster Recovery Plan |

|  |
| --- |
|  |

Table of Contents

[1. INTRODUCTION 2](#_Toc421628954)

[2. POLICY OBJECTIVE 2](#_Toc421628955)

[3. IT ENVIRONMENT 2](#_Toc421628956)

[4. CRITICAL APPLICATIONS 2](#_Toc421628957)

[5. BACKUPS 2](#_Toc421628958)

[6. RESPONSIBILITY 3](#_Toc421628959)

[7. MAINTENANCE 3](#_Toc421628960)

[8. USAGE GUIDELINES 3](#_Toc421628961)

# INTRODUCTION

The objective of this document is to provide Kareeberg Municipality (“KM”) with a clearly defined, documented course of action to implement and maintain KM’s Information Technology disaster recovery strategy.

# POLICY OBJECTIVE

The procedures set out within the Information Technology Disaster Recovery Plan (IT DRP) are aimed at enabling KM to resume or continue normal processing of critical IT applications and systems. Throughout the business recovery effort, this plan establishes clear modus operandi and priorities work efforts.

Specifically, the objectives of the IT DPR are to:

* Minimise the duration of a serious disruption to business operations;
* Facilitate effective co-ordination of recovery tasks;
* Reduce the complexity of the recovery effort; and
* Align recovery efforts with recovery requirements from the perspective departments within each department.

# CRITICAL APPLICATIONS

The following applications were identified as critical (i.e. the relevant business departments cannot continue operations without these systems):

* AfriRaad Financial System;
* Microsoft Office (Excel)
* Email
* Prepaid Electricity Vending (Conlog System)
* Telephony system;
* System networking (including switching equipment)
* eNatis
* ADSL and dial-up lines
* VIP

In addition, an external disk backup is necessary to contain these critical applications.

Further detail on the criticality of systems per department and directorate are listed in **Appendix A.**

# BACKUPS

The application and system backup procedures for Kareeberg Municipality is contained within the Backup Strategy. The IT DRP should be read in conjunction with the Backup Strategy to understand the full extent of the backups maintained and how this relates to the IT DRP.

Refer **Backup Strategy** for further information.

# RESPONSIBILITY

The Chief Financial Officer (CFO) is responsible for defining and maintaining the policy framework for Business Continuity Management and supporting practices, which includes the IT DRP. The CFO is also responsible for initiating IT disaster recovery tests and reviews.

# MAINTENANCE

An effective IT DRP is a *live* recovery plan. The plan must be maintained current and tested/exercised regularly.

The CFO will ensure that the IT DRP is reviewed annually or sooner as required.

Maintenance of the plan is critical to the success of the actual recovery. The plans must reflect changes to the environments that are supported by he plans. It is critical that existing change management processes are revised or updated to take IT DRP and BCP maintenance into account. The plan must be reviewed for possible updating after every major operational of system change that will have a material effect on the recovery strategy of any service provided.

# USAGE GUIDELINES

This plan should be read in conjunction with the **Business Continuity Plan** of Kareeberg Municipality, as well as the **Business Continuity Management Policy Framework.**

**Accepted Council meeting: 20 Junie 2017**