Remote Access Policy

TABLE OF CONTENTS

1. INTRODUCTION

Information security is becoming increasingly important to the Municipality, driven in part by changes in the regulatory environment and advances in technology. Information security ensures that ICT systems, data and infrastructure are protected from risks such as unauthorised access, manipulation, destruction or loss of data, as well as unauthorised disclosure or incorrect processing of data.

2. LEGISLATIVE FRAMEWORK

The policy was developed with the legislative environment in mind, as well as to leverage internationally recognised ICT standards.

The following legislation, amongst others, were considered in the drafting of this policy:

- Constitution of the Republic of South Africa Act, Act No. 108 of 1996;
- Copyright Act, Act No. 98 of 1978;
- Electronic Communications and Transactions Act, Act No. 25 of 2002;
- Minimum Information Security Standards, as approved by Cabinet in 1996;
- Municipal Finance Management Act, Act No. 56 of 2003;
- Municipal Structures Act, Act No. 117 of 1998;
- Municipal Systems Act, Act No. 32, of 2000;
- National Archives and Record Service of South Africa Act, Act No. 43 of 1996;
- Promotion of Access to Information Act, Act No. 2 of 2000;
- Protection of Personal Information Act, Act No. 4 of 2013;
- Regulation of Interception of Communications Act, Act No. 70 of 2002; and
- Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.

The following internationally recognised ICT standards were leveraged in the development of this policy:

- Western Cape Municipal Information and Communication Technology Governance Policy Framework, 2014;
- Control Objectives for Information Technology (COBIT) 5, 2012;
- ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls; and
- King Code of Governance Principles, 2009.

3. OBJECTIVE OF THE POLICY

The purpose of this policy is to define requirements for connecting to Bergrivier Municipality's network from an outside entity. These requirements are designed to minimize the potential exposure to Bergrivier Municipality's network from damages which may result from unauthorized use of its resources. Damages include the loss of sensitive or confidential information, damage to public image and damage to critical DoIT internal systems..

4. AIM OF THE POLICY

The aim of this policy is to ensure that the Municipality conforms to standard remote access management controls in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, service efficiency and that risks associated to the management of user access are mitigated. This policy supports the Municipality's Corporate Governance of ICT Policy.

5. SCOPE

This policy applies to all the Municipality's employees, contractors, vendors and agents with a Municipal or personally-owned computer used to connect to the Municipality's network. This policy applies to remote access connections used to perform work by service providers.

6. BREACH OF POLICY

Any failure to comply with the rules and standards set out herein will be regarded as misconduct and/or breach of contract. All misconduct and/or breach of contract will be assessed by the Municipality and evaluated on its level of severity. Appropriate disciplinary action or punitive recourse will be instituted against any user who contravenes this policy. Actions include, but are not limited to:

- Revocation of access to Municipal systems and ICT services;
- Disciplinary action in accordance with the Municipal policy;
- Civil or criminal penalties e.g. violations of the Copyright Act, Act No. 98 of 1978; or
- Punitive recourse against the service provider/vendor as stated in the service provider/vendor's SLA with the Municipality.

7. ADMINISTRATION OF POLICY

The Head IT & Archives and Application owners within the municipality is responsible for maintaining this policy. The policy must be reviewed by the ICT Steering Committee on an annual basis and recommended changes must be approved by Council

8. DELEGATION OF RESPONSIBILITY

In accordance with the ICT Governance Policy, it is the responsibility of the Municipal Manager to determine the delegation of authority, personnel responsibilities and accountability to Management with regards to the Corporate Governance of ICT.

9. CONDITIONS TO CONNECT TO COUNCIL'S INTERNAL COMPUTER NETWORK

9.1 Remote access must be strictly controlled by the use of unique user credentials.

9.2 All remote access connections that utilize a shared infrastructure, such as the Internet, must utilize some form of encryption.

9.3 A remote access log must be maintained, a request (Annexure: A) must be submitted to IT for remote access. (Form contains comprehensive detail not in first policy)

9.3.1 Any deviations to be approved by the Municipal Manager in conjunction with relevant Director.

Annexure: A: Remote Access Request Form

Part I: Request

Requestor / User

Last Name _____ First Name_____ Date _____

Company Name_____ Phone _____

Company representative name _____

Name of Application/ Database: _____

Describe Purpose of Remote Access _____

_____

Describe resources needed (Network Drives, Printers, etc.)_____

_____

Access start Date: _____ End Date: _____

Access start time:_____ End time: _____

Municipal Sponsor

Municipal Sponsor can be a Manager or Director of the department requiring the non-employee remote access.

Last Name _____First Name _____Date _____

Department _____ Phone _____

Provided application or database login details: Yes/No

Authorizing Signature _____ Title _____

Technical Sponsor

Technical Sponsor is the IT Department

Approved/ Denied/ Date Created: _____

Last Name _____First Name _____Date _____

Application or protocol used:_____

Authorizing _____ Title _____

Process reviewed by Head IT & A: Yes/No

Date: _____ Signature: _____