# BERGRIVIER MUNICIPALITY

# POLICY FOR THE USE OF IMIS

**DATE APPROVED** : BK4117 – 18/06/2013

**COMMITTEE** : MAYORAL COMMITTEE

# BERGRIVIER MUNICIPALITY

# POLICY FOR THE USE OF THE INTEGRATED MANAGEMENT INFORMATION SYSTEM - IMIS

APPROVED COUNCIL RESOLUTION 4117
DATED 18 JUNE 2013

| DOCUMENT NUMBER | REVISION | REVISION DATE | ISSUE LEVEL | PAGE |
|---|---|---|---|---|
| | | | | 1 of 5 |

The purpose of this policy is to outline the acceptable use of the IMIS system within the application of the Organisation. These rules are in place to protect the organisation, its staff and interns. Inappropriate use exposes the organisation to risks including virus attacks, compromise of network systems and services, legal issues and confidentiality requirement.

The use of the IMIS system in connection with business activities and minimal personal use is a privilege extended to various members in good standing of the organisations community; it is not a right. Users of IMIS system are required to comply with this Policy. By using these resources, all users are also subject to, and required to comply with, Bergrivier Municipality ICT policies, Password Policy, and other policies that apply to their specific role with the organisation. Users also agree to comply with all applicable laws and to refrain from engaging in any activity that is inconsistent with the organisation status or would subject the organisation to liability. It is the user's responsibility to find out which policies exist and are applicable to them.

This policy applies to all staff members and interns of the Organisation who make use of the IMIS system.

**Objective**

To provide guidelines and a set of rules for the use of the IMIS system by employees of the Organisation and to support continuing conduct of business and better service delivery.

These resources must be used responsibly by everyone, since misuse by even an individual has the potential to disrupt business or the work of others. Users are required to exercise responsible, ethical behaviour when using the IMIS system.

Acceptable use of IMIS electronic communication resources demonstrates respect for unobstructed access, intellectual property rights including copyright, trademark, and applicable licenses, truth in communication, ownership of data, system security and integrity, and individuals' rights. Acceptable use includes, but is not limited to, respecting the rights of other users, sustaining the integrity of systems and related physical resources, and complying with all relevant policies, laws, regulations, and contractual obligations.

System Administrators and IT Support Staff must also comply with the IT Policy and sign the organisation Confidentiality Statement.

The organisation reserves the right to amend this Policy at any time without prior notice and to take such further actions as may be necessary or appropriate to comply with applicable laws.

**Legislative requirements**

The organisation is committed to protecting interns, staff, suppliers, and guests from illegal or damaging actions by individuals, either knowingly or unknowingly. This Policy was written to support and protect IMIS resources, and all users of those resources, by defining the Standards for Acceptable Use.

**Standards of Acceptable Use**

Use of IMIS electronic communication resources requires each user to adhere to the following standards of acceptable use:

- Observe all laws, as well as policies of Organisation in the use of IMIS resources.
- Do not use the IMIS resources for any unlawful purpose, such as the distribution of fraudulently or illegally obtained software. The organisation may take any immediate steps necessary to deal with alleged violations of law or policy, including removing illegal material from the IMIS server or other municipal computing or electronic communication resources, and organisation reserves the right to lodge criminal proceedings against the offender if deemed necessary.
- Respect the privacy and personal rights of others by ensuring that use of IMIS resources does not constitute invasion of privacy, harassment, defamation, threats, intimidation, unwarranted annoyance or embarrassment, or discrimination based on race, sex, national origin, disability, age, religion, or sexual orientation.
- Respect and preserve the performance, capacity, integrity, and security of IMIS resources. Ensure that use of those resources does not circumvent system security and does not achieve or aid others to achieve unauthorized access. The organisation may take any immediate steps necessary to deal with threats to performance or degradation of its computing and electronic communication resources.
- Protect the purpose of IMIS resources to carry out the Organisation's primary mission. Use the IMIS resources only for the organisation-related purposes for which they were authorized. As with all municipal equipment, use of the computer resources, including the IT Network, for private or commercial purposes is prohibited, except as expressly authorized. Reasonable minimal personal use is permissible within the guidelines of this policy when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other municipal responsibilities, and is otherwise in compliance with IMIS policy. Further limits may be imposed on personal use by units or departments.
- Respect the intellectual property rights of others by ensuring that use of IMIS resources does not violate any copyright or trademark laws, or municipal licensing agreements (including licensed software).
- Senior managers are responsible for the implementation of this policy in their respective units.
- IMIS reports will be distributed on a monthly basis as a monitoring tool for compliance.
- Monthly reports will be submitted to Management.

- **Procedure for handling correspondence**
  - All incoming and outgoing correspondence must be sent to the Registry from where it will be scanned and distributed electronically via IMIS to the relevant employees.
  - All correspondence will be allocated a file number according to the file plan which must be used on all correspondence. (Letter, e-mail or fax)
  - Printouts may only be made in urgent circumstances and where response must be given on the original, in which case a copy must be put on the file.

- Where original contracts are involved needing signatures, the original must be requested on hard copy file from the Registry, and a copy of the signed document must be returned to Registry for safekeeping.
- Problems concerning the use of IMIS can be directed to the Administrator or IT personnel if an IT related problem is encountered.
- No hard copies of incoming faxes or mail will be distributed; it is the responsibility of every individual to check his/her inbox on IMIS on a regular basis.
- IMIS provides an audit trail of all internal messages; mail or instructions When going on leave employees must complete all their correspondence and make sure that their IMIS will be transferred to someone who will attend to it via the IN/OUT whiteboard.
- Before leaving the service of the Organisation each user must ensure that all outstanding items in IMIS had been completed and properly dealt with. The relevant Manager must ensure that this is done.

## Violation of Policy

Violations of acceptable use of IMIS resources include, but are not limited to:

- Use of another person's User account
- Providing one's user account and password to someone else to use;
- Accessing or transmitting information that belongs to another user or for which no authorization has been granted;
- Any attempt to make unauthorized changes to information stored on IMIS system;
- Viewing data that one does not have security rights to, or should not have rights to view;
- Unauthorized copying of information stored on the IMIS system;
- Any action that jeopardizes the availability or integrity of any IMIS resources;
- Use of IT resources that interferes with the works of IMIS resources, staff or the normal operation of the municipal computing systems;
- Any attempt to bypass the IMIS security systems including the Network Access Control system (NAC);
- Copying or distributing IMIS data without proper authorization;
- Stating or implying that one speaks on behalf of the IMIS system or using the IMIS name, marks or logos without proper authorization;
- Violation of laws, including copyright infringement;
- Use of IMIS resources for personal commercial purposes; and
- Using IMIS resources irresponsibly or in a way that might needlessly interfere with the work of others. This includes transmitting or making accessible offensive, annoying, or harassing material, or materials such as chain letters, unauthorized mass mailings, or unsolicited advertising; intentionally, recklessly, or negligently damaging any system, material, or information not belonging to the user; intentionally intercepting electronic communications or otherwise violating the privacy of information not belonging to or intended for the user; intentionally misusing system resources or making it possible for others to do so; or loading software or data from untrustworthy sources on to the IMIS system.

## Enforcement

Failure to use IMIS resources responsibly in accordance with the standards set forth in this policy threatens the atmosphere for the sharing of information, the free exchange of ideas, and the secure environment for creating and maintaining information. Any member of the organisation who violates this policy may be subject to disciplinary action under appropriate municipal disciplinary procedures.

The organisation may take such action as may be necessary in its discretion to address any use violation(s) under this policy, up to and including termination of a user's account. IT may temporarily suspend or block access to an account when it reasonably appears necessary to protect the integrity, security, or functionality of IMIS resources, or to protect the organisation from liability. In addition, TGIS reserves the right to limit or restrict the use of its IMIS resources when there is evidence of a violation of applicable municipal policies, contractual agreements, laws. The organisation may refer suspected violations of applicable law to the appropriate law enforcement agencies.

## Training

The Administrator will give each employee his/her username and help to set up the program with basic instructions.

All users will be trained. New staff members will be assigned a mentor by HOD from that particular department.

## Definitions

| | |
|---|---|
| TGIS: | Total Geo-spatial Information Solutions |
| IMIS: | Integrated Municipal Information System |
| NAC: | Network Access Control – NAC software tests and verifies that all computers connected to the municipal network have current virus protecting and operating system updates applied in order to protect the network. |

## References

National Archives and Records Services of South Africa Act

IMIS Training Manual