ICT Network Policy

1. Preamble

Access to computer systems and networks owned or operated by Mohokare Municipality is a privilege which imposes certain responsibilities and obligations and is granted subject to Municipality's policies laws.

The objective of this policy is to ensure an available, reliable, secure, and responsive network environment at Mohokare Municipality. It is the responsibility of each User to ensure that the municipality's technology is used appropriately.

This policy has been developed considering the following prescripts and or acts:

- Promotion of Access to Information Act (Act no 43 of 1996);
- Electronic Communications and Transactions Act (Act no 25 of 2002);
- The Constitution of the Republic of South Africa (Act 108 of 1996)
- The protection of Information Act (Act 84 of 1982)
- The National Archives of South Africa Act (Act 43 of 1996)
- The Municipal Finance Management Act (act 1 of 2002)
- Organizational policies and Procedures (Mohokare Municipality)

2. Scope

This policy is applicable to all employees of the Mohokare Local Municipality, including permanent and temporary employees as well all other stakeholders who make use of the Mohokare Local Municipality ICT network technologies.

3. Acceptable Use

Any activity that compromises the performance of the municipality's computers and/or network such that others are negatively affected is not acceptable.

Acceptable use is always ethical, reflects academic honesty, and shows restraint in the consumption of shared resources.

It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and an individual's rights to privacy and freedom from intimidation, harassment, and unwarranted annoyance.

Examples of inappropriate use at any time include but are not limited to:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by municipality.

- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which municipality or the end user does not have an active license.

- Introduction of malicious programs onto any device connected to the campus network (i.e., viruses, worms, Trojan horses, e-mail bombs, etc.).

- Using a municipality's computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

- Port scanning or security scanning is expressly prohibited unless prior notification to the Information Technologies Department is made.

- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

- Circumventing user authentication or security of any host, network or account.

- Interfering with or denying service to any user or network (i.e. denial of service attack).

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

4. Policy Review

This policy shall be reviewed annually.