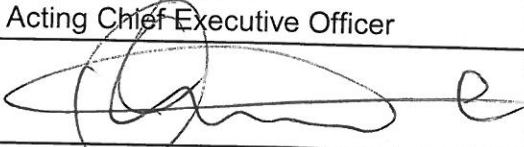




**MUNICIPAL INFRASTRUCTURE SUPPORT AGENT
(MISA)**

POLICY

**INFORMATION TECHNOLOGY EMAIL AND INTERNET ACCEPTABLE
USE**

Policy Number:	MISA
Version Number:	V1
Effective Date:	04/04/2014
Review Date:	31/03/2016
Authorised By:	Ongama Mahlawe Acting Chief Executive Officer
Signature:	

Contents

1.	PREAMBLE	3
2.	PURPOSE	3
3.	SCOPE	3
4.	DEFINITIONS	4
5.	POLICY PRINCIPLES.....	5
6.	LEGISLATIVE IMPERATIVES.....	7
7.	COMMENCEMENT DATE	7

O.M.

1. PREAMBLE

The Municipal Infrastructure Support Agent (MISA) is a government component established by the Minister of Cooperative Governance and Traditional Affairs (CoGTA) in terms of Chapter 6 of the Public Service Act. MISA's mandate is to accelerate municipal infrastructure provisioning by supporting municipalities with technical expertise in the planning, development, operations and maintenance of infrastructure provisioning throughout South Africa.

MISA occupies offices at Letaba House, Riverside Office Park, 1303 Heuwel Avenue, Centurion.

2. PURPOSE

- 2.1. This policy serves as a measure to control the utilisation of the internet and email facilities at MISA.
- 2.2. To prevent reputational risk to MISA. when an e-mail is sent from a MISA e-mail address, the general public tend to view that message as a MISA employee statement. This risk must be mitigated.
- 2.3. To define the rules of accessing the internet at MISA.
- 2.4. This policy seeks to ensure that Employees do not violate MISA's corporate internet and email facilities for personal gain, acts of sabotage, defamation of MISA's corporate image or any form of abuse related to the organisations technology infrastructure and systems.
- 2.5. Any Employee/s found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. It is in the Employees' best interest to familiarise themselves with this policy and strictly adhere to all aspects of the policy.

3. SCOPE

- 3.1. This policy applies to all employees, contractors, and other authorised third party entities that use the MISA's email and internet facilities. The ICT department, in an effort to safeguard the MISA's information technology resources and to protect the confidentiality of data, must introduce email and internet usage measures in the working environment.
- 3.2. This Policy specifies appropriate use of any e-mail sent from MISA's e-mail addresses and applies to all employees, vendors, and agents operating on behalf of the Agency.
- 3.3. This policy applies to all personnel with access to the internet and related services via MISA's network infrastructure. Internet related services include all services provided with the TCP/IP protocol, including but not limited to electronic mail (e-mail), file transfer Protocol (FTP), Gopher, and World Wide Web (WWW) access.

O.M

4. DEFINITIONS

MISA	Municipal Infrastructure Support Agent
CHAIN E-MAIL OR LETTER	E-mail, typically the body of the note has direction to send out multiple copies of the note and promises good luck, charity drives? or money if the direction is followed.
E-MAIL PROTOCOL	(i.e. SMTP, POP3, IMAP) is a method by which a communication channel is established between two computers and email is transferred between them.
E-MAIL DISCLAIMER	
EMPLOYEE	A person who is appointed to an approved post on the MISA establishment on a permanent, temporary or fixed term contract of employment.
FIREWALL	A device designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks.
FORWARDED E-MAIL	E-mail resent from an internal network to an outside point.
IT DEPARTMENT	Information Technology Office / Directorate.
INTERNET	
IT STAFF	Personnel (MISA appointed and contractors) working in the IT Department.
PROXY SERVER	
SENSITIVE INFORMATION	Information is considered sensitive if it can be damaging to MISA or its customers reputation or industry standing.
TCP / IP	
UOS	Uninterruptable Power Supply.
VENDOR	A supplier who provides goods or services to a company.
ICT	ICT refers Information and Communication Technologies which is a "diverse set of technological tools and resources used to communicate, and to create, disseminate, store, and manage information." These technologies include computers, the internet, broadcasting technologies (radio and television), and telephony.
TCP / IP	Transmission Control Protocol/Internet Protocol - is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination

D.M.

UNAUTHORISED DISCLOSURE	The intentional or unintentional revealing of restricted information to people, both inside and outside MISA, who do not have a need to know that information.
VIRUS WARNING	E-mail containing warnings about virus or malware. The overwhelming majority of these e-mails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.

5. POLICY PRINCIPLES

- 5.1. E-mail (electronic mail) is a channel of communication that enables messaging from one person to another or to groups of people via computer networks. E-mails are cost and time efficient as it allows the user to send a message to another user at any given time, at the cost of a local telephone call and, in turn it allows the receiver to read the message and respond to it in his/her own time.
- 5.2. The internet is a global network of computers linked together by diginet lines and other communication apparatus, which allows a host of global user's access to the most dynamic form of communication and sharing of data and information. The internet, with its diverse information content and communication capabilities, is a powerful and productive tool that provides fast and cost-effective communication via e-mail and web services. It provides access to current information and data.
- 5.3. Email and internet are enabling tools provided by MISA and those who have access (employees, contractors or authorised third parties) must familiarise themselves with the provisions of this Policy and ensure compliance. Breaches or suspected breaches of this policy and its terms must be reported to the IT Director.
- 5.4. MISA's computers and computer workstations, terminals, printers, telephones, facsimile machines and other devices either owned by MISA or authorised by MISA to be connected to its networks are primarily for business purposes.
- 5.5. The following applies to all information technology resource users at MISA:
 - 5.5.1. Respect the privacy of other users;
 - 5.5.2. Respect the rights of other users;
 - 5.5.3. Respect the intended use of resources and systems;
 - 5.5.4. Respect the integrity of the system or network; and
 - 5.5.5. Comply with all MISA's policies and procedures applicable to ICT as prescribed by the ICT Director and approved by the Chief Executive Officer.
- 5.6. *Use Of E-Mail Facilities*
 - 5.6.1. MISA's corporate e-mail system shall not to be used for the creation and/or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

- 5.6.2. Employees who receive any emails with this content from a MISA e-mail address should report the matter to management and the IT Director.
- 5.6.3. E-mails that are not work related should be kept at a minimum; and such non-work related emails must be saved in a separate folder from work related e-mails.
- 5.6.4. Sending chain letters or joke emails from a MISA's e-mail account is prohibited.
- 5.6.5. Virus or other malware warnings and mass mailings from MISA's corporate network must first be approved by the IT Director before sending. These restrictions also apply to the forwarding of mail received by an employee.
- 5.6.6. MISA's employees, contractors, and third parties utilizing the MISA e-mail facility shall have no expectation of privacy in anything they store, send or receive as MISA will from time to time monitor messages, that is, random checks will be undertaken without notice.
- 5.6.7. All outgoing e-mails must have an e-mail disclaimer as an appendix. This will be automatically set up on the e-mail server and will be as default to all outgoing e-mails. The disclaimer is as follows:

This e-mail is a business record of the Municipal Infrastructure Support Agent (MISA). Any files transmitted with it are confidential and are intended solely for the use of the individual or entity to which they are addressed. This communication represents the originator's personal views and opinions, which do not necessarily reflect those of MISA. If you are not the original recipient of this communiqué, any use, dissemination, forwarding, printing, or copying of this e-mail is strictly prohibited.

- 5.7. MISA will ensure that employee's e-mails are retained and archived for a period of 3 years after which they will be automatically deleted from the central storage. If an employee wishes to retain an e-mail for a longer period, it is the responsibility of such an employee to archive such e-mails for that period.

5.8. Use of Internet Facilities

- 5.8.1. Access to the internet through MISA's network facilities is a privilege. Users granted this privilege must adhere to strict guidelines concerning the appropriate use of this information resource. Users who violate the provisions outlined in this document are subject to disciplinary action up to and including suspension, termination that will be determined based on the seriousness of the offence. In addition, any inappropriate use that involves a criminal offence will be dealt with in accordance with the criminal justice system.
- 5.8.2. Access to the internet is specifically limited to activities in direct support of MISA's business operations. Access the internet for educational and research purposes is permitted but care should be taken to limit such access outside of MISA's working hours so that productivity is not hampered.
- 5.8.3. Access to internet using MISA network will be controlled using a internet proxy server.
- 5.8.4. When in doubt about what constitutes acceptable internet use the user is advised to contact the IT Director or delegated official for guidance.

- 5.8.5. MISA's internet facilities SHALL NOT be used for the following:
 - 5.8.5.1. Illegal or unlawful activities. Examples of this would be the transmission of violent, threatening, defrauding, pornographic, obscene or otherwise illegal or unlawful subject matter.
 - 5.8.5.2. Private, recreational or other non-company related activities.
 - 5.8.5.3. Commercial or political purposes.
 - 5.8.5.4. Personal gain such as undertaking work for profit.
- 5.9. Employees shall not attempt to circumvent or subvert security measures implemented by MISA to protect its resources or any other system connected to or accessible through the internet.
- 5.10. Employees shall not use internet access for interception of network traffic for any purpose unless they are undertaking in authorised network administration.
- 5.11. Employees shall not make or use illegal copies of copyrighted material, store such copies on The Agency's equipment, or transmit these copies over the Agency network.

6. LEGISLATIVE IMPERATIVES

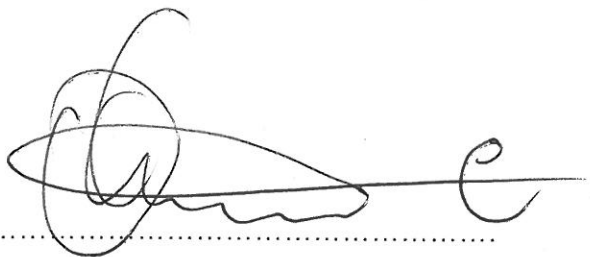
- 6.1. Should any third party, who has a contractual relationship with MISA contravene the provision of this Policy they will be dealt with in terms of the penalty clause of the agreement entered into by and between him/her and MISA.
- 6.2. Employees who violate this Policy will be disciplined in terms of measures contained in or published in one or more of the following acts, regulations and policy prescripts (this list is by no means exhaustive):
 - 6.2.1. Labour Relation Act, 1996 as amended
 - 6.2.2. Public Service Act, 1999;
 - 6.2.3. Public Service Regulations 2001 as amended;
 - 6.2.4. Public Finance Management Act, 1999 (Act No.1 of 1999);
 - 6.2.5. Treasury Regulations issued in terms of PFMA, 1999;
 - 6.2.6. SITA act, 1998 as amended
 - 6.2.7. Any other applicable legislation, regulation or policy.

7. COMMENCEMENT DATE

This policy becomes effective on the date of approval and signature by the CEO.

D.M.

Adopted for implementation on this 1st day of April
in the year 2014

A handwritten signature in dark ink, consisting of a large, stylized 'G' followed by a horizontal line and a small 'e' at the end.

CHIEF EXECUTIVE OFFICER (Acting)