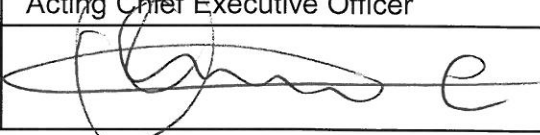




**MUNICIPAL INFRASTRUCTURE SUPPORT AGENT
(MISA)**

POLICY

***USE AND STANDARDISTION OF IT COMPUTER EQUIPMENT,
PERIPHERALS AND APPROVED SOFTWARES***

Policy Number:	MISA
Version Number:	V1
Effective Date:	01/04/2014
Review Date:	31/03/2016
Authorised By:	Ongama Mählawe Acting Chief Executive Officer
Signature:	

Contents

1.	PREAMBLE	3
2.	PURPOSE	3
3.	SCOPE	4
4.	DEFINITIONS	4
5.	POLICY PRINCIPLES.....	5
6.	LEGISLATIVE IMPERATIVES	9
7.	COMMENCEMENT DATE	9

D.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. The purpose of this policy is to provide guidelines for the provision and allocation of computer equipment and peripherals to employees, for the execution of their duties.
- 2.2. The purpose of this policy is to ensure all ICT equipment and software at MISA is procured efficiently, effectively, economically and that value for money is achieved. A standardised network system, standard software and administrative computing systems are essential for this, as is the standardisation of the hardware that will run these systems. MISA will benefit from lower ICT costs and a total managed environment
- 2.3. MISA is responsible for providing its employees with computer equipment and peripherals for the performance of their duties, execution of managerial instructions and communication purposes in and outside the office.
- 2.4. All new computer purchases by MISA should meet a minimum standard for both hardware and operational systems requirements. Such standards shall be reviewed on a regular basis to ensure computer systems are adequately provisioned to meet the needs of MISA and the IT Industry, this is done in order to achieve optimal productivity and ensure that MISA derives value for money from IT Resources.
- 2.5. MISA will implement stringent software control measures and related policies to ensure that employees cannot download or install unauthorised or illegal software. Illegal or unauthorised software can be detrimental to MISA in terms of network integrity, cause of malicious harm to the computer network and applications and attract fines or penalties from the Original Equipment Manufacturers (OEM's) for unlicensed/pirated software.
- 2.6. To ensure that all IT related equipment either owned by MISA or authorised by MISA to be used within MISA and connecting to its networks are primarily for MISA business functions. As such, all information technology resource and equipment users within MISA are expected to:
 - Respect the privacy of other users.
 - Respect the rights of other users.
 - Respect the intended use of resources, equipment and systems.
 - Respect the integrity of the system or network.
 - Adhere to all MISA policies and procedures mandated by the Chief Executive Officer or Delegate.
- 2.7. To provide a regulatory framework for the acquisition and use of software utilised in the systems environment at MISA
- 2.8. This policy strives to ensure that employees comply with MISA's rules and regulations with regard to issuing and usage of computer equipment and related peripherals.

- 2.9. It ensures that employees do not use illegal, unlicensed or non-approved software on MISA's computers and corporate network; and that MISA's reputation, integrity and computer security cannot be compromised by the use of illegal, unlicensed or non-approved software.

3. SCOPE

- 3.1. This policy applies to all MISA employees.
- 3.2. The scope of this policy includes all administration based employees who are permanently or temporarily employed by MISA. Other employees (cleaners, labourers, etc.) may have access to central shared computer equipment for access to e-mail or mandatory application systems.
- 3.3. This policy applies to all employees, contractors, and other authorised third party entities that use MISA's IT Equipment as working tools, in order to safeguard the use of it Computer equipment and related peripherals. This include standardize on software and IT related equipment in order to conform to best industrial practices.
- 3.4. All employees, contractors and authorised 3rd party entity must familiarise themselves h this Policy's provisions and ensure compliance. Everyone is responsible for reporting any suspected breaches of this policy terms to the IT Director or the Senior Management of MISA.
- 3.5. The policy is applicable to all computer, network and system users purchased and employed by MISA Respectively.

4. DEFINITIONS

MISA	Municipal Infrastructure Support Agent
ASCII	American Standard Code for Information interchange. It is the character-encoding scheme based on the ordering of the English alphabet. ASCII codes represent text in computers, communications equipment, and other devices that use text.
CEO	Chief Executive Officer
COMPUTER EQUIPMENT	Refers to a laptop, desktop and printers
E-MAIL PROTOCOL	(i.e. SMTP, POP3, IMAP) A method by which a communication channel is established between two computers and email is transferred between them.
EMPLOYEE	A person who is appointed to an approved post on the MISA establishment on a permanent, temporary or fixed term contract of employment
ICT	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.
IT STAFF	Personnel working in the IT Department.
IT DEPARTMENT	Information Technology Office / Directorate.
NETWORK DEVICES	Computers and devices interconnected by communications channels that facilitate communications among users.
SOFTWARE	written programs or procedures or rules and associated documentation pertaining to the operation of a computer system and that are installed on a computer or laptop
SITA	State Information Technology Agency as regulated In terms of the SITA act 88 of 1998 as amended.
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.

5. POLICY PRINCIPLES

5.1. The Issue and Use of Computer Equipment and Peripherals

- 5.1.1. Laptop computers are a standard issue for Senior Management, Provincial Programme and Project Managers and field workers. An employee who does not fall under this category may be issued with a laptop computer, subject to such an employee submitting a comprehensive request to the Chief Executive Officer (CEO). The motivation must clearly state why the employee requires a laptop computer. The Chief Executive Officer may then approve or disapprove the request based on the employee's actual job requirements.
- 5.1.2. All administration based employees will be issued with desktop computers as a standard work tool. Other employees (labours, cleaners, field employees, etc.) may be issued with shared computing facilities for access to email or MISA's mandatory applications (leave forms, etc.)
- 5.1.3. Desktop colour laser printers are a standard issue for senior management and employees printing confidential reports (salaries, human resource records, etc.) Other employees must utilise shared printing facilities or multi-function centres.
- 5.1.4. Employees requiring other computer equipment or peripherals must submit a request to the CEO, clearly motivating the need for such, the request must be recommended by the relevant line manager and then presented to the CEO for approval IT Department will only act on a signed approval from the CEO.
- 5.1.5. *Custodianship of Equipment, Usage and Security –*

O.M.

- 5.1.5.1. All equipment procured / leased belongs to MISA and not to any employee. When equipment is assigned, it is assigned to a particular post. The employee occupying that post is responsible for that particular equipment until such time as the employee resigns or is transferred to another post.
- 5.1.5.2. Employees who have been allocated with laptops, memory sticks digital cameras or any other mobile device must take the utmost care in preventing theft, damage or loss of such equipment.
- 5.1.5.3. In the unfortunate instance where any equipment has been stolen, the responsible employee must report the matter to the South African Police Services (SAPS) within 24 hours. The case number and a report detailing the incident must then be submitted to the IT Director.
- 5.1.5.4. If any equipment is lost/stolen due to the employee's negligence (e.g. leaving the equipment in an unlocked office, visible areas in motor vehicle, not locked to workstation, etc.), or damaged (broken laptop screens, keyboards, etc.) due to mishandling, the employee shall make good the loss financially.
- 5.1.5.5. If the loss is incurred within twelve (12) months of allocation of the equipment, the value shall be equal to the replacement value of new equipment of the same make and type. If the loss is incurred after 12 months of allocation of the equipment, then the depreciation value shall be taken into account when determining the value of the equipment.
- 5.1.5.6. No person other than the employee may have access to the computer equipment. The exceptions are 3rd party contracted support service providers.
- 5.1.5.7. No employee may use any of MISA's computer equipment for personal financial gain.
- 5.1.5.8. Employees must handle all equipment with care and respect; and in accordance with terms and conditions stipulated in the asset allocation form. Mobile equipment should be transported in their appropriate carry bags.
- 5.1.5.9. Regular cleaning should also be done by the employee who has been issued with such equipment. This should be enforced by the employee's respective supervisors.
- 5.1.5.10. If there is any evidence of an employee deliberately damaging equipment, then such an employee will be subject to MISA's disciplinary code.
- 5.1.5.11. All desktop computers and laptops must be secured with a locking device to combat theft.

5.1.6. *Replacement, Transfer and Movement of Equipment*

- 5.1.6.1. The industry standard for replacement of laptops and desktop computers is 36 month intervals. MISA will adhere to this

standard.

- 5.1.6.2. Dysfunctional equipment will however be replaced as and when required regardless of the 36 month cycle
- 5.1.6.3. Redundant / obsolete equipment which is MISA's property will be disposed of via MISA's asset disposal policy as administered by the asset management unit.
- 5.1.6.4. Printers will be replaced over a 54 month cycle.
- 5.1.6.5. Only dysfunctional or redundant printers will be replaced before the 54 month refresh cycle period.

5.1.7. Leased and Outright Purchased Equipment

MISA may decide to lease all IT equipment or Purchase outright depending on MISA financial standing. All the lease equipment should be lease not for more than 36 month. Only the IT Network Infrastructure Equipment (i.e. Server, Switches and etc.) may be lease for 54 months.

5.2. Standardisation of Computer Equipment

- 5.2.1. The IT Director is responsible for selecting and standardising all ICT equipment for MISA. ICT equipment must be *Tier 1* products and must be able to have suitable processing power to run MISA specific applications.
- 5.2.2. Desktops, laptops and printers must be standardised with superior products while ensuring that value for money is derived.
- 5.2.3. MISA is not brand specific with regard to ICT equipment however the IT Director must use his/her discretion to ensure that ICT equipment are products which have fair standing in the ICT industry and in accordance with that recommended by the ICT Steering Committee.

5.3. Standard Approved Software

- 5.3.1. MISA uses Microsoft desktop operating systems, Microsoft Exchange for its e-mail application, Microsoft Office Professional and Microsoft server operating systems as products of choice for its corporate network. The software suite must be based on all corporate edition products and be fully licensed by the software vendor.
- 5.3.2. Acrobat Reader is the standard software of choice for viewing pdf documents. Certain employees may have Acrobat Writer Professional for converting documents into pdf formats.
- 5.3.3. WinZip is the standard software for zipping and unzipping large documents.
- 5.3.4. As per the National Treasury approval, MISA shall have its own financial systems, however the selected system or application software should be in line with the SITA interoperability and security standards..
- 5.3.5. MISA may procure any other product specific software (Project, Visio, Rightfax, etc.) or replace any of its existing software and applications as may be required. All software that is purchased must be informed by the actual

O.M.

needs of MISA and must be recommended by the ICT steering committee and rated by ICT advisory bodies (Gartner, and so on)

5.3.6. Open Source Software (OSS) applications and systems may be considered for use depending on the specifics of the application and systems, the benefits of using such and the user friendliness of the application and system. The cost benefit and support factor must also be considered before using or migrating to any OSS platforms, applications or systems.

5.3.7. *Software Upgrades and Licensing*

5.3.7.1. Software may be upgraded when new versions are released or when the need for such arises.

5.3.7.2. All software used on MISA's corporate network must be fully licensed and must be in line with the IT Security Policy. No unlicensed or unauthorised software will be permitted on MISA's corporate network or any of MISA's computers and equipment.

5.3.7.3. Software licenses must be renewed annually and MISA must have the exact number of license seats as the number of network users on the corporate network. The licenses must be stored in MISA's strong room, safe or filing room.

5.3.8. *Antivirus Software*

5.3.8.1. MISA will use corporate antivirus software which runs on desktops, and servers and has all layers of protection (virus, worms, Trojan, spam filters, and so on) as a complete suite and in accordance with the stipulations of the IT Security Policy.

5.3.8.2. Antivirus software must be installed on a dedicated server from which desktops and laptops must download the regular updates.

5.3.8.3. The updates must be set for automatic downloads whenever the new virus definition patterns are released. This is applicable for the host server as well as desktops and laptops.

5.3.8.4. Always scan any external storage media (flash drives, external hard drives, etc.) for viruses before using them on MISA's computer equipment.

5.4. Interception and Monitoring

5.4.1. In terms of the regulation of Interception of Communication and Provision of Communication - Related Information Act, Act 70 of 2002, and in particular section 5, 6 and 16, MISA may intercept and / or monitor an employee's communication from time to time.

5.4.2. MISA may therefore intercept any communication and indirect communication:

5.4.3. By means of which a transaction is entered into in the course of that business;

5.4.4. Which otherwise relates to that business; or

O.M.

- 5.4.5. Which otherwise takes place in the course of the carrying on of that business, in the course of its transaction over telecommunication system;
- 5.4.6. This monitoring may include (but is not necessarily limited to) listening to, recording, viewing, examining or inspecting your emails, correspondence, text messages, internet use, telephone and other conversations.
- 5.4.7. Any employee 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 its stipulations.
- 5.4.8. This policy is subject to change and amendments in line with technology refreshes, changes and updates. Such changes and amendments will be reflected in this policy as a version change and will be circulated to all employees
- 5.4.9. The policy shall be reviewed when necessary.

6. LEGISLATIVE IMPERATIVES

6.1 Documents that should be read with this policy:

6.1.1 Treasury practice note 9 of 2009

(<http://www.treasury.gov.za/divisions/sf/sc/PracticeNotes/default.aspx>)

6.1.2 IT Security Policy

6.1.3 Regulation of Interception of Communications and Provision of Communication-related information Act 70 of 2002 (<http://www.info.gov.za/gazette/acts/2002/a70-02.pdf>)

6.1.4 Patch Management Procedure

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

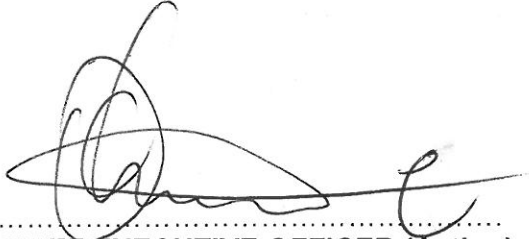
6.2.7. Any other applicable legislation, regulation or policy.

7 COMMENCEMENT DATE

O.M.

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

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

A handwritten signature in black ink, consisting of a large, stylized 'C' followed by a series of loops and a long horizontal stroke ending in a small 'e'.

CHIEF EXECUTIVE OFFICER (Acting)