MUNICIPAL INFRASTRUCTURE SUPPORT AGENT
(MISA)

POLICY

INFORMATION TECHNOLOGY SECURITY POLICY

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

Contents

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.

This policy applies to all employees, contractors, and other authorised third party entities that use MISA's computer network. In order to safeguard MISA's information technology resources and to protect the confidentiality of data, adequate security measures must be implemented.

This Information Technology Security Policy (hereafter, "IT Security Policy") reflects MISA's commitment to comply with leading practice principles that govern, protect, and secure sensitive and confidential information, as well as ICT equipment. Wherever possible, this policy attempts to establish a balance between the risk of loss of information resources, including data misuse, and the effort and cost of the security measures. It includes feasible provisions to reduce the risk of theft, fraud, destruction and other misuses of MISA's IT resources.

Administrative information processing, digital telecommunications and related technology are critical business operations of MISA. Inappropriate exposure of confidential and/or sensitive information, loss of data and inappropriate use of computer networks and systems can be minimised by complying with reasonable standards, attending to the proper design and control of information systems and applying sanctions when violations of this Security Policy occur.

2. PURPOSE

The purpose of the policy is to establish rules to ensure the security of confidential and/or sensitive information stored or transmitted electronically and to ensure protection of MISA's information technology resources. The policy assigns responsibility and provides guidelines to protect MISA's systems and data against misuse and/or loss.

3. SCOPE OF APPLICABILITY OF THE POLICY

This policy applies to the IT Department and covers every computer and computer workstation, terminal, telephone, facsimile machine and other devices either owned by MISA or authorised by MISA to connect to its networks.

It also applies to every employee, contractor and authorised third party entity accessing MISA's networks and resources.

4. USER AWARENESS

Security is the responsibility of everyone who uses MISA's information technology resources. Every employee, contractor and authorised 3rd party entity should become familiar with this Policy's provisions and the importance of adhering to it when using MISA's computers, networks, data and other information resources. Each Employee is responsible for reporting any suspected breaches of its terms to the IT Director or delegated official.

MISA's computers and computer workstations, terminals, telephones, facsimile machines and other devices either owned by MISA or authorised by MISA to connect to its networks are primarily for Agency business functions hence all information technology resource users within MISA are expected to:

4.1. Respect the privacy of other users.
4.2. Respect the rights of other users.
4.3. Respect the intended use of resources and systems.
4.4. Respect the integrity of the system or network.
4.5. Adhere to all Agency policies and procedures mandated by the CEO or Delegate.

5. DEFINITIONS

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.
EMPLOYEE	refers to a person appointed permanent in terms of the public service act, 1994 (act no 103 of 1994 as amended) or temporary employees under the employ of MISA A person who is appointed to an approved post on the MISA establishment on a permanent, temporary or fixed term contract of employment.
IT STAFF	Personnel working in the IT Department
IT DEPARTMENT	Information Technology Office / Directorate within MISA.
FIREWALL	A device designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks.
MBSA	Microsoft Baseline Security Analyser
NTFS	New Technology File System which is the standard file system of windows.
OS	Operating System which is a collection of software that manages computer hardware resources and provides common services for computer programs.
MISA	Municipal Infrastructure Support Agent (MISA)
UPS	Uninterruptable Power Supply
VENDOR	A supplier who provides goods or services to a company
VPN	Virtual Private Network which enables a computer to send and receive data across shared or public networks as if it were directly connected to the Local Area Network

O. M-

WSUS	Window Server Update Services which is a computer programme developed by Microsoft Corporation that enables administrators to manage the distribution of updates and hotfixes released for Microsoft products to computers in a corporate environment.
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.

6. IT SECURITY POLICY PRINCIPLES

6.1. Data Backup

6.1.1. A full backup will be performed by the IT Administrator / delegate at least once a month.

6.1.2. Daily backups will be performed as incremental backups.

6.1.3. Backups will be scheduled to run automatically every night.

6.1.4. Backup logs will be checked daily to ensure successful completion of backups.

6.1.5. Cleaning of backup devices will be performed according to manufacturer's specifications.

6.1.6. Completed backups will be stored off-site at a location identified by MISA.

6.1.7. Backups will be validated and tested at least once every three months.

6.1.8. MISA will enter into an agreement for the offsite storage/solution with a reputable service provider to store backup.

6.2. Physical Security

6.2.1. All server and switch rooms will be constructed with concrete walls, raised floors and fire resistant doors.

6.2.2. All third-party vendor access to server and switch room will be logged in a register in the format (Name, Surname, Company, Purpose of Entry, Date and Time).

6.2.3. Third-party vendors must be accompanied by an IT staff member at all times, unless in cases where prior arrangement has been made and approved by the IT Director or delegated official.

D. M.

6.2.4. Where possible, server and switch rooms must be equipped with a temperature monitoring system which allows for alerts to be sent by e-mail and SMS when a high or low temperature alarm is triggered.

6.2.5. Log files will be maintained for equipment maintenance schedules according to manufacturer's specifications.

6.2.6. All computer equipment and peripherals in server and switch rooms will be connected to a UPS device.

6.2.7. The backup generator must be serviced according to manufacturer's specifications and a log must be maintained.

6.2.8. Server and switch rooms must be equipped with a fire detection system.

6.2.9. Where possible a fire preventions system (Halon or CO2) must be made available in server and switch rooms.

6.2.10. Before temporary off site removal of any computer equipment, a computer removal document must be completed and approved by the line manager.

6.2.11. Server rooms must be equipped with electronic access control devices and logs of all entries must be maintained.

6.2.12. Switch rooms must be locked when access is not required.

6.2.13. A print out of access control logs to the server room will be generated on a monthly basis or as and when required.

6.2.14. All unused computer equipment must be stored in a secure location.

6.2.15. Users are responsible for the safe keeping of equipment assigned to them. All Laptop users will be equipped with a lockup cables to assist with save guarding.

6.3. User Account and Password Management

6.3.1. All accounts shall be reviewed at least quarterly to ensure that access and account privileges are commensurate with the job description, need-to-know, and employment status.

6.3.2. The Human Resource Management must provide the necessary sign-on form when new appointments are made; no user account will be created or modified without a New/Modified User Form signed by HR and approved by the line manager.

6.3.3. All user accounts will be terminated immediately by the Network Administrator, upon an employee's departure from MISA either by dismissal, transfer, resignation, retirement, death or any other forms of departure. The Network Administrator will generate a monthly report to the IT Director, providing details regarding the terminated user accounts.

6.3.4. An employee's access to a user account will be changed/modified by the Network Administrator, in the case of a transfer to another directorate within MISA; and in accordance with the employee's new job functions and requirements.

O.M.

6.3.5. The Human Resource Department will ensure that IT Department is informed at least one month in advance of any resignations or transfers. This must be done by signing a User Termination Form.

6.3.6. All user accounts at MISA are created as Standard User Accounts. This means that users have standard privileges to log onto the network, use network printers that have been assigned to them, access their email, and use the internet and any other privilege that is a core requirement of their job function (example: financial systems).

6.3.7. User names are standardised and the employee's first name and surname will be used to enable the user to log onto the network, and user's computer. Email addresses are also standardised with the employee's first name and surname.

6.3.8. Where there are users with same surname and full names, the user's full name or second name may be used as an email address.

6.3.9. The password that an employee uses to log onto the network will be applied to access the employees email account and internet applications.

6.3.10. Users that require access to work on Human Resource and Financial systems will be issued with system passwords to access such applications. The system passwords and approval to use financial system are only granted and issued by the relevant System Manager / CFO / Delegate and not the IT Staff of MISA.

6.3.11. Internship Programme personnel and temporary appointed contractors will be issued with usernames and passwords for the duration of their term where upon it will be terminated.

6.3.12. Passwords must not contain the user's entire Account Name value or Full Name value. Both checks are not case sensitive.(i.e. changing of account name or full name values from lowercase to uppercase or vis-à-vis is not allowed).

6.3.13. Passwords must contain characters from three of the following five categories:

6.3.13.1. Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)

6.3.13.2. Lowercase characters of European languages (a through z, sharps, with diacritic marks, Greek and Cyrillic characters)

6.3.13.3. Base 10 digits (0 through 9)

6.3.13.4. Any Unicode character that is categorised as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

6.3.13.5. Non alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/

6.3.14. Passwords must never be written down on a piece of paper.

6.3.15. Never share passwords with anyone.

6.3.16. Use different passwords for all user accounts.

6.3.17. Passwords should be changed every 60 days.

O. M -

6.3.18. Example of Alphanumeric Password: Pass@1234! . This example is not to be used as a real password.

6.4. Virus Protection

6.4.1. Every system must be protected by anti-virus software.

6.4.2. Configurations must allow for removable media to be scanned for viruses before allowing access on MISA network.

6.4.3. A scheduled virus scan must be conducted on a monthly basis.

6.4.4. Automatic updating must be configured to allow for the latest virus definitions in order to keep systems secure and protected against new threats.

6.4.5. Reporting must be enabled to monitor and manage threats.

6.4.6. Anti-Virus clients must be configured to prevent users from disabling anti-virus protection.

6.5. Firewalls

6.5.1. All external connections must be protected by a firewall.

6.5.2. Every firewall must be configured with a deny-by-default policy.

6.5.3. Internet Access must be controlled by a proxy server.

6.5.4. Authentication to the firewall must be controlled by individual account access and the administrator user name and password must be changed and renamed.

6.5.5. User accounts must be assigned with the lowest level of privileges required to perform duties.

6.5.6. Firewall software should be patched and updated regularly, preferably, monthly.

6.5.7. Logging of firewall data must be enabled.

6.5.8. Logs must be reviewed weekly.

6.5.9. Logs must be archived monthly.

6.5.10. Configuration logs must be backed up monthly after every configuration change.

6.5.11. Administrators must be alerted in the event of possible attacks and in the event of system failure.

6.6. Patch Management

6.6.1. Automated tools will scan for available patches and patch levels, which will be reviewed as specified in the Patch Management Procedures document.

D.M-

6.6.2. Manual scans and reviews will be conducted on systems for which automated tools are not available.

6.6.3. Vendor supplied patch documentation will be reviewed prior to being applied to ensure compatibility with all system components.

6.6.4. Where possible, patches will be successfully tested on nonproduction systems installed with the majority of critical applications/services prior to being loaded on production systems.

6.6.5. Successful backups of mission critical systems will be verified prior to installation of patches. A mechanism for reverting to the patch levels in effect prior to patching will be identified.

6.6.6. Patches will be applied during an authorised maintenance window in cases where the patch application will cause a service interruption for mission critical systems.

6.6.7. Patches will be prioritised and applied in accordance with the Patch Management Procedures document.

6.6.8. Logs will be maintained for all system categories (servers, secure desktops, ASCII, switches, etc.) indicating which devices have been patched. System logs are useful for recording the status of systems and provide continuity among administrators. The log may be in paper or electronic form. The recorded information will include, but is not limited to, date of action, administrator's name, patches and patch numbers that were installed, problems encountered, and system administrator's remarks.

6.6.9. In the event that a system must be reloaded, all relevant data on the current OS and patch level will be recorded. The system should be brought back to the patch levels that were in effect before reloading started.

6.7. Remote Access Connections

6.7.1. Remote access connections are permitted; and all minimum security measures will be taken. MISA will configure a VPN tunnel for all remote users

6.7.2. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to MISA internal networks.

6.7.3. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.

6.7.4. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.

6.7.5. Dual (split) tunneling is NOT permitted; only one network connection is allowed.

6.7.6. All computers connected to MISA internal networks via VPN or any other technology must use the most up-to-date anti-virus software; this includes personal computers.

D.M -

6.7.7. VPN users will be automatically disconnected from MISA's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

6.7.8. The VPN concentrator is limited to an absolute connection time of 12 hours.

6.8. Workstation Security

6.8.1. The "auto run" function for removable devices and CD-ROMs must be disabled. A standard image must be configured for every model number of workstation.

6.8.2. The standard image must include anti-virus, latest patches, drivers and software.

6.8.3. The standard image must be reviewed monthly.

6.8.4. Users are not allowed to have administrative access on workstations and Laptops.

6.8.5. Local administrator accounts must be renamed and password changed.

6.8.6. User "My Documents" folder must be redirected to a server shared drive to enable backups to be performed. No user must save important documents and files on the desktop.

6.8.7. Automatic updates must be configured to obtain the latest patched from the WSUS server.

6.8.8. In cases where client data contains sensitive information, encryption software must be used to protect the data.

6.8.9. Security and event logs must be available for a minimum of thirty (30) days.

6.8.10. Any services not required must be disabled.

6.8.11. A screensaver password must be configured.

6.9. Server Security

6.9.1. All new servers must be deployed by using a standard image.

6.9.2. The standard image must include anti-virus, latest patches, drivers and software.

6.9.3. The standard image must be reviewed on a monthly basis.

6.9.4. All users with administrative access must be documented.

6.9.5. The local and domain admin accounts must be renamed and passwords changed.

O.M-

6.9.6. Automatic updates must be configured to obtain the latest patched from the WSUS server.

6.9.7. All volumes should be formatted with the NTFS file system.

6.9.8. All events must be logged and log files exported and archived.

6.9.9. Log files should be reviewed weekly before archiving.

6.9.10. All unneeded services must be disabled.

6.9.11. All servers must be secured with the MBSA tool on a regular basis.

6.9.12. A screensaver password must be configured.

6.10. Client Data

User Data folders must have permissions enabled and only the owner of the folder and files and administrators should be allowed access to these folders.

7. ACCOUNTABILITY

7.1. IT is responsible for ensuring that information resources are maintained in compliance with MISA's IT Security policies and procedures.

7.2. Systems administrators not managed by IT are responsible for ensuring that their systems are maintained in compliance with MISA's IT Security policies and procedures.

7.3. The IT Director is responsible for auditing and monitoring information systems to ensure that they comply with MISA's IT Security Policy, this function may be delegated to the relevant IT Manager.

7.4. MISA IT staff and/or IT service providers are responsible for ensuring that systems are maintained in compliance with MISA's IT Security Policy.

7.5. Human Resources will be responsible for informing IT regarding staff movements, i.e. transfer of staff in and out of MISA, new appointment, death, termination of employment or voluntary retirement and resignation. This information is to be supplied to IT a month in advance where appropriate.

8. LEGAL FRAMEWORK AND LEGISLATIVE IMPERATIVES

8.1. 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.

8.2. 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):

8.2.1. Labour Relation Act, 1996 as amended

D. M.

8.2.2. Public Service Act, 1999;

8.2.3. Public Service Regulations 2001 as amended;

8.2.4. Public Finance Management Act, 1999 (Act No.1 of 1999);

8.2.5. Treasury Regulations issued in terms of PFMA, 1999;

8.2.6. Any other applicable legislation, regulation or policy.

9. COMMENCEMENT DATE

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

Adopted for implementation on this 01 *day of* April

in the year 2014

....
CHIEF EXECUTIVE OFFICER (Acting)