094847

EPHRAIM MOGALE
LOCAL MUNICIPALITY

111
MARBLE HALL
0450
☎ 013-261 8400
013-261 2985

Leeuwfontein Office (013) 266 7025
Elandskraal Office (013) 268 0006
Zamenkomst Office (013)973 9160
Traffic Section (013) 261 8400

EXTRACTS FROM THE MINUTES OF THE 3RD ORDINARY COUNCIL MEETING OF EPHRAIM MOGALE LOCAL MUNICIPALITY HELD ON WEDNESDAY THE 29TH APRIL 2015

FILE/S: ~~8/4/P~~ 6/2/2/P

OC3/15/2015 INFORMATION COMMUNICATION TECHNOCLOGY (ICT) RELATED POLICIES ~~8/4/P [00/02/P]~~

RESOLVED

1. That the Council takes cognizance of the circulated report.
2. That the Council approves the following ICT related policies and procedures:
2.1 Account Management Policy.
2.2 Change Management Procedure.
2.3 End User Management Policy.
2.4 Patch Management Policy.
2.5 User Management Procedure.
2.6 ICT Global Policy.
2.7 ICT Security Policy.
3. That the Council approve the reviewal of the following policies and procedures:
3.1 Back up Policy & Procedure.
3.2 Allocation of Movable ICT Devises Policy & Procedure.
4. That the Council refer the policies to the LLF.
5 That the approved policies and procedures be implemented with effect from the 1st April 2015
6 That there be a clear policy that distinguish the ownership of the i-pad equipment carried by Councillors,
7. That the Council instruct the Municipal Manager to implement the decision accordingly.

LB Modisha

L.B. MODISHA
SPEAKER **29 APRIL 2015**

FINALISATION BY:

Referred to ...Director Corporate Services.....by Municipal Manager

.....

M.M. Mathebela
Municipal Manager

05/05/15.

.....

Date Received

OC3/15/2015 INFORMATION COMMUNICATION TECHNOCLOGY (ICT) RELATED POLICIES 8/4/P [06/02/P]

PURPOSE

For the Council to approve of the attached ICT policies.

BACKGROUND

Ephraim Mogale Local Municipality is an ICT environment as most of our administrative activities are carried out through the utilization of computers and network systems. It therefore becomes necessary to have policies to regulate the utilization of this important tool and yet vulnerable to misuse and abuses that may have detrimental consequences.

The policies further aims to regulate access to the municipal network, possibly from when a new employee comes into the system and when he/she leaves the institution.

The various attached policies in brief aims to cover inter alia the following:

- Establishing a standard for the administration of computing accounts that facilitate access or changes to the Ephraim Mogale Local Municipality. An account, at minimum, consists of a user ID and a password; supplying account information will usually grant access to some set of services and resources. This policy establishes standards for issuing accounts, creating password values, resetting password and managing accounts.
- regulating the implementation of changes in the current systems prompted by upgrades and the vital changes in systems technology used in the Municipality.
- establishing ethical guidelines for Ephraim Mogale Local Municipality's ICT users, assets and computing facilities.
  (ICT assets include desktop computers, desktop components, laptops, servers, switches, routers, printers, photocopiers, phones, 3G, Tablets, email, internet, mobile modems, firewall, software, business applications, municipal data and information).
- Describing the requirements for maintaining up-to-date operating system security patches on all Ephraim Mogale local municipality owned and managed workstations and servers.
- Procedure for the creation of new users on the system.
- regulating the use of ICT assets, provides guidelines, roles and responsibilities for acceptable use, prescribe minimum requirements for acceptable use, provides guidelines on the protection against unauthorized access, provides measures to safeguard intentional or unintentional loss of information and provides measures for adequate security protocols.
- Cover the ICT security,
- Addressing the procedures for backup.
- Regulate the allocation of movable ICT devised.

They are as follows:

1. Account Management Policy.
2. Change Management Procedure.
3. End User Management Policy.
4. Patch Management Policy.
5. User Management Procedure.
6. ICT Global Policy.
7. ICT Security Policy.
8. Back up Policy & Procedure.
9. Allocation of Movable ICT Devises Policy & Procedure.

RECOMMENDATIONS OF THE EXECUTIVE COMMITTEE

1. That the EXCO takes cognizance of the circulated report.
2. That the Council approves the following ICT related policies and procedures:

2.1 Account Management Policy.
2.2 Change Management Procedure.
2.3 End User Management Policy.
2.4 Patch Management Policy.
2.5 User Management Procedure.
2.6 ICT Global Policy.
2.7 ICT Security Policy.

3. That the Council approve the reviewal of the following policies and procedures:

3.1 Back up Policy & Procedure.
3.2 Allocation of Movable ICT Devises Policy & Procedure.

4. That the Council approves that the reviewed policies replaces any other policy that existed prior the reviewal of the policies.
5 That the approved policies and procedures be implemented with effect from the 1st April 2015
6. That the Council instruct the Municipal Manager to implement the decision accordingly.

RECOMMENDATIONS OF THE PORTFOKLIO COMMITTEE

1. That the Committee takes cognizance of the circulated report.
2. That the Council approves the following ICT related policies and procedures:

2.1 Account Management Policy.
2.2 Change Management Procedure.
2.3 End User Management Policy.
2.4 Patch Management Policy.
2.5 User Management Procedure.
2.6 ICT Global Policy.
2.7 ICT Security Policy.

3. That the Council approve the reviewal of the following policies and procedures:

3.1 Back up Policy & Procedure.
3.2 Allocation of Movable ICT Devises Policy & Procedure.
4. That the Council approves that the reviewed policies replaces any other policy that existed prior the reviewal of the policies.
5 That the approved policies and procedures be implemented with effect from the 1st April 2015
6. That the Council instruct the Municipal Manager to implement the decision accordingly.

RECOMMEND TO RESOLVE

1. That the Council takes cognizance of the circulated report.
2. That the Council approves the following ICT related policies and procedures:
2.1 Account Management Policy.
2.2 Change Management Procedure.
2.3 End User Management Policy.
2.4 Patch Management Policy.
2.5 User Management Procedure.
2.6 ICT Global Policy.
2.7 ICT Security Policy.
3. That the Council approve the reviewal of the following policies and procedures:
3.1 Back up Policy & Procedure.
3.2 Allocation of Movable ICT Devises Policy & Procedure.
4. That the Council approves that the reviewed policies replaces any other policy that existed prior the reviewal of the policies.
5 That the approved policies and procedures be implemented with effect from the 1st April 2015
6. That the Council instruct the Municipal Manager to implement the decision accordingly.

EPHRAIM MOGALE LOCAL MUNICIPALITY

ICT SECURITY POLICY & PROCEDURE

DOCUMENT APPROVAL

Responsible Person:	Name	Signature	Date
	Mahlobela MM		18/06/15

Date approved: 29 April 2015.

1. PURPOSE

The purpose of the policy is to set the standard for Information, Communication & Technology (ICT) security and to ensure appropriate security for all ICT data, equipment and processes within its domain of control.

2. SCOPE

Security policy and procedure is intended to support the protection, control and management of the organisation's information assets. This policy is required to cover all aspects of information within the municipality which could include data, hardware, software, users etc. The following are important concerning Security Policy:

- Confidentiality of information
- Integrity of data
- Assets
- Efficient and appropriate use
- System availability

3. USER REGISTRATION AND ALLOCATION

3.1 Human Resource division shall accordingly notify ICT section of the any newly employed personnel, then a network registration form shall be filled by the applicant with the approval of the Director or Manager of the department or section to which the applicant belongs to.

3.2 An Account setup and modification shall require the signature of the requestor's supervisor.

3.3 A completed "Network Registration form" shall be filed in the user's personal file, ICT section and records section. The identity number, full names of the applicant, department and the signature of the immediate supervisor shall be required to register a user on to the Ephraim Mogale Local Municipality's network.

3.4 Allocation of computer equipment shall commence after the registration process has been finalized by the ICT section. The equipment shall be allocated to the user by the ICT personnel.

4. PASSWORDS

4.1 Access to the Municipal network shall be through password.

4.1.1 All users shall create strong password that include numbers and case charactors.

4.1.2 Poor, weak password shall be identified by having the following characteristics:

- password that contains less than six characters.
- Password contains common usage word such as:
  - names of family, pets, friend, co-worker, fantasy characters, etc.
  - computer terms and names, commands, sites, companies, hardware, software, etc.
  - Birthdays and other personal information such as addresses and phone numbers.
  - words or numbers patterns like aaaabbb, qwert, 123321, etc.
  - words patterns preceded by a digit (e.g secrete1, 1secrete).

4.2 Strong password

Strong password shall be identified by having the following characteristics:

- contains both upper and lower case characters such (e.g a-z, A-Z).
- have digits and punctuation characters as well as letters (e.g 0-9, #$@*^>.
- six alphanumerical characters long and is a passphrase.
- language, slang, dialect, jargon, etc.
- are not based on personal information, names of family etc.
- Password should never be written down or stored on line.

4.3 Password protection

4.3.1 Users shall not use the same password for Ephraim Mogale Local Municipality accounts and other non-Municipal access such as personal internet account. Where possible users shall not use the same password for various Municipal access needs, and shall select one password for each access needs.

4.3.2 Users shall not share password with anyone, including Supervisors, Managers and Secretaries, all password are to be treated as sensitive and confidential information.

4.3.3 The following shall be classified as things not to be done:

- Reveal a password over the phone to anyone.
- Reveal a password via an email.
- Talk about a password in front of others.
- Hint at the format of the password.
- Share password with family members.
- Reveal password to co-workers while on vacation.
- Write down and store password in your office and in a file on any computer without encryption.

4.3.4 The following shall be classified as things to be done:

- Change password on monthly basis.
- In the event an account is suspected to have been compromised, it must be reported immediately and be changed.

4.3.5 Password resetting shall be performed on a periodic or random basis by the ICT personnel upon logging a call. Should the password be changes the user shall be required to fill in the Password Reset form.

4.3.6 Where possible, system software must enforce the following password standards:

- Passwords routed over a network must be encrypted.
- Passwords must be entered in a non-display field.
- System software must enforce the changing of passwords and the minimum length.
- System software must disable the user identification code when more than three consecutive invalid passwords are given within a 15 minute timeframe. Lockout time must be set at a minimum of 30 minutes.
- System software must maintain a history of previous passwords and prevent.

5. USER ACCESS RIGHTS

5.1 The municipality has different types of users on the server and all other municipal applications namely (VIP, Munsoft & Collaborator). All users on the

municipal network who has one of these applications shall have an individual password to access the system. Not all users shall have full privileges to any of the system besides the system administrator or any other nominated user as per application.

5.2 A user of information shall be expected to do the following:

- Comply with all ICT policies.
- Access information only in support of their authorized job responsibilities.
- Access information only in his/her respective departmental drive.
- Not to use another users password to access an application in the absence of the user and to keep personal authentication devices (e.g. passwords, PINs, etc.) confidential.
- Not to download and install any software.
- Adhere to the restriction of access to computers at a level which compensates the risk associated with the application to which access can be gained.

6. SOFTWARE, LISENCING & APPLICATION

6.1 Software & Licensing

6.1.1 All software acquired for or on behalf of the municipality or developed by municipality employees or contract personnel on behalf of the municipality shall be deemed municipal property and must be used in compliance with applicable licenses, notices, contracts, and agreements.

6.1.2 Only approved licensed software shall be installed and downloaded on municipal computers by the ICT personnel, the unauthorized copying of licensed and unlicensed software is prohibited. All computers shall be subject to regular reviews for unlicensed and unauthorized software.

6.1.3 Unlicensed software is illegal and not allowed on any computer in the Municipality. The Copyright Act, Act 98 of 1978 protects intellectual property against theft. If an employee uses software without a license,

the employee may be found guilty of a criminal offence. The author of the software may also seek civil damages. If an employee knows or suspects that software on computer equipment is unlicensed, the employee must contact the ICT section immediately. If employees infringe on applicable licensing and copyright laws the Municipality shall hold such employees liable for criminal or civil action.

6.2 Applications

The municipality has a variety of business applications that users need to have and depending on the nature of the job while others are compulsory to all users on the municipal network.

The applications shall be installed by the ICT section based on the completed Network Registration Form of the user.

The table below illustrates the user requirements for applications:

	MUNSOFT	COLLABORATOR	VIP	MICROSOFT OFFICE	NOD 32
Directors	✓	✓		✓	✓
Managers	✓	✓		✓	✓
Budget & Treasury	✓	✓	✓	✓	✓
All Users		✓		✓	✓
Human Resources		✓	✓	✓	✓

Some applications do not apply to all users, they are user defined.

7. ANTIVIRUS

7.1 Computer viruses are programs designed to make unauthorized changes to programs and data. Therefore, viruses can cause destruction of corporate resources. It is important to know that computer viruses are much easier to prevent than to cure. All municipal computers shall be installed an **ESET Nod32 Antivirus** software which updates daily for signature updates. Defenses against computer viruses shall include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining Virus-scanning software.

7.2 Employees shall therefore;

- Not knowingly introduce a computer virus into the municipality computers.
- Not deactivate the anti-virus software on the computer.
- Not load any other media type of unknown origin
- Not to bring unknown USB drives to the municipality without being scanned by ICT for viruses and malicious software.
- Open gaming websites and all other prohibited websites using a 3G modem.
- Do not open email attachments that you don't understand.
- Do not connect non-municipal computers on the municipal network, unless it has been scanned for viruses before loaded or executed.
- Unplug the network cable and/or IMMEDIATELY POWER OFF the workstation if it is suspected that his/her workstation has been infected by a virus and notify the ICT personnel to take corrective action.

8. WORKSTATION SECURITY

Appropriate measures shall be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including protected health information (PHI) and that access to sensitive information is restricted to authorized users.

- Restricting physical access to workstations to only authorized personnel.
- Offices containing desktops shall be locked where possible.
- Computers should be located away from environmental hazards (i.e. be careful of liquids when near electronic equipment like keyboards, laptops, printers, etc.).
- The municipality will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.
- Liquids should not be placed near or on any part of the computer.
- No smoking rules and regulations should be maintained and therefore there shall be no smoking near computers.

- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Users with laptops must be responsible for the safekeeping of the asset.
- Complying with all applicable password policies and procedures
- Ensuring workstations are mainly used for authorized business purposes.
- Securing laptops and desktops by using cable locks at all times.
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates and exit running applications and close open documents.
- Written permission to be obtained from the Asset office, in consultation with ICT section for the removal of any desktop bound equipment from the Municipality's premises (this excludes laptops allocated to individuals and authorized by Director/Manager/ICT section to carry out at any time as a tool).

9. DIAL IN AND VPN

9.1 It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Municipal internal networks via their VPN.

9.2 VPN use shall be controlled using password authentication. When actively connected to the administrative network, VPNs shall force all traffic to and from the PC over the VPN tunnel: all other traffic shall be dropped.

9.3 Dual (split) tunneling is NOT permitted; only one network connection shall be allowed.

9.4 All computers connected to Municipal's internal networks via VPN or any other technology shall use the most up-to-date anti-virus software that is the administrative standard and internal networks via VPN must have the latest operating system security patches applied.

9.5 Peer-to-peer software shall not be allowed over VPN. Computer with multiple user accounts (ie true multiuser hosts) shall not be allowed to create VPN connections to the trusted network for the entire host and its users.

10. INTERNET AND E-MAIL SECURITY

10.1 Personal Use:

As with any Municipality provided tool of work, the use of electronic mail services shall be dedicated to legitimate Municipality business and shall be governed by rules of conduct similar to those applicable to the use of other information technology resources.

10.1.1 Access to e-mail services is declared a privilege which imposes certain responsibilities and obligations on users and is subject to government policies and laws.

10.1.2 Acceptable use of e-mails must be legal, ethical, reflect honesty, show restraint in the consumption of shared resources and demonstrate respect for intellectual property, ownership of information, system security mechanisms, and the individual's rights to privacy and freedom from intimidation, harassment and unwarranted annoyance.

10.2 All E-mail users shall:

- comply with Municipality policies, procedures, and standards;
- protect other's privacy and confidentiality;
- be responsible for the use of their e-mail accounts; and
- be information technology resources efficiently and productively.
- have an official assigned electronic signature of the employee, which consist of the full name, position, departmental section, office number, mobile number, municipal logo, HIV logo and email address.

10.2.1 Users shall be courteous and abide by accepted standards of etiquette rules as which include but not limited to the following:

- Being polite.
- Using appropriate language.
- Refraining from revealing personal particulars about themselves or other Users to anyone else on the Internet.
- Refraining from revealing credit, credit checking accounts or identification numbers across the Internet.

- Attempting to gain illegal access to system programs or computer equipment.
- Using all appropriate precautionary measures to detect viruses and if necessary, prevent its spread.

10.3 Prohibited Use:

Creation, transmission, receipt or storage of certain content may be in violation of regulatory and statutory requirements and shall therefore be prohibited within the Municipality. This content shall includes, but not limited to the following:

- Threats.
- Pornographic or sexually explicit material.
- Material containing derogatory racial, gender, religious or hate-oriented comments.
- Libellous remarks about products or other companies.
- Defamatory remarks, including defamation of character.
- Discriminatory language or remarks that would constitute harassment of any type.
- Any other comment that offensively addresses someone's age, sexual orientation, political beliefs, national origin, or disability.

To ensure bandwidth is not abused the following is prohibited:

- Causing congestion on the network by distribution of, chain letters, jokes, bitmaps and applications that add no value to the business.
- Broadcasting unsolicited commercial e-mail (Junk e-mail or "Spam") to mailing lists.
- Sending inappropriate messages to groups or individuals, and spreading broadcasts without permission of the ICT section or Municipal Manager.

10.4 General Considerations

- E-mail accounts, and the e-mail messages contained within these accounts, are important to the business functions of the Municipality. As such, the messages and e-mail accounts are the property of the

Municipality and will be managed by the Information Technology Section. In the event of any employee termination, the employee's e-mail account shall remain with the Municipality. All messages may be reviewed and redirected to the employee's successor or otherwise deleted, as appropriate.

- Users are prohibited from sending a message to someone else from another user's account
- All official email must have an official signature on the bottom of the mail.
- Users must ensure that their "out of office" reply is activated when they are away for a day or more if they will not have access to a computer.
- The size of e-mails may not exceed 5Mb (Megabyte).
- Internet/E-mail users shall be held personally responsible for all activity conducted under his/her user ID and password.

10.5 Unacceptable use:

Employees shall not use the Internet or e-mail for purposes that are malicious, illegal, unethical, harmful to the municipality (including statements, actions or omissions that do, or could, lead to civil and/or criminal liability to the municipality or damage or loss to the municipality or its reputation) or fellow employees.

10.5.1 Employees shall not:

- Receive, store, download, print, distribute, send or access any content or material that is offensive, harassing, fraudulent, racist, illegal or obscene (including any form of pornography).
- Participate in e-mail "chain letters" or unsolicited e-mail ("spam"), for example, email messages containing instructions to forward the message to others where not for official or municipality business purpose.
- Send or forward joke e-mails, electronic greeting cards, Christmas cards, copyrighted music files (e.g. MP3), copyrighted video clips (not related to official business) and games that can

negatively impact on the overall performance of the municipality's communication resources.

- Represent personal opinions as that of the municipality via e-mail or publication of unauthorised statements onto web sites, bulletin boards, discussion areas or newsgroups.
- Modify an e-mail message and forwarding or replying therewith without noting the changes, i.e. deletions, removal of recipients or modification of content.
- Send, reply to or forward e-mail messages or other electronic communications which hides the identity of the sender or represents the sender as someone else.
- Use information, e-mail, files, downloads or data to commit fraud or any other criminal offence/s.
- Conduct a personal business using municipality resources.
- Transmit confidential information to any person not authorised to receive it.
- Conduct any form of a campaign that may be considered as damaging against fellow employee/s or any third party by e-mail or by any other electronic means.
- Use third party e-mail providers, i.e. "Hotmail", "Yahoo mail", "Free mail" or any other e-mail service provided by an outside Internet Service Provider or party, to send municipality information or any files emanating from within the municipality to external parties.
- Use a modem whilst connected to the municipality's internal network. Under no circumstances shall a modem be allowed to when a workstation or laptop is connected directly to the municipality's network, thereby bypassing existing security mechanisms.

11. INTELLECTUAL PROPERTY

All information developed by or for the Municipality remains the property of Ephraim Mogale Local Municipality.

12. ASSETS MANAGEMENT

All involved systems and information remain the assets of municipality and are expected to be protected from misuse, unauthorized manipulation, and destruction. These protective measures may be physical and/or software based as stated in the ICT Global Policy.

13. INFORMATION SECURITY

Information Security activities concerns the protection of Information from unauthorised use or accidental modification, loss or release and is based on the following five elements:

- **Confidentiality** - ensuring that Information is only accessible to those with authorised access.
- **Integrity** - safeguarding the accuracy and completeness of Information and processing methods.
- **Availability** - ensuring that authorised Users have access to Information when required.
- **Compliant Use** - ensuring that every user meets all legal and contractual obligations.
- **Responsible Use** - ensuring that appropriate controls are in place so that Users have access to accurate, relevant and timely Information but that Users of Ephraim Mogale Local Municipality ICT resources do not adversely affect other Users or other Systems.

14. INFORMATION AND COMPUTER CONTROL

- Appropriate control mechanisms (e.g. Username and password) will be in place for authenticating access to all Information Systems and Information Assets. Access control must be in accordance with the security policy.
- Access granted to Third Party shall take into account the risks involved, with adequate controls put in place to protect the municipality's Information (e.g.

the most limited access rights in the system as possible in order to carry out the work).

- Remote access to Restricted Information Systems will only be provided by ICT section with the explicit authorization.
- All users have shared drives as per department, no user has access to a different drive in the network rather that the department that the user is placed in.
- Users must save all the municipal official data in the server/network as the user has declared when completing and signing the Network Registration Form.

15. PHYSICAL AND HARDWARE SECURITY

14.1 Adequate security shall be provided to ensure the protection of the physical ICT equipment.

14.2 Physical access to the ICT environment and sensitive areas shall be restricted in order to protect the confidentiality, integrity and availability of information systems, information and resources.

14.3 The ICT environment and sensitive areas shall be protected from damage from any relevant natural or other disaster including but not limited to, fire, flood and explosion.

14.4 Sensitive areas include but not limited to computer operations areas, air conditioning, power control panels and supply, network facilities, risers, tape and disc libraries, remote sites, back-up sites, transport facilities and storerooms etc. These requirements apply in the municipal ICT environment and where ICT environments is managed by an external service provider.

14.4.1 Municipal employees shall ensure the following:

- Other hazards to hardware such as food, smoke, liquids, high or low humidity and extreme heat or cold is avoided.
- No equipment installations, disconnection, modifications, and relocations are done without the permission of the ICT Supervisor.
- No portable equipment such as laptop computers are removed out of the office without the informed consent of the

department's Director and the IT Supervisor. (Informed consent means that the manager knows what equipment is leaving, what data is on it and for what purpose it will be used).

- Care is taken to safeguard the valuable electronic equipment assigned to them. (employees who neglect this duty shall be accountable for any loss or damage that may result).
- Under no circumstance connect any other equipment to the municipality's network without prior, written approval by the ICT section.

16. SITE SECURITY

The physical work environment, the service area and the building perimeter shall have adequate facilities and access controls to prevent damage, interference and unauthorised physical access where confidential information or systems are kept.

15.1 Physical Access:

15.1.1 Physical access to the ICT environment and sensitive areas must be restricted and granted only to authorised ICT personnel by signing registration access form with the need to access those areas in accordance with their responsibilities in the course of their duties, and taking into account relevant health and safety regulations and standards.

15.1.2 Access to physical and sensitive areas by third parties, including vendors, visitors and maintenance personnel is restricted and strictly controlled, only accessible through granted authorised ICT personnel.

17. REMOVAL OF ICT PROPERTY

The municipal ICT equipment, information or software shall not be taken off-site without appropriate authorization from the ICT section. Where appropriate, removal and subsequent return of ICT property shall be logged and noted in the ICT Files.

18. CLEAR DESK POLICY

When not in use, printouts containing sensitive information shall be locked away in suitable security furniture, preferably in a lockable drawer, cabinet or safe and with the key removed from the lock and appropriately secured. Printouts containing sensitive

information must be cleared from printers immediately. Care must also be taken with printed information around photocopiers and facsimile machines.

19. USER DEREGISTRATION (DISABLING, SUSPENSIONS)

It is important that the Human Resource Department notifies the ICT section concerning the suspensions, transfers and termination of employment at any circumstances that may occur.

18.1 Post-employment:

Procedures for ensuring hardware and information security during the separation of employees from termination, transfer or suspension; Human Resources shall accordingly notify ICT section of the terminated, transferred or suspended personnel via confirmation of e-mail to the ICT section (Supervisor/Manager). The necessary arrangement shall be done with the department on limitation of some functions on applications during the notice period given by the user. Then the user shall be disabled for 60 days, after which the user shall be deleted from the municipal server.

20. VIOLATIONS

Unintentional or intentional violations of security policies and procedures must be subject to appropriate remedial advice and training, or disciplinary action according to Ephraim Mogale Local Municipality human resources policies and procedures. Users who deliberately or repeatedly violate security provisions shall have their access privileges suspended until the appropriate remedial action has been determined.

21. POLICY VIOLATION

A Formal Incident Response will be followed in the event of any breaches of security with the view to providing appropriate outcomes based on the risk and/or impact. Action to correct and recover from security breaches shall be defined in a way that will ensure the following:

- only authorized Users are allowed access to ICT systems and data; emergency action is reported to management; and

- the integrity of the municipal systems and security controls is confirmed with minimal delay.

22. COPYRIGHT VIOLATIONS

Users who install, store or use illegal, unapproved or copied software shall be subject to appropriate disciplinary action.

23. COLLECTION OF EVIDENCE

22.1 Appropriate processes must be followed to ensure that adequate evidence is available in support of actions against a person or organisation, and that the quality and completeness of such evidence is maintained.

22.2 All Users shall be made aware of the procedures for reporting an incident and be required to report any observed or suspected incidents as quickly as possible to the ICT section. A formal reporting procedure shall be established together with an incident response procedure.

22.3 Compliance with this policy is mandatory. Each user must understand his/her role and responsibilities regarding information and hardware security issues, and protecting the municipality's information assets. Any compromise or suspected compromise of this policy must be reported to the ICT Department.

22.4 Failure to comply with this policy and all supporting policies, standards and guidelines may lead to the instigation of the relevant disciplinary procedures and, in certain circumstances, legal action.

24. IMPLEMENTATION

The policy become effective upon approval, and shall be reviewable on a need basis.