MANGAUNG

AT THE HEART OF IT ALL

METRO MUNICIPALITY
METRO MUNISIPALITEIT
LEKGOTLA LA MOTSE

ICT SECURITY MANAGEMENT POLICY

14 MAY 2020

INDEX

DOCUMENT AND VERSION CONTROL

Description	**INFORMATION COMMUNICATION TECHNOLOGY** **ICT SECURITY MANAGEMENT POLICY**		
Purpose	The Information and Communications Technology (ICT) Division has the mandate to deliver services, support and maintain ICT infrastructure, for the Mangaung Metropolitan Municipality to realise its mandate. The plan of action to direct and enforce Security, in a controlled manner, to meet required levels of service. Provide direction and enforcement for Security monitoring & direct control of pre-emptive measures in accordance with International IT Security Processes.		
Applicable to	*Information Communication Technology Sub Directorate*		
Supersedes	*N/A*		
Document Owner	*ICT Security Administrator*	**Owner Org**	*ICT - MMM*
Effective Date	Upon approval	**Revision Date**	

VERSION HISTROY			
VERSION	**DATE**	**AUTHOR(S)**	**CHANGE SUMMARY**
1.0	1 February 2018	Wynand Bezuidenhout	Initial Document
1.1	20 April 2020	Wynand Bezuidenhout	Initial Document
2.0	14 May 2020	Alfred Jenkinson Wynand Bezuidenhout David Nkaiseng	Update DRAFT with requests by HOD and submit reviewed document.

1. MANDATE OF THE ICT DIRECTORATE

The Information and Communications Technology (ICT) Division has the mandate to deliver services, support and maintain ICT infrastructure, for the Mangaung Metropolitan Municipality to realise its mandate.

2. OBJECTIVE OF THE POLICY

This policy has the following objectives:

a) To protect the Mangaung Metropolitan Municipality's information by safeguarding its confidentiality, integrity and availability.
b) To establish safeguards to protect the information resources from theft, abuse, misuse and any form of damage.
c) To establish responsibility and accountability for Information Security in the Mangaung Metropolitan Municipality.
d) To encourage management and employees to maintain an appropriate level of awareness, knowledge and skill to allow them to minimise the occurrence and severity of Information Security incidents.
e) To provide suitable coverage of International Standards ISO 17799 and related information security best practices.

3. APPLICABILITY OF THE POLICY

This policy applies to all employees of the Mangaung Metropolitan Municipality, including Contractors and Consultants, who use ICT services and assets.
This policy is supported by a range of security controls documented within operating procedures, technical controls embedded in information systems and other controls that will be advised to employees from time to time by ICT Division through information security standards, procedures and guidelines.

4. TERMS AND DEFINITIONS

- **GOVERNANCE**

  The mechanisms an organisation uses to ensure that its constituents follow its established processes and policies. It is the primary means of maintaining oversight and accountability in a loosely coupled organizational structure. A proper governance strategy implements system to monitor and record what is going on, takes steps to ensure compliance with agreed policies, and provides for corrective action in cases where the rules have been ignored. (http://looselycoupled.com/glossary/governance)

- **INCIDENT**

  Any event which is not part of the standard operation of a service which causes, or may cause, an interruption to, or a reduction in, the quality of that service

- **STANDARD**

Guideline documentation that reflects agreements on products, practices, or operations by nationally or internationally recognised industrial, professional, trade associations or governmental bodies.

- **SYSTEM**

  An integrated composite that consists of one or more of the processes, hardware, software, facilities and people, that provides a capability to satisfy a stated need or objective (ISO12207, 1995:5)

- **USER**

  An individual utilising Information Systems to achieve the business goals required to realise the mandate.

5. ACRONYMS

- **COBIT:** Control Objectives for Information Technology
- **ICT:** Information and Communication Technology
- **ICTSC:** Information and Communication Technology Steering Committee
- **ITIL:** Information Technology Infrastructure Library

6. REFERENCES

6.1 INTERNATIONAL GUIDELINES

- Control Objectives for Information Technology (COBIT)

6.2 INTERNATIONAL STANDARDS

- Information Technology Infrastructure Library (ITIL)
- ISO/IEC 17799: Edition 1, 2000 – Information Technology – Code of practice for Information Security Management

6.3 NATIONAL POLICY

- Constitution of the Republic of South Africa, Act 108 of 1996
- The Electronic Communications and Transactions (ECT) Act 25 of 2002
- National Strategic Intelligence Act 2 of 2000 applicable for South Africa
- Regulation of Interception of Communications Act 70 or 2002
- State Information Technology Act 88 of 1998

7. PRINCIPLES

7.1 This policy addresses the associated risks to the information assets and includes risks such as:

a) Uncontrolled access, connections, and unintentional user errors
b) Security of the information systems compromised by unsupported business practices
c) Ensuring the integrity and validity of data
d) Poor operating procedures
e) Malicious code and viruses
f) Uncontrolled system or data changes
g) Internet and public domain access
h) Breach of legislation or non-compliance with regulatory or ethical standard

7.2 The implemented controls shall be reviewed annually or if the need arises and adjusted where necessary.

8. APPLICATION & INFORMATION SECURITY POLICY STATEMENTS

This section contains formal policy requirements each followed by a policy statement describing the supporting controls and supplementary guidance.

8.1. INFORMATION SECURITY

- Roles and responsibilities for information security governance shall be identified and a Risk Committee shall be established.
- Third parties will be identified and managed in accordance with a legal contract to ensure that no unauthorised access is gained to the Mangaung Metropolitan Municipality – both logically and physically.
- Senior Management Commitment to Information Security: Senior management should fully support and commits to the enforcement of all aspects of security throughout the Mangaung Metropolitan Municipality.

8.2 SECURITY OF APPLICATIONS BY USE OF ANTIVIRUS

- Mangaung Metro automatically installs Anti-Virus / anti-malware software protection on all employees' computers when getting setup and connected onto the Municipal Network with an official computer or device.
- When infected computers are discovered through routine scanning processes, or reported to the Office of Information Technology, managers, or owners, will be given until 17:00p.m. that day to correct the problem or remove the computer from the network.
- ICT will remove network access if the problem has not been corrected and reserves the right to remove any infected computer at any time should security of Mangaung data or networks be compromised.
- Any person found to have violated this rule will be subject to appropriate disciplinary action as defined by current Metro policy, employee code of conduct, and/or collective bargaining agreements. This rule will not supersede any Mangaung Metro developed policies but may introduce more stringent requirements than the current ICT policy.

8.3 PATCH MANAGEMENT PROCESSES

a) Patching is a process to repair a vulnerability or a flaw that is identified after the release of an application or a software. Newly released patches can fix a bug or a security flaw, can help to enhance applications with new features, fix security vulnerability.
b) Unpatched software can make the device a vulnerable target of exploits. Patching a software as and when the patch is released is critical to deny malware access.
c) Patch management is the process that helps acquire, test and install multiple patches (code changes) on existing applications and software tools on a computer, enabling systems to stay updated on existing patches and determining which patches are the appropriate ones. Managing patches thus becomes easy and simple.
d) Patch Management is mostly done to fix problems with the different versions of software programs and to help analyse existing software programs and detect any potential lack of security features or other upgrades.
e) Patch management process features to detect missing patches, install the patches or hotfixes that are released from time to time, and provide instant updates on the latest patch deployment status.
f) Patch management enable all the computers to remain up to date with the recent patch releases from the application software vendors. It is critical to take necessary steps to enhance the security posture of enterprises – large and small. Therefore, consistent patching of operating systems and applications with an automated patch management solution is important to mitigate and prevent security risks.

g) Stages of the patching process

- Scan the applications of devices for missing patches
- Automate the downloading of missing patches that are released by the application vendors.
- Automated Patch Deployment ensures to automatically deploy patches based on the deployment policies, without any manual interference.
- Once the patches are deployed, reports on the status of the automated patch management tasks are updated.

h) Patch Management Best Practices

- Understanding the importance of patch management: Knowing why patch management is an important aspect of cybersecurity solution is critical. Quick response to latest patch updates would deny and protect vulnerable systems from zero-day threats.
- Outcome of delayed patch application: Delayed patch application creates a severe impact causing major security breaches. The latest Wannacry attack revealed the vulnerability of not updating the software with patch fixes. The victims of Wannacry were those who delayed in updating the patch released by Windows to fix the SMB v1 protocol vulnerability – this resulted in loss of data, and business.

- Availing the services of managed service providers: Managed service providers offer patch management software to fit the requirements of the business – big or small. MSPs take full control of the patch management process – while the businesses can focus on the management and revenue-generating aspects.
- Deploying patch testing: Some patches are incompatible with certain operating systems or applications and leads to system crashes. It is good for IT admins, to run a patch test before the patches are deployed on to the endpoint systems.

i) Patch Management Life Cycle

- Update vulnerability details from software vendors
- Scan the enterprise network for vulnerability
- Examine the Vulnerability and identify the missing patches
- Deploy patches and validate patch installation
- Generate Status Report on the latest patch updates

j) Patch Management for Cyber Security

- Software vendors release patches to fix vulnerabilities identified after the release of a software or application. Patch Management enables patch testing and deployment which is a critical aspect of cyber security. Quick and instant responses to patch updates would mitigate the chances of data breaches that can cause due to unpatched software.
- Identify which endpoints contain vulnerabilities and need to be patched
- Create policies to automatically apply updates to groups of tagged endpoints at scheduled times
- Remotely deploy operating system updates for Windows and Linux machines
- View dashboard statistics for breakdowns of available updates for endpoint machines.
- Identify which endpoints contain vulnerabilities and need to be patched
- Create policies to automatically apply updates to groups of tagged endpoints at scheduled times
- Remotely deploy operating system updates for Windows and Linux machines
- View dashboard statistics for breakdowns of available updates for endpoint machines

k) Patch-Compliance Review Procedure

- The IT Security team will generate and review patch management/compliance reports on at least a monthly basis from the company vulnerability management tools.

- In reviewing the patch reports, The IT Security team will identify unpatched machines that connect to the company network and either patch or define an exception.
- IT security will conduct an external vulnerability scan on at least a monthly basis using Nessus to identify known and potential vulnerabilities with the publicly facing system. Vulnerabilities will be brought to the attention of the system/application administrator(s) for mitigation.

8.4 PASSWORD MANAGEMENT AND CONFIGURATIONS

Security Configuration	**Setting**
Password Policy - General User Accounts	
Minimum password length	8 characters
Maximum password age	30 days
Password history	6 passwords remembered
Password complexity	Enabled
Password Policy - Administrative/Super User Accounts	
Minimum password length	12 characters
Maximum password age	30 days
Password history	12 passwords remembered
Password complexity	Enabled
Account Lockout Policy - General User Accounts	
Account lockout duration	60 minutes
Account lockout threshold	3 attempts
Account lockout counter threshold	30 minutes
Account Lockout Policy - Administrative/Super User Accounts	
Account lockout duration	60 minutes
Account lockout threshold	3 attempts
Account lockout counter threshold	60 minutes
Audit Policy	
Account logon events	Failure
Account management	Success, Failure
Logon events	Failure
Policy change	Success, Failure
Privilege use	Success, Failure
System events	Failure
Event Logs	
Application Log: Maximum log size (KB)	32 768
Application Log: When maximum event log is reached	Overwrite events as needed
Security Log: Maximum log size (KB)	81 920
Security Log: When maximum event log is reached	Overwrite events as needed
System Log: Maximum log size (KB)	32 768

System Log: When maximum event log is reached	Overwrite events as needed
Additional Settings	
Screen saver	Enable
Screen saver: Wait	10 minutes
On resume, display logon screen	Enabled
Accounts: Rename administrator account	Not Administrator or admin
Accounts: Rename guest account	Not Guest
Accounts: Guest account status	Disabled
Windows Firewall: Firewall state (Domain)	Enabled (1)
Windows Firewall: Firewall state (Private)	Enabled (1)
Windows Firewall: Firewall state (Public)	Enabled (1)

8.5 MANAGEMENT PROCESS FOR PRIVILEGED USERS

8.5.1 USER ACCESS RIGHTS ASSIGNMENT

a) Access must follow a **"PRINCIPLE OF LEAST-PRIVILEGE"** approach, whereby all access is revoked by default and users are only allowed access based on their specific requirements.
b) Access rights include, but are not limited to:

- General office applications (E-mail, Microsoft Office, SharePoint, etc.);
- Department specific applications and/or databases;
- Network Shares;
- Administrative tasks;
- RAS/VPN Access;
- Wi-Fi; and BYOD.

c) The levels or degrees of access control to classified information must be restricted in terms of legislative prescripts.
d) Access rights must be assigned to a group/role. A user must then be assigned to that group. Access rights must not be assigned to individual users.

8.5.2 USER PERMISSION / ROLE CHANGE REQUEST

a) A formalised user access management process must be implemented and followed in order to adjust user access rights.
b) All user access change requests must be formally documented, along with their access requirements, and approved by duly authorised personnel.

c) Access must only be granted once approval has been obtained by the respective line manager.
d) User access change requests must be obtained from HR on change of an employee's role or permissions. The template for this type of request can be found attached to this policy in Annexure B. The form must be sent to the service provider/line manager for access requirements to be signed off. Once the access requirements have been signed off, the form must then be sent to the ICT department for approval and adjustment of employee's access rights based on specified requirements. The form must then be sent back to HR for record keeping purposes. Records of user access granted and removed must be stored for a minimum of 10 years.
e) User access rights that are no longer required must be removed immediately.

8.5.3 NETWORK USER ACCESS RIGHTS ASSIGNMENT

a) Access to the Municipality's network must only be allowed once a formal user registration process has been followed.
b) Access to Wi-Fi must only be provided to users who require access to the network throughout the Municipality, to fulfil their business function.
c) RAS/VPN access must only be granted to users who require the service to fulfil their business function.
d) Best practice states that RAS access must only be granted to employees who require remote access to a system in order to administer the environment.
e) Best practice states that VPN access must only be granted to employees who:

    ☑ Work remotely (Not at the office);
    ☑ Work overtime, or not within regular office hours.

f) It is the responsibility of the ICT Steering Committee to ensure all users must be made aware of the security risks and obligations associated with RAS/VPN access.
g) RAS/VPN access must be monitored, and audit logs reviewed every quarter (3 months) by system administrators.
h) All reviews must be formally documented and signed off by the ICT Manager. Documentation must be kept for record keeping purposes. Records of RAS/VPN access reviews must be stored for a minimum of 10 years.
i) The ICT Manager must approve all hardware and software, owned by Municipal employees and service providers/vendors, if it is to be used for official purposes (BYOD).
j) The ICT team must ensure that all mobile devices must be protected with a PIN.

8.5.4 OPERATING SYSTEM ACCESS RIGHTS ASSIGNMENT

a) Each system administrator must be given their own accounts within the administrator group. Should share accounts be required to fulfil a business function, then this account must be approved and documented by the Risk Management Committee.
b) The default administrator account must be renamed, and a password must be randomly generated and sealed in an envelope and kept in a safe.
c) The default guest account must be removed or renamed and disabled.

8.5.5 APPLICATION USER ACCESS RIGHTS ASSIGNMENT

a) Segregation of duties must be practiced, in such a way that application administrators cannot perform general user tasks on an application. This is to prevent any fraudulent activity from taking place.
b) Applications administrators must remain independent of the department utilising the application, apart from the ICT department.

8.5.6 DATABASE USER ACCESS RIGHTS ASSIGNMENT

a) The ICT Manager must limit full access to databases (e.g. sysadmin server role, DB owner database role, sa built-in login etc.) to ICT staff who need this access. Municipal employees who use applications may not have these rights to the application's databases.
b) The ICT Manager must ensure that Municipal employees who access databases directly (e.g. through ODBC) only have read access.
c) The ICT Steering Committee must approve all instances where Municipal employees have edit or execute access to databases.
d) The ICT Manager must review database rights and permissions on a quarterly basis (every 3 months). Excessive rights and permissions must be removed.

8.5.7 REVIEWING USER ACCESS AND PERMISSIONS

a) User access and user permissions must be reviewed every quarter (3 months) by system administrators.
b) On a monthly basis, HR must send a list of all terminated employees for that month to the ICT department. This list must be used to ensure that all terminated users have had their access revoked. Should one or more terminated users still have access to the environment, and investigation into the finding must be conducted.
c) On a monthly basis, the ICT Manager must review all users with administrative access to the environment and assess their rights for appropriateness. Should a user be found with excessive rights, a user access change request must be performed.
d) All reviews must be formally documented and signed off by the ICT Manager. Documentation must be kept for record keeping purposes. Records of user access review must be stored for a minimum of 10 years.

8.5.8 TERMINATED USER REMOVAL

a) A formalised user termination process must be implemented and followed in order to revoke access rights.
b) All user termination requests must be formally documented and approved by duly authorised personnel. Access must be disabled immediately, with accounts being removed after 6 months once authorisation has been obtained by line manager.
c) Terminated user requests must be obtained from HR on the termination of an employee. The template for this type of request can be found attached to this policy in Annexure B. The form must be sent to the service provider/line manager for access revocation to be signed off. Once access revocation has been signed off, the form must be sent to the ICT department for approval and deactivation of employee based on specified requirements. The form must then be sent back to HR for record keeping purposes. Records of user access removal must be stored for a minimum of 10 years.

8.5.9 USER AND ADMINISTRATOR ACTIVITY MONITORING

a) User and administrator activity must be monitored through audit and event logging.
b) Once a month, system administrators and application owners must review audit and event logs for suspicious and malicious activities. A template for the reviewing of audit logs can be found in Appendix D of this Policy.
c) Dormant accounts should be disabled and a request to remove the access should be performed in line with section 11. User Permission/Role Change Request.
d) All reviews must be formally documented and signed off by the ICT Manager. Documentation must be kept for record keeping purposes. Records of user activity monitoring must be stored for a minimum of 10 years.

8.6 ASSET MANAGEMENT

- All physical and information assets shall be classified according to their criticality to the Mangaung Metropolitan Municipality, enabling an appropriate level of protection. Assets will be handled in line with its identified criticality.
- Information Asset Owners shall be identified and held accountable for the protection of assets under their authority.

8.7 EMPLOYEE SECURITY

- Security education, training and awareness programmes will be conducted to ensure that employees are aware of security threats and concerns and are always equipped to apply the security principles. The employees should follow the security guidelines below

CYBER SAFETY TIPS PROTECT YOURSELF AGAINST CYBER ATTACKS OR THREADS

SOFT WARE UPGRADES

- Update your software and operating systems on your personal phone and other gadgets: This means you benefit from the latest security patches. ICT will update your workplace operating systems and soft ware

UNTI-VIRUS AND SECURITY SOLUTIONS

- Use anti-virus software: There are several security solutions that will detect and remove threats. Ensure that your personal gadgets have at least one of security solutions. Keep your software updated for the best level of protection. All municipal gadgets have cyber security solutions.

PASSWORDS

- Use strong passwords: Ensure your passwords are not easily guessable and don't give those to anyone. Do not share your passwords with others except authorised ICT support practitioners. Change your password immediately thereafter sharing it with ICT support practitioners. ICT sub directorate has measures in place to disable your password once every month, to enable you to create new one. If your password is not disabled after a month, please report this to ICT and create a new password.

INTRUDERS AND SUSPICIOUS EMAILS

- Do not open email attachments from unknown or suspicious senders: These could be infected with malware.
- Do not click on links in emails from unknown senders or unfamiliar websites: This is a common way that malware is spread.
- Where possible switch off your Bluetooth or linking capabilities to other gadgets when in public places

WI FIs

- Avoid using unsecure WIFI networks in public places: Unsecure networks leave you vulnerable to man-in-the-middle attacks.

ONLINE MEETINGS

- If you are invited to participate in the online meeting platform not officially recognised by the municipality, apply utmost care and be on the lookout for intruders or suspicious software or communication.
- If there is a suspicious foreign intrusion during online meetings, you are advised to withdraw from the meeting until the thread is cleared by ICT. Constantly check online meeting participants and where necessary identify intruders and raise this with the meeting organiser.
- When participating in an online meeting do not allow an uninvited person to be closer to the devise you use for such meeting. Try to participate in the meeting from a private or secure environment in the workplace or at home.
- Where possible, you are encouraged to disable your Bluetooth or other device linking capabilities in if you are participating in an online meeting whilst you are in a public or crowded place

PERSONAL DETAILS

- Do not share your municipal sensitive and private information such as Identity Number, residential address, banking information to suspicious SMSs, emails and calls.

8.8 PHYSICAL AND ENVIRONMENTAL SECURITY

- Physical and environmental controls shall be in place to protect the Mangaung Metropolitan Municipality and its supporting information processing facilities from unauthorised access, intentional or accidental damage or interference.

8.9 COMMUNICATIONS AND OPERATIONS MANAGEMENT

- All operational procedures shall be documented and implemented to ensure correct and secure operations in the Mangaung Metropolitan Municipality and its supporting information processing facilities, communication facilities and networks. Exchange of information will be managed to prevent the loss, modification or misuse of information.
- All breaches of security shall be reported and managed accordingly.

8.10 ACCESS CONTROL

- Access (both locally and remotely) to computers, systems and networks shall be granted in line with requirements. This access will be managed and monitored to ensure that no unauthorised access is gained. The use of mobile computing facilities will be managed to ensure protection of these facilities.

8.11 DISASTER RECOVERY MANAGEMENT

- Business continuity management plans and procedures shall be established and maintained to facilitate the normal functioning of critical business activities in the event of failures or disasters.

8.11 DATA CLASSIFICATION

- Sensitive information: Information in this category may not be distributed without consideration of its sensitive nature.

- Private information is personal information, including personal intellectual property, which is accessible only by its owner and those to whom the owner directly entrusts it, except under exceptional circumstances. Examples: Intellectual property, email;

- Confidential information is Mangaung Metropolitan Municipality information normally handled in the same manner as private information but may be accessed by other authorised employees under limited additional circumstances. Examples: ID number, date of birth, medical records, education record, financial record;

    - Internal information is Mangaung Metropolitan Municipality information that is intended for distribution within the Mangaung Metropolitan Municipality.

- Public Information: Information in this category is distributed without restriction. Examples: Marketing materials, Mangaung Metropolitan Municipality website

- Top Secret: shall be applied to information, the unauthorised disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security. Example: Compromise of complex cryptologic and communications intelligence systems.

- Secret: shall be applied to information, the unauthorised disclosure of which reasonably could be expected to cause serious damage to the national security. Example: Revelation of significant intelligence operations.

8.12 INFORMATION HANDLING

- Unauthorised disclosure of sensitive information is prohibited.
- Unauthorised tampering or alteration of sensitive information is prohibited.
- Unauthorised destruction or disposal of sensitive information is prohibited.
- Laws and policies governing information retention must be complied with.
- When confidential information is being transported or stored, it must be protected from unauthorised disclosure, modification, or destruction.
- When possible, confidential information must be protected with enough publicly vetted encryption algorithms while in transit and at rest.
- If encryption is not possible appropriate compensating controls must be considered and implemented.
- Before access is granted to confidential information, a signed non-disclosure agreement must be on file for that individual or organisation.
- When appropriate, criminal and reputational background checks must be conducted.
- Confidential information being transported to or stored with a third party outside of the Mangaung Metropolitan Municipality network or physical premise must be approved by the Information Owner.
- Confidential information, both digital and physical, must be disposed properly to prevent unauthorised disclosure.

8.13 IDENTITY AND ACCESS

- Anonymous identities should be avoided and are prohibited when accessing confidential information unless an exception is granted by the Information owner.
- Information users will be given the minimum level of access to systems and information that their duties require.
- Human Resources Management division must report change of an employee employment status or role to ICT.
- Remote access to the network or systems is will be strictly granted and monitored

- Passwords, passphrases, and private keys (physical and private digital) must be protected and may not be shared.

8.14 INFORMATION COMPROMISE

- Should it be suspected that "sensitive" data has been accessed by an unauthorised party or has been used improperly by an authorised party, then the discovering individual must report the incident immediately to ICT Division.
- Should a password, passphrase, or key be believed to have been compromised, it must be changed immediately. If that password authorises access to sensitive information, the incident must be reported to ICT.

8.15 ICT INFRASTRUCTURE

- Unauthorised eavesdropping, redirection, sniffing, and tapping of network traffic or systems is prohibited.

    - ICT infrastructure must be protected from theft, intrusion, malicious code, and abuse.
    - ICT infrastructure must be regularly patched for security and stability.
    - Locations that house digital and paper copies of confidential data must have appropriate physical preventative, detective, and deterrent controls.
    - ICT infrastructure must be reinforced with appropriate redundancy, backup, and disaster recovery plans and technologies.
    - A “defence in depth” or layered security strategy must be applied to information, network, and system architecture and design whenever possible, especially pertaining to sensitive information.

8.16 ASSESSMENT AND COMPLIANCE

- Risk assessments must be regularly conducted to reveal security posture, and to identify vulnerabilities and weaknesses in software, infrastructure, policy, procedure and practices
- Employees must participate in information security awareness that will be provided by the ICT.
- Controls shall be in place to ensure compliance with legal, legislative, regulatory or contractual obligations and any other security requirements.

9. ROLES AND RESPONSIBILITIES

9.1 THE RISK COMMITTEE SHALL:

a) Ensure that the necessary information security controls are implemented and complied with as per this policy

9.2 THE ICT DIVISION SHALL:

a) Approve and authorise information security procedures
b) Ensure that all users are aware of the applicable policies, standards, procedures and guidelines for information security.
c) Ensure that policy, standards and procedural changes are communicated to applicable users and management.
d) Evaluate information security potential risks and introduce counter measures to address these risks.
e) Revise the information security policy and standards for effective information security practices.
f) Facilitate and coordinate the necessary information security procedures within the Mangaung Metropolitan Municipality.
g) Report and evaluate changes to information security policies and standards
h) Coordinate the implementation of new or additional information security controls.
i) Review the effectiveness of information security measures and implement remedial controls where deficits are identified.
j) Coordinate awareness strategies and rollouts to effectively communicate information security mitigation solutions.

10. POLICY COMPLIANCE

a) Violation of this policy may lead to restriction of access to the ICT facilities or disciplinary action.
b) Any damage, security breach or loss of information which can be deemed to have been caused by negligence or intention on the part of the user or any identified individual will be the responsibility of that user or that individual. The penalty, thereof, will be determined by the Mangaung Metropolitan Municipality disciplinary process.
c) The Mangaung Metropolitan Municipality may use any legislation relevant to the usage or protection of Information Systems (or information), in prosecuting the person who has violated this policy.

11. POLICY REVIEW

This policy shall be reviewed on an annual basis by the ICT Division to:

a) Determine if there have been changes in International, National or Internal references that may impact on this policy.
b) Determine if there are improvements or changes in the ICT process that should be reflected in this policy.