ICT-05-24

ICT Security Policy

Document Name: ICT Security Policy

Policy Number: ICT-005

Version: 003

Date Issued: May 2024

Document Information

Policy	ICT Security Policy
Version	003
Policy Code	ICT-005
File Name	POL-ICT-05-2024 ICT Security Policy.doc
Date Issued	May 2024
Policy Enforcer	ICT Manager

Table of Contents

I. Acronyms and Abbreviations

4G	Fourth Generation
ICT	Information Communication Technology
IS SBU	Information Communication Technology Sub Business Unit
IS Manager	Information Communication Technology Manager
VPN	Virtual Private Network

II. Definitions

Third Generation (3G) Networks: Mobile technology and standard used to access the Internet.

Accountability: ensuring that the actions of an entity/individual may be traced uniquely to that entity/individual, who may then be held responsible for that action.

Authentication: establishing the validity of a claimed entity/verification of the identity of an individual or application.

Availability: being accessible and useable upon demand by an authorized entity.

Confidentiality: the principle that information is not made available or disclosed to unauthorized individuals, entities or processes.

Identification and authentication: functions to establish and verify the validity of the claimed identity of a user.

Information and communication systems: applications and systems to support the business, utilizing information technology as an enabler or tool.

Information technology: any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of vocal, pictorial, textual and numerical data or information.

Integrity: the inherent quality of protection that maintains the accuracy of entities of an information and communication system and ensures that the entities are not altered or destroyed in an unauthorized manner.

Monitoring: performance measurement to ensure the confidentiality, availability and integrity of operational systems and information.

Password: confidential authentication information composed of a string of characters.

RAS DIAL-BACK: Method of using a telephone line to dial into the network.

Remote access: the access of remote users to corporate ICT services by means of telephone lines or 3G data card through a gateway/computing that is performed at a location that is distant from a central site, over a network connection.

1. Preamble

1.1. Increasingly, municipalities and their information and communication systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, viruses, computer hacking and denial of service attacks. Dependence on information and communication systems and services means Municipality are more vulnerable to security threats.

1.2. Management shall set a clear policy direction and demonstrate support for, and commitment to, information and communication system security through the issue and maintenance of this Information and Communication System Security Policy and Standards across all Polokwane Municipality offices. This document shall be read in concurrence with the Minimum Information Security Standards (MISS).

2. Purpose and objectives

The purpose of this policy is to provide Polokwane Municipality with minimum rules, guideline and standard in order to apply an effective and consistent level of security to all information and communication systems that process Polokwane Municipality information.

The objectives of this policy are:

2.1. Apply cost-effective protection to security classified information which is processed by Polokwane Municipality information and communication systems;

2.2. Apply a reasonable level of protection to unclassified information so that Polokwane Municipality offices can exercise control over that information.

2.3. Be able to demonstrate accountability by a structured method of information and communication system security implementation and verification across Polokwane Municipality cluster offices;

2.4. Develop an information and communication system security culture that reflects a consistent approach, based on an understanding of the security issues and a cost-effective way of dealing with them.

3. Scope of Application

This policy is applicable to everyone who make use of the Polokwane Municipality ICT network.

4. Legal Framework

The following publications govern the execution of the Information Security Policy and were taken into consideration during the drafting of the guidelines and policy:

4.1. Constitution of the Republic of South Africa, 1996 (Act No. 108 of 1996)

4.2. Protection of Information Act (Act no 84 of 1982)

4.3. Protection of Personal Information Act (Act no 4 of 2013)

4.4. Minimum Information Security Standards (MISS), Second Edition March 1998

4.5. Municipal Email Policy

4.6. Municipal Password Policy

4.7. Municipal ICT Equipment Usage Policy.

5. Administration of the policy

ICT Manager is responsible for enforcing this policy and continuously ensuring monitoring and compliance.

6. Information System Security

6.1. Individual Accountability

6.1.1 All personnel who use/access/perform any function on or manages any part of the Municipal ICT Systems are responsible and accountable for following appropriate recommended procedures and for taking all possible steps to safeguard the information handled by that system and any sensitive assets involved. All ICT Systems shall provide means by which individual users can be uniquely identified and held individual accountable for their actions, in respect of which the system shall provide for appropriate records.

6.1.2 Everyone using the Municipal ICT systems are responsible, within the span of their control, to ensure that no actions are taken which could degrade or compromise the confidentiality, the level of accuracy, completeness, dependability and responsiveness levels of the programmes, services and information handled by the system.

6.1.3 Users of the systems should report any observed or suspected action/security weaknesses in, or threat to, systems or services to ICT SBU.

6.1.4 ICT Manager is the overall custodian of this policy.

6.2. Controlled Access

6.2.1 Only authorized users shall be granted access to the classified level of information and assets for which appropriate access authorization(s) and the need to know have been approved.

6.2.2 Every user shall be granted access to only those ICT system resources necessary to perform the assigned functions and only when such access will not lead to a breach of this or any other security principles.

6.2.3 Appropriate segregation of duties, specifically allocated and defined in writing, shall apply.

6.2.4 Controlled access will be achieved via physical and procedural means. Unique identification of the user to the system must be provided. An access

authorization structure shall determine access and privileges, grant such access and privileges and record, control and monitor these.

6.3. Categorization of information and information classification system

The comprehensive information classification system as developed by the Security Manager in terms of the Municipal Security Policy shall apply to the categorization and classification of information.

6.4. Levels of protection

6.4.1 The protection applied to information technical systems shall be matched with the sensitivity levels of the information and assets involved and shall take into consideration the identified threats to and vulnerabilities of the information system.

6.4.2 Risks or threats that ICT systems are exposed to shall be identified, analysed, evaluated and quantified in terms of the probability of them occurring and the potential impact of such an event in Polokwane Municipality and its activities. A documented risk register shall be revised on an annual basis and as when emerging risk are identified.

6.5. Disaster Recovery Plan

A documented disaster recovery plan and procedures for ICT Systems should be classified as Top Secret and handled on a need-to-know basis in order to minimize the impact of any type of disaster.

6.6. Security awareness

Officials who have access to systems should be subjected to a programme of effective and appropriate security awareness to foster their security knowledge on risks and documented ICT system principles.

6.7. System Access Control and Password Security

6.7.1. Access to computer systems shall be controlled by means of an approved computer access control system which identifies the authorized user and verifies his/her identity.

6.7.2. The access control system shall update an audit trail of all authorised and unauthorised efforts to gain access to the computer systems. Unauthorised access attempts shall be considered a breach of security.

6.7.3. Passwords shall be individual, exclusive and shall not be disclosed without authorisation in forced exceptional cases, and without documenting the incident. Unauthorised disclosure of passwords shall be considered a breach of security.

6.8. ICT equipment security

6.8.1. ICT equipment shall be in a physically protected environment where access control measures have been instituted and are applied consistently. Unattended equipment shall have appropriate security protection.

6.8.2. All portable computers are governed by the Municipal ICT Equipment Usage Policy.

6.8.3. Access to computer systems on which classified data is processed, shall be controlled, and limited by means of approved access control software.

6.9. Physical Security

Areas where computer-related equipment are accommodated, or office areas where classified information is dealt with, shall be protected in such a way that unauthorised access is prevented. Access control systems and procedures should regulate record and monitor movement in these areas.

6.10. Utilization of private computers

Private computers are prohibited to be used for official purpose.

6.11. ICT Hardware and Software

The procurement and usage of hardware and software shall be done in accordance with the Municipality ICT Equipment Usage policy.

6.12. ICT Communication Security

To ensure a safe environment in which information of a classified nature could be communicated, electronically or verbally.

6.13. Security of data transmission

Communication pertaining to classified information should be encrypted in accordance with the Polokwane Municipality approved cryptographic devices.

6.14. Internet and email

The use of electronic mail and internet is governed by the Municipality Electronic mail and Internet usage policies.

6.15. Mobile Devices

Mobile devices like I-Pads and Smart Phones shall be allowed to connect to the Municipality's email facility for sending and receiving of emails. These mobile devices shall be correctly configured to access the Municipal email facilities as per the device operational manual. Users shall familiarize themselves with the operation of these devices and the security risks involved.

7. ICT Security Systems Controls

7.1. Antivirus and Patch Management

To secure the network, it is necessary that:

7.1.1. All computers accessing office network shall be installed with Polokwane Municipality approved Anti-Virus software

7.1.2. All computers with old antivirus updates shall be quarantined and denied network access until antivirus is updated with the latest virus definitions and signatures

7.1.3. If any ICT equipment poses a risk to the network and other hosts, the host shall be disconnected from the network until the risk has been resolved.

7.1.4. The antivirus software shall be configured to automatically scan all incoming and outgoing files.

7.1.5. ICT SBU shall maintain virus-scanning software to protect the Municipal network against any virus attacks.

7.1.6. The following activities are the responsibility of the Polokwane Municipality's ICT SBU:

- ICT SBU is responsible for maintaining, reviewing and updating this Anti-Virus configuration policy.
- ICT SBU shall check antivirus updates regularly for updated information or definitions;
- ICT SBU shall perform Malware threat analysis on all Polokwane Municipality computer systems

Classification of Malwares

Viruses	These are programs that spread copies of themselves from computer to computer. Their transmission methods vary, but can include executable files, macros within data documents such as word processing files and are transmitted via floppy disks, CD-ROMs, external hard drives, email and other file-sharing methods. Viruses may or may not have a destructive component often known as a payload
Worms	A worm is similar to a virus in that it propagates from computer to computer.

	The method of transmission is somewhat different, however in that a worm can propagate itself in a standalone fashion (i.e. it does not require a file to be transmitted containing the malicious code). Worms often exist as executing processes on the host machine, firing users into opening emails which then allows the worm to be executed on the target computer
Trojan Horses	A Trojan horse is a program which appears to have one function (often posing as a game) whilst working in the background to perform some malicious action (such as inserting a backdoor or spyware). Trojan horses cannot replicate themselves, but often rely on users passing the program around as a 'bit of fun'
Backdoor	A backdoor is a program which allows access to a computer system bypassing standard authentication procedures. A backdoor can be installed by a worm or Trojan and allows a remote attacker to directly execute commands on the targeted machine. Often, machines compromised with backdoor are used to send spam emails to other computer systems or to perform further attacks on

	other systems, usually without the knowledge of the compromised system's user. A backdoor program cannot replicate, but is often inserted into the system by a virus, worm or Trojan
Spyware	Spyware is a term which covers software which reports back to the attacker the actions taken by the legitimate user of the computer. This can include key presses, mouse actions, screen information and network traffic. More usually, spyware reports back on the user's web browsing habits, often linking with software known as 'adware' to provide 'targeted' adverts to the user (often in the form of annoying popups)
Exploit	Although not strictly speaking a program in itself, an exploit is a fault in a piece of code on the system which may be used by viruses, worms and Trojan in order to compromise a system. Exploits are often published by computer security teams and are regularly patched by the software manufacturer. It is critical that any serious exploits are patched as soon as possible to ensure that vulnerabilities do not remain on computer systems

7.1.7. All desktops, laptops and servers shall use the latest security patch levels.

7.1.8. Polokwane Municipality is currently using SCCM for Windows updates.

7.1.9. Automated tools shall scan for available patches and patch levels, which shall be reviewed in accordance with Microsoft severity rating level

7.1.10. Manuals scan and reviews shall be conducted on systems for which automated tools are not available

7.1.11. Service provider supplied patch documentation shall be reviewed in order to ensure compatibility with all system components prior to being applied

7.1.12. Where feasible, patches will be tested on non-production systems installed the majority of critical applications or services prior to being loaded on production systems

7.1.13. Reports will be generated for all system categories i.e. servers and desktop. The reports may be in paper or electronic format.

7.2. Firewall and perimeter security.

The Municipality's secure network is protected from the internet and non-secure networks with firewalls and Intrusion prevention systems.

7.2.1. Refer to the Firewall Policy

7.2.2. Polokwane Municipality network shall have firewall appliances installed with built-in security rules to regulate entry and exit from the internal network. Open ports shall be used for applications or services used by ICT SBU to control traffic that goes in and out of the internal network. All opened ports on the firewall shall be described and properly documented.

7.2.3. Assistant Manager Infrastructure shall review the firewall rules to determine the relevance of the opened ports on monthly basis and provide caution on possible vulnerabilities

7.2.4. The build-in IDS/IPS shall at all times be activated to enable detection and prevention of security threats

7.2.5. Control measures shall be put in place for all the ports that needs to be opened on all the firewalls. Request for opening ports on a firewall shall require a formal detailed request with timeframes those ports need to be opened and the

request need to be recommended by the Security specialist and approved by the ICT Manager

7.2.6. External network connections to the internal network may only be through VPN access and be used for the purpose(s) it was authorized and intended for. All services being accessed from external or non-secure networks shall use secure protocols.

7.2.7. Access to Polokwane Municipality wireless connectivity shall be available to everyone with municipal official equipment such as gadgets and/or laptops

8. Security breaches

8.1. Responsibility for reporting security breaches

Everyone within Polokwane Municipality has the responsibility to report any incident of security breach to ICT SBU. Security breaches shall at all times be dealt with using the highest degree of confidentiality in order to protect the official(s) concerned and prevent him/her from unnecessary injustice.

9. Inception Date

This policy comes into effect from the date of approval.

10. Policy Review

This policy shall be reviewed every three (3) years.

11. Enquiries

Enquiries about the policy should be directed to the ICT Manager.

* * *