Municipal Corporate Governance of Information and Communications Technology Policy

Document Name:	**Municipal CGICT policy**
Document Number:	POL-002
Version:	003
Date Issued:	May 2024

Document Information

Document name	Municipal CGICT policy
Version	003
Policy Code	POL-002
File Name	POL-ICT-05-24 Municipal CGICT policy.doc
Date Issued	May 2024
Policy Enforcer	ICT Manager

Table of Contents

1. Preamble

ICT Governance has been described as an effective and efficient management of ICT resources to facilitate the achievement of business goal and objectives. ICT Governance framework is important to ensure that the business achieves sustainable success. This ICT Governance Framework of Polokwane Municipality will provide guidance to the Political and Administrative leadership on how to effectively develop and manage the Municipal ICT infrastructure in a stable and regulated manner. Corporate governance of ICT will enhance service delivery, resource utilization, performance, and quality, driving digital transformation strategies and enabling strategic performance measurement for the municipality.

According to CobiT (Control Objectives for IT and Related Technology) Corporate Governance is the set of responsibilities and practices exercised by the Council and executive management with the goals of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise ‘s resources are used responsibly. ICT governance can be seen as a structure of relationships and processes to direct and control the enterprise use of ICT to achieve the enterprise ‘s goals by adding value while balancing risk vs. return over ICT and its processes.

The Department of Public Service and Administration (DPSA) released a circular that requires all government departments and entities to adopt an ICT governance framework. The Department has issued a “Corporate Governance of ICT (CGICT) Policy Framework version 2” which maps out how governance of ICT within government entities is to be applied, structured, and implemented.

This policy framework outlines the policies, plans and structures that need to be implemented to ensure proper governance and to promote integrity, security, reliability, and privacy of the entire information infrastructure including the information and data it contains, the network, the computers and other access devices.

2. Terms and Definitions

AGSA: Auditor-General of South Africa
Applicability: Appositeness, appropriateness, relevance, pertinence, relatable, affiliation.
Assessment Standard: Corporate Governance of ICT Assessment Standard.
Business: The business of the municipality refers to the municipal core activities and internal support activities.
CGICTPF: Corporate Governance of ICT Policy Framework This term in this revised Policy Framework will also mean governance of ICT, IT governance, and Enterprise governance of Information & Technology. This approach recognizes that other global best practice frameworks use these terms interchangeably.
Corporate governance: King IV defines corporate governance as the exercise of ethical and effective leadership by the governing body towards the achievement of the following governance outcomes: Ethical culture; Good performance; Effective control; and Legitimacy.
Governance champion: The Head of Department is the corporate governance champion. The accountability cannot be delegated, but this function may be delegated to an executive or senior manager responsible for driving corporate governance within the department.
Corporate governance of ICT: The system by which the current and future use of ICT is directed and controlled. Corporate governance of ICT involves evaluating and directing ICT use to support

the organisation and monitoring this use to achieve plans. It includes the strategy and policies for using ICT within an organisation. (ISO/IEC 38500:2015)

DPSA: Department of Public Service and Administration.

EXCO: Executive Management Committee (consists of executive management members of the municipality).

GITO: Government Information Technology Officer (Cabinet Memorandum 38(a) of 2000).

Head of ICT: Refers to the person heading the ICT component/office and could be the GITO/ICT Manager depending on the naming convention used in the municipality.

ICT: Information and communication technology.

ICT initiative: Includes all ICT information systems and related information technology used to enable business/services. An ICT initiative refers to using information and application systems and technology to achieve business objectives to enable service delivery. In terms of planning, this refers to related existing and planned initiatives.

IT: Information technology

IT Service Management: A set of policies and practices for implementing, delivering, and managing IT services for end-users in a way that meets the stated needs of end-users and the stated goals of the business (IBM, 2020)

IEC: International Electrotechnical Commission.

Institutionalisation: Embed corporate governance of ICT as a custom or norm within the municipality or culture.

ISO: International Organization for Standardization.

ISO/IEC 38500:2015: An international standard for corporate governance of IT published jointly by ISO and the IEC.

King IV: Report on Corporate Governance for South Africa, 2016.

MTEF: Medium-Term Expenditure Framework.

Policy Framework: This Public Service Corporate Governance of ICT Policy Framework (CGICTPF).

Regime: A set of rules or a system or an ordered way of doing things that regulate the operation or way of doing things within the municipality.

Responsible: Refers to the person who must ensure that activities are completed successfully.

Responsible, Accountable, Consulted, Informed (RACI) chart: A diagram that identifies users' key roles and responsibilities against major tasks within a project (Software Advice, 2020).

Risk appetite: The amount of residual risk that the department is willing to accept (PSRMF 2010:15).

Risk management: A systematic and formalised process to identify, assess, manage and monitor risks (PSRMF 2010:16)

3. Purpose and objectives

The purpose of this policy framework is to establish and integrate the corporate governance of ICT as a fundamental component of the corporate governance practices within municipality in a uniform and coordinated manner. This Policy Framework mandates municipal strategic leadership to oversee ICT corporate governance and the effective use of ICT to achieve municipal strategic objectives. This Policy Framework describes the principles, practices, and governance system that will enable and sustain effective provision of ICT within the municipality.

4. Scope of Application

This policy framework is applicable to Polokwane Municipality Information Communication Technology strategic leadership who take responsibility for the corporate governance of ICT and provide leadership for the use of ICT resources.

5. Legislative Framework and ICT standards

The following publications govern the strategic planning and corporate governance were taken into consideration as applicable to the ICT operation:

5.1. Public Service Governance of ICT Framework Policy version 2;

5.2. The constitution of the Republic of South Africa, 1996;

5.3. Local Government: Municipal Systems Act, 2000 (Act 32 of 2000);

5.4. Local Government: Municipal Finance Management Act, 2004 (Act 56 of 2004);

5.5. Electronic and Communications Act, 2005 (Act 36 of 2005);
5.6. Electronic Communication Security Act, 2002 (Act 68 of 2002);
5.7. Polokwane Municipality: Supply Chain Management Policy;
5.8. Preferential Procurement Policy Framework Act, 2000 (Act 5 of 2000);
5.9. ITIL Information Technology Infrastructure Library;
5.10. Control Objectives for Information Technology (COBIT).
5.11. Minimum Information Security Standards (MISS), Second Edition March 1998

6. Corporate Governance of ICT in the Municipality.

Polokwane municipality reviewed the current governance framework policy to incorporate the new developments on KING V, COBIT 5, and ITIL V4. These corporate governance frameworks are ICT related and municipal will realize the benefits of implementing corporate governance of ICT as following:

a) Improved effective service delivery through ICT-enabled access to municipal information and services.
b) Improved delivery of ICT service quality.
c) Increased alignment of ICT investment towards municipal integrated development plans.
d) Improved return on ICT investments.
e) ICT risks managed in line with the ICT priorities and risk appetite of the Municipality.
f) Appropriate security measures to protect both the Municipality and its employees' information.
g) Improved management of municipal-related ICT projects.

6.1. Layered approach to corporate governance of ICT.

Corporate governance of ICT encompasses two levels of decision-making which are governance and management.

- **Corporate governance of ICT**: the Executive Management Committee (EXCO) is accountable for achieving the municipal's mandate and strategic objectives through, among other things, the use of ICT. The accountability for corporate governance of ICT must be facilitated through clearly defined, implemented, and audited controls.

- **Management of ICT**: entails a process whereby all operational activities concerning ICT resources are aligned to the municipal's priorities and needs. It includes tangible resources like networking hardware, computers, and people and intangible resources like software and data. ICT management aims to generate value through technology, with the ICT function responsible for managing processes for effective execution and monitoring of ICT.

6.2. Accountability structure for corporate governance of ICT

The corporate governance of ICT accountability structure provides for the roles and responsibilities of the different levels of corporate governance.

6.2.1 Polokwane municipality Governance structure.

6.2.1.1 EXCO

Polokwane municipality established Executive management committee which is chaired by the Municipal Manager and ICT manager form part of the EXCO members. This committee is the highest level of municipal accountability structure must provide monitoring and oversight to ensure ICT usage aligns with the municipal's strategic goals. EXCO is responsible for:

- Recommend for approval of ICT plan (MTEF), ICT operational plan, and other related plans and procedures, ICT policies to next structural level.
- Monitor that the ICT plan supports the municipal directorates to deliver on its objectives per the IDP.
- Monitor and evaluate the performance of the ICT steering committee and processes.
- Provide support to the functioning of the ICT steering committee.
- Oversee the implementation of the CGICT Policy Framework and associated policies and strategies.
- Review and ratify quarterly ICT steering committee reports.

6.2.1.2 ICT Steering Committee

Polokwane municipality established an Information Communication Technology Steering Committee comprised of ICT Manager, all directors and directorates nominees that set standards and consider how ICT is invested and used within Polokwane Municipality. The committee chairperson is independent member of APAC. The committee is responsible for:

- Providing oversight on the management and use of ICT in the municipality.
- Providing strategic leadership towards the digitalization of the municipality, including ICT projects and services.
- Monitoring the implementation of approved plans, policies, strategies.
- Monitoring that ICT related business risks are mitigated, benefits realization from the ICT investments (ICT projects), and audit issues from assurance providers.
- Providing recommendations and reporting to APAC on ICT governance implementation including ICT strategies and plans.

The ICT Steering Committee term of reference are developed and approved by Municipal Manager.

6.3 Role and Responsibilities

6.3.1 Municipal Manager

Municipal Manager plays an important role in setting up strategic goals for the Municipality. The Municipal Manager is the designated governance champion accountable for the corporate governance of ICT and is responsible for the establishment of corporate governance of the ICT system and monitoring of its performance. Within Polokwane municipality the corporate governance champion responsibility may be delegated to Director Corporate and Shared services with the authority to establish and monitor the corporate governance of the ICT system.

6.2.4 ICT Manager

ICT Manager is responsible for ensuring the strategic use of ICT aligns with business requirements to fulfil its mandate within a secure information environment. Other responsibilities are as follows:

- Overseeing and directing the day-to-day activities of the ICT Strategic Business Unit (ICT SBU)
- Ensuring that systems, services, and infrastructure work reliably and securely.

- Participation in developing the digital transformation strategy focusing on the municipal's optimization and transformation of ICT.
- Provide a quarterly report to the ICT steering committee on the following key general IT controls: **Information security management**; **User access management; ICT service continuity**; **Management of external service providers (3rd parties)**; **Configuration management (IT assets lifecycle management); and IT Service management.**
- Report on ICT performance to EXCO on key ICT operational matters that potentially impact the achievement of municipal objectives through the implementation of ICT-enabled projects.

6.3. **RACI matrix.**

Table below details the RACI for decision-making with the municipality.

DECISION TOPIC	SCOPE	Responsible, Accountable, Consulted and Informed (RACI)					
		Executive Management	Risk Committee	Audit Committee	ICT Steering Committee	ICT Management	Municipal Employees
ICT governance	• Aligning with Corporate Governance • Principles, Establishing, Structures and Objectives • Alignment of ICT Strategy and the IDP	**A/R**	**I**	**I**	**R**	**A/R**	**I**
Municipal strategy	• Defining Business goals and objectives • Deciding where and how ICT can enable and support Business Objectives	**A/R**	**I**	**I**	**R**	**A/R**	**I**
ICT policies	• Providing accurate, understandable, and approved policies, procedures, guidelines and documentation to other stakeholders	**A/R**	**I**	**I**	**R**	**A/R**	**I**

	• Developing and implementing ICT policies • Enforcing ICT Policies						
ICT Strategy	• Engaging with Top Management in Aligning ICT Strategic Planning with current and future business needs • Understanding the current ICT Capabilities	**A/R**	**I**	**I**	**R**	**A/R**	**I**
ICT Technology Direction	• Planning Infrastructure maintenance • Providing appropriate platforms for the Business Applications in line with the defined ICT Architecture and Technology Standards	**A/R**	**I**	**I**	**R**	**A/R**	**I**
ICT methods and framework	• Establishing transparent, flexible and responsive ICT Organizational Structure. • Defining and Implementing ICT processes that integrate owners, roles and responsibilities into Business and decision processes • Defining an ICT process Framework • Defining Roles and Responsibilities	**A/R**	**I**	**I**	**R**	**A/R**	**I**

7. ICT principles, practices, and systems.

This policy framework provides for the following:

7.1 Principles which are rules that guide decision making and behaviours. These principles establish the context for effective, efficient, and acceptable use of ICT.

The Polokwane Municipality has identified and adopted 234 principles and addition of 6 principles that are compulsory as per DPSA. Therefore, only 105 principles out of 240 are documented, and other can be referred to from the old policy.

Principle 1: Strategic Mandate

The ICT (Current and future capabilities) must enable the municipality's Strategic Mandate and objectives.
Principle 2: Institutionalisation of corporate governance of ICT
Corporate governance of ICT must be institutionalised within the corporate governance regime of the municipality.
Principle 3: Value and benefit realisation from ICT investment
All ICT investments must achieve the predetermined value and benefits.
Principle 4: Manage ICT-related business risks
ICT related business risks including security and cybersecurity must be managed.
Principle 5: Change management /departmental behaviour
Corporate governance of ICT must be implemented through appropriate change management interventions.
Principle 6: Monitoring and evaluation
Monitor and evaluate the use and performance of ICT
Principle 7: Corporate Governance of ICT
The Accounting Officer is responsible for the Corporate Governance of ICT and must create an enabling environment in respect of the Corporate Governance of ICT within the applicable judiciary and information security context.
Principle 8: ICT Strategic Alignment
The Executive Management must ensure ICT service delivery aligns with the municipality's strategic goals, considering current and future ICT capabilities, and is fit for purpose at the correct service levels and quality.
Principle 9: Significant ICT Expenditure
Executive management must oversee significant ICT expenditure, ensuring it's justified for municipal business purposes, managing its benefits, opportunities, costs, and risks, and ensuring adequate management of information assets.
Principle 10: Risk Management and Assurance

Executive management is tasked with managing ICT risks within municipal risk management practices and ensuring the ICT function is audited as part of the municipal audit plan.
Principle 11: Organisational Behaviour
Executive management must ensure ICT service delivery is sensitive to organizational behavior and culture, demonstrating understanding and respect for such factors.
Principle 12: Management Commitment
The Executives and Management of Polokwane Municipality are committed to establish top managements direction on Information Security, and Commitment demonstrated.
Principle 13: Security Policy
The Executives and Management of Polokwane Municipality are committed to produce and communicate a comprehensive, documented information security policy to all individuals with access to the enterprise's information and systems.
Principle 14: Staff agreements
The Executives and Management of Polokwane Municipality are committed to establish a staff agreement that specify information security responsibilities, are incorporated into staff agreements and are taken into account when screening applicants for employment
Principle 15: Information Security Function
The Executives and Management of Polokwane Municipality are committed to establish a specialist information security function, which has enterprise-wide responsibility for promoting information security
Principle 16: Security awareness
The Executives and Management of Polokwane Municipality are committed to undertake specific activities, such as a security awareness program, to promote security awareness to all individuals who have access to the information and systems of the enterprise.
Principle 17: Local Security Co-ordination
The Executives and Management of Polokwane Municipality are committed to make arrangements to co-ordinate information security activity in Directorates/ Business units.
Principle 18: Security Education
The Executives and Management of Polokwane Municipality are committed to educate and train staff in how to run systems correctly and how to develop and apply security controls.
Principle 19: Security Classification Scheme
The Executives and Management of Polokwane Municipality are committed to establish a security classification scheme that applies throughout the enterprise, based on the importance and sensitivity of information and systems in use.
Principle 20: Ownership

The Executives and Management of Polokwane Municipality are committed to assign 'Ownership' of critical information and systems to capable individuals, with responsibilities clearly defined and accepted.
Principle 21: Legal and Regulatory Compliance
The Executives and Management of Polokwane Municipality are committed to establish a process to identify and interpret the information security implications of relevant laws and regulations.
Principle 22: Secure Environment
The Executives and management of Polokwane Municipality are committed to establish the responsibility for managing information privacy and to apply security controls for handling personally identifiable information.
Principle 23: Security Requirements
The Executives and management of Polokwane Municipality are committed to subject important or critical applications, computer installations, networks and systems under development to a structured information risk analysis on a regular basis.
Principle 24: Business Requirements for Security
The Executives and management of Polokwane Municipality are committed to assess the business impact of unauthorized disclosure of information associated with the application.
Principle 24: Integrity Requirements
The Executives and management of Polokwane Municipality are committed to assess the business impact of the accidental corruption or deliberate manipulation of business information stored in or processed by the application.
Principle 26: Availability Requirements
The Executives and management of Polokwane Municipality are committed to assess the business impact of business information stored in or processed by the application being unavailable for any length of time.
Principle 27: Security Architecture
The Executives and management of Polokwane Municipality are committed to establish 'information security architecture', which provides a framework for the application of standard security controls throughout the enterprise.
Principle 28: Asset Management
The Executives and management of Polokwane Municipality are committed to use proven, reliable and approved hardware/software that meet security requirements and are recorded in an inventory.
Principle 29: Inventory of Desktop Application
The Executives and management of Polokwane Municipality are committed to record critical desktop applications used in the end user environment in an inventory, or equivalent.
Principle 30: Physical Protection

The Executives and management of Polokwane Municipality are committed to physically protect all buildings throughout the enterprise that house critical IT facilities (e.g. data centres, network facilities and key user areas) against accident or attack.
Principle 31: Power Supplies
The Executives and management of Polokwane Municipality are committed to protect critical computer equipment and facilities against power outages.
Principle 32: Hazard Protection
The Executives and management of Polokwane Municipality are committed to protect that computer equipment and facilities against fire, flood, environmental and other natural hazards.
Principle 33: Resilience – System Management
The Executives and management of Polokwane Municipality are committed to run the computer installation on robust, reliable hardware and software, supported by alternative or duplicate facilities.
Principle 34: Resilience – Live Environment
The Executives and management of Polokwane Municipality are committed to run the applications on robust, reliable hardware and software, supported by alternative or duplicate facilities
Principle 35: Resilience – Network Management
The Executives and management of Polokwane Municipality are committed to run the network on robust, reliable hardware and software, supported by alternative or duplicate facilities
Principle 36: Resilience – Voice Networks
The Executives and management of Polokwane Municipality are committed to run the voice network by a robust, and reliable set of hardware and software, with alternative facilities available when required.
Principle 37: Resilience - Service Providers
The Executives and management of Polokwane Municipality are committed to only obtain computer and network services required to support the application from service providers capable of providing required security controls, and be supported by documented contracts or service level agreements.
Principle 38: Installation and Design
The Executives and management of Polokwane Municipality are committed to design computer installations to cope with current and predicted information processing requirements and be protected using a range of in-built security controls.
Principle 39: Host System Configuration
The Executives and management of Polokwane Municipality are committed to configure host systems to function as required and to prevent unauthorised or incorrect updates.
Principle 40: Workstation Protection
The Executives and management of Polokwane Municipality are committed to purchase workstations connected to the application from a list of approved suppliers, tested prior to use, supported by maintenance arrangements and protected by physical controls

Principle 41: Hand Held Devices
The Executives and management of Polokwane Municipality are committed to ensure that Hand-held devices (e.g. Personal Digital Assistants (PDAs), WAP-based mobile phones and smartphones) used in the end user environment should be approved, protected by software controls and supported by standards/procedures for acceptable use.
Principle 42: Portable Storage Devices
The Executives and management of Polokwane Municipality are committed to approve the use of portable storage devices in the end user environment, restrict access to them, and protect the information stored on them.
Principle 43: Configuration of Network
The Executives and management of Polokwane Municipality are committed to configure network devices to function as required, and to prevent unauthorized or incorrect updates
Principle 44: Network Documentation
The Executives and management of Polokwane Municipality are committed to ensure networks are supported by accurate, up-to-date documentation
Principle 45: Identity and Access Management
The Executives and management of Polokwane Municipality are committed to establish identity and access management arrangements to provide effective and consistent user administration, identification, authentication and access mechanisms across the organization
Principle 46: Access control
The Executives and management of Polokwane Municipality are committed to restrict access to the application and associated information to authorized individuals and enforce accordingly.
Principle 47: User Authorisation
The Executives and management of Polokwane Municipality are committed to authorize all users of the computer installation before they are granted access privileges.
Principle 48: Firewall
The Executives and management of Polokwane Municipality are committed to route network traffic through a firewall, prior to being allowed access to the network
Principle 49: Third Party Access
The Executives and management of Polokwane Municipality are committed to uniquely identify, subject to a risk analysis, approve, and support by contracts all connections from third parties
Principle 50: Internet Access

The Executives and management of Polokwane Municipality are committed to approve the use of internet by end users, protected by restricting the types of use permitted, deploying approved web browsers and promoting awareness of the risks associated with Internet access
Principle 51: Wireless Access
The Executives and management of Polokwane Municipality are committed that all wireless access be authorized, authenticated, encrypted and only permitted from approved locations
Principle 52: Remote Working
The Executives and management of Polokwane Municipality are committed to purchase personal computers used by staff working in remote locations from a list of approved suppliers, tested prior to use, supported by maintenance arrangements and protected by physical controls
Principle 53: Remote Maintenance
The Executives and management of Polokwane Municipality are committed to restrict remote maintenance of the network to authorized individuals, confined to individual sessions, and subject to review.
Principle 54: General Security Controls
The Executives and management of Polokwane Municipality are committed to consider the full range of general security controls when designing the system under development
Principle 55: Cryptography
The Executives and management of Polokwane Municipality are committed to approve, document and apply cryptographic solution enterprise-wide
Principle 56: Cryptographic Key Management
The Executives and management of Polokwane Municipality are committed to manage cryptographic keys tightly, in accordance with documented standards/procedures, and protected against unauthorized access or destruction.
Principle 57: Public Key Infrastructure
The Executives and management of Polokwane Municipality are committed to protect a public key infrastructure (PKI) where used, it should be protected by ‘hardening’ the underlying operating system(s) and restricting access to Certification Authorities
Principle 58: Public Key Infrastructure - Application
The Executives and management of Polokwane Municipality are committed to protected any public key infrastructure (PKI) that is used by the application by ‘hardening’ the underlying operating system(s) and restricting access to Certification Authorities
Principle 59: E-mail
The Executives and management of Polokwane Municipality are committed to protect E-mail systems by a combination of policy, awareness, procedural and technical security controls

Principle 60: Instant Messaging
The Executives and management of Polokwane Municipality are committed to protect instant messaging services by setting management policy, deploying Instant Messaging application controls and configuring the security element of an Instant Messaging Infrastructure
Principle 61: Web-Enabled Application
The Executives and management of Polokwane Municipality are committed to apply specialized technical controls to web-enabled applications
Principle 62: Web-Enabled Development
The Executives and management of Polokwane Municipality are committed to apply specialized technical controls to the development of web-enabled applications
Principle 63: Electronic Commerce
The Executives and management of Polokwane Municipality are committed to establish a process to ensure that information security is incorporated into electronic commerce initiatives enterprise-wide
Principle 64: Voice Over IP (VOIP) Networks
The Executives and management of Polokwane Municipality are committed to ensure that Voice Over IP (VOIP) networks are approved, and protected by a combination of general network and VOIP – specific controls
Principle 65: Outsourcing
The Executives and management of Polokwane Municipality are committed to establish a process to govern the selection and management of outsource providers supported by documented agreements that specify the security requirements to be met
Principle 66: Secure Environment
The Executives and management of Polokwane Municipality are committed to establish documented standards/procedures for developing business continuity plans and for maintaining business continuity arrangements throughout the enterprise
Principle 67: Application Management
The Executives and management of Polokwane Municipality are committed to develop a business continuity plan, supported by contingency arrangements, and tested periodically
Principle 68: Service Continuity – Contingency Plan
The Executives and management of Polokwane Municipality are committed to develop and document a business continuity plan
Principle 69: Contingency Arrangements
The Executives and management of Polokwane Municipality are committed to established alternative processing arrangements and be made available when required.
Principle 70: Validation and Maintenance

The Executives and management of Polokwane Municipality are committed to test contingency plans and arrangements on a periodic basis
Principle 71: Network Operations
The Executives and management of Polokwane Municipality are committed to develop a service continuity plan, supported by effective contingency arrangements, and tested periodically
Principle 72: IT Environments
The Executives and management of Polokwane Municipality are committed to subject the information security status of critical IT environments to thorough, independent and regular security audits/reviews
Principle 73: Application
The Executives and management of Polokwane Municipality are committed to subject the information security status of the application to thorough, independent and regular security audits/reviews
Principle 74: Computer Installation
The Executives and management of Polokwane Municipality are committed to subject the information security status of the computer installation to thorough, independent and regular security audits/reviews.
Principle 75: Network
The Executives and management of Polokwane Municipality are committed to subject the information security status of the network to through, independent and regular security audits/reviews
Principle 76: Development
The Executives and management of Polokwane Municipality are committed to subject the information security status of systems development activity to thorough, independent and regular security audits/reviews
Principle 77: Security Monitoring
The Executives and management of Polokwane Municipality are committed to monitor the information security condition of the enterprise periodically and report to top management
Principle 78: Development Management
The Executives and management of Polokwane Municipality are committed to carry out development activities in accordance with a documented methodology
Principle 79: Development Management
The Executives and management of Polokwane Municipality are committed to carry out development activities in accordance with a documented methodology
Principle 80: Development Environment

The Executives and management of Polokwane Municipality are committed to perform System development activities in specialized development environments, isolated from the live environment, and protected against disrupted and disclosure of information
Principle 81: Quality Assurance
The Executives and management of Polokwane Municipality are committed to performing quality assurance of key security activities during the development cycle
Principle 82: Specifications of Requirements
The Executives and management of Polokwane Municipality are committed to document and agreed upon business requirements (including those for information security) before detailed design commences
Principle 83: Access Control
The Executives and management of Polokwane Municipality are committed to individuals restrict access to the application and associated information to authorized and enforce accordingly. The Executives and management of Polokwane Municipality are committed to establish access control arrangements to restrict access by all types of user to approved system capabilities of the computer installation.
Principle 84: Access Privileges
The Executives and management of Polokwane Municipality are committed to assign all users of the computer installation of minimum and specific privileges to allow them to access particular information or systems
Principle 85: Application Management
The Executives and management of Polokwane Municipality are committed to ensure the full range of application controls are considered, and required controls identified
Principle 86: Design and Build
The Executives and management of Polokwane Municipality are committed to ensure the full range of application controls are considered when designing the system under development
Principle 87: Sensitive Information – Application Management
The Executives and management of Polokwane Municipality are committed to provide additional protection for applications that involve handling sensitive material or transferring sensitive information
Principle 88: Handling Computer Media – System Operation
The Executives and management of Polokwane Municipality are committed to protect information held on data storage media (including magnetic tapes, disks, printed results, and stationery) against corruption, loss or disclosure and additional security controls applied to media containing sensitive information
Principle 89: System Design

The Executives and management of Polokwane Municipality are committed to consider information security requirements for the system under development when designing the system
Principle 90: System Build
The Executives and management of Polokwane Municipality are committed to carry out system build activities (including coding and package customization) in accordance with industry good practice, performed by individuals provided with adequate skills/tools and inspected to identify unauthorized modifications or changes which may compromise security controls
Principle 91: Acquisition - Design and Build
The Executives and management of Polokwane Municipality are committed to ensure that robust, reliable hardware and software are acquired, following consideration of security requirements and identification of any security deficiencies
Principle 92: Testing Process
The Executives and management of Polokwane Municipality are committed to test all elements of a system (i.e. application software packages, system software, hardware and services) before the system is promoted to the live environment
Principle 93: Acceptance Testing
The Executives and management of Polokwane Municipality are committed to subject systems under development to rigorous acceptance testing in an isolated area that simulates the live environment
Principle 94: Installation Process - Implementation
The Executives and management of Polokwane Municipality are committed to install new systems in the live environment in accordance with a documented installation process
Principle 95: Post Implementation Review - Implementation
The Executives and management of Polokwane Municipality are committed to conduct post-implementation reviews for all new systems
Principle 96: Resilience
The Executives and management of Polokwane Municipality are committed to only obtain computer and network services required to support the application from service providers capable of providing required security controls, and be supported by documented contracts or services level agreements
Principle 97: Service Agreements
The Executives and management of Polokwane Municipality are committed to classify users service requirements in a way that identifies their critically to the business and documented in agreements, such as contracts or service level agreements
Principle 98: Service Providers

The Executives and management of Polokwane Municipality are committed to obtain network services from service providers capable of providing relevant security controls, and be supported by documented contracts or service level agreements
Principle 99: Host System Configuration
The Executives and management of Polokwane Municipality are committed to configure host systems to function as required and to prevent unauthorized or incorrect updates
Principle 100: ICT Governance Function
The Executives and Management of Polokwane Municipality are committed to establish an ICT Governance function, which has enterprise-wide responsibility for promoting good ICT Governance and implementation of the governance Key Performance Indicators
Principle 101: ICT Enterprise Architecture Function
The Executives and Management of Polokwane Municipality are committed to establish an ICT Enterprise Architecture function, which has enterprise-wide responsibility for promoting a collaboration of ICT to Business
Principle 102: ICT Project Management Office Function
The Executives and Management of Polokwane Municipality are committed to establish an ICT Project Management Office function, which has enterprise-wide responsibility for promoting good ICT projects, procurement, SLAs and contract management
Principle 103: ICT for Rural Broad Band
The Executives and management of Polokwane Municipality are committed to ensure that the following principles are executed: **Communication is a fundamental human right, Rural Polokwane is diverse, Local ownership and investment in community is the priority, and Network neutrality and open access are vital**
Principle 104: ICT Catalog
The Executives and management of Polokwane Municipality are committed to ensure that ICT Business Unit is well established to effectively and efficiently provide all services identified in ICT Catalog
Principle 105: ICT Processes
The Executives and management of Polokwane Municipality are committed to ensure that ICT Business Unit is well established to effectively and efficiently execute all ICT Processes

6.3 **Practices** are specific actions that prescribe how and by whom the principles will be implemented.

The below table outlines corporate governance of ICT practices that will be used cascade the principles implementation.

Number	Practice Description
Practice 1	The Municipal Manager is required to ensure that the municipality's use of information and communication technologies enhances service delivery to the public, ensuring equal access to municipal services as outlined by regulation 93 of the Public Service Regulations (PSR), 2016. The PSR further provides for the municipal manager to ensure that such acquisition, management, and use of information and communication technologies improve the municipal's productivity. In terms of governance of ICT, this shall include: a) Ensuring that corporate governance of ICT is included in the strategic leadership and oversight responsibility of the municipality to achieve the strategic objectives; b) Providing strategic structural requirements of the ICT function to provide adequate capacity and capability for the use of ICT to enable business; and c) Ensuring that ICT planning methodology and instruments are aligned with the business requirements.
Practice 2	a) Ensuring that corporate governance of ICT is embedded in the corporate governance regime of the municipality; and b) Providing oversight to ensure that effective ICT prescripts, structures, strategic plans, and corporate governance of the ICT system (see Section 14) are institutionalized to evaluate, direct, and monitor ICT use.
Practice 3	In terms of governance of ICT, this shall include: a) Ensuring that responsible ICT investment practices are in place to promote good governance and the creation of value and benefits; b) Determining upfront the expected benefits and value from an ICT investment; c) Oversee the value and benefits delivered through these major ICT investments and significant ICT operational expenditure; d) Concurrence of the Head of ICT in all ICT related decisions, including procurement; and e) Ensuring that an executive manager responsible for the ICT initiative/project signs off, confirming value realization.
Practice 4	In terms of governance of ICT, this shall include: a) Ensuring that ICT related business risks (including cybersecurity) are addressed as part of the risk and audit regime of the department; and b) 4.2 Overseeing that financial and other risks of major ICT investments are managed.

Practice 5	a) Setting the example to adopt and influence culture change within the municipality (lead by example); b) Direct and oversee that culture change of municipal behaviour is effected through change management; and c) Support and be early adopters of change initiatives.
Practice 6	In terms of governance of ICT, this shall include: a) Providing oversight to ensure that the principles and practices are implemented, monitored, and evaluated to ensure the governance mechanisms remain functional and effective; b) Overseeing compliance with regulatory prescripts, policies, and standards that have an impact on the performance of ICT; and c) Overseeing performance against targets and objectives (benefits realisation, alignment with business goals, risk management, and resource optimisation).

6.4 **A system** is a set of means and mechanisms that enable the implementation of corporate governance of ICT. The system explains how the ICT effort of a municipality is governed through the governance tasks of evaluation, directing and monitoring.

- This Policy will be implemented through corporate governance of the ICT system, highlighting the interplay between governance, strategic leadership, and management's responsibilities.
- Corporate governance of the ICT system directs and controls resource use to achieve municipal strategic objectives.
- The system mentions the corporate governance tasks of evaluating, directing, and monitoring used to apply the principles and practices.
- The functioning of the corporate governance of the ICT system is depicted in below as Figure 1: Corporate governance of the ICT system (Adapted from ISO/IEC 38500: 2015)

This figure 1 is explained as follows:

- At the core of the corporate governance of the ICT system are leadership, structures, prescripts, and procedures to evaluate, direct and monitor the efficient and effective use of ICT to achieve the strategic mandate and objectives of the municipality, appropriate management of risks and responsible use of resources. It includes determining the alignment between business requirements and ICT plans;
- Through these governance tasks, stakeholder needs and options are evaluated to determine the municipal objectives. Direction is provided through prioritization of proposals/options, and decision-making and monitoring are done by measuring performance and compliance against agreed-on direction and objectives;
- EXCO, which is accountable, provides the strategic direction of the municipality. The strategic direction and the external and internal context determine the strategic objectives. The management of business execution is done through the organizational structure and use of the relevant resources;
- The different accountability structures must monitor, evaluate and report on the execution of these initiatives to ensure that the desired outcomes are achieved within the prescriptive and a secure environment; and

- All the ICT-related initiatives, such as regulatory prescripts, standards, and transversal initiatives, which impact ICT performance, must be reviewed regularly.

8. ICT policies, frameworks, and plans.

To enable the performance of ICT, specific ICT-related policies and/or frameworks are required. The municipality has developed and implemented the following policies and plans, the ones highlighted in blue still need to be developed and implemented:

a) Municipal corporate governance of ICT policy
b) Information security policy
c) ICT service continuity plan
d) ICT project management framework
e) ICT end-user policy (acceptable use)
f) IT service management policy
g) Departmental strategic plan
h) ICT plan (three-year plan)
i) ICT plan (three-year plan)

9. Monitoring and Evaluation

The implementation of this policy is measured through the Assessment Standard and/or other related standards.

(a) The Assessment Standard will measure the compliance with the Policy and the performance of the ICT function to enable the achievement of business objectives and value creation for the municipality.

(b) The Assessment Standard includes a balanced scorecard with guiding criteria to assess the compliance and performance of ICT.

(c) This Assessment Standard will provide municipality with self-assessment criteria to measure ICT compliance and performance.

10. Inception Date

This policy comes into effect from the date of approval.

11. Policy Review

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

12. Enquiries

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

* * *