

APPENDIX A

DEPARTMENT: CORPORATE SERVICES

SUB-DEPARTMENT: INFORMATION TECHNOLOGY



IT STRUCTURE, FUNCTIONS AND SERVICES

VISION:



A City of Excellence that is a Citizen-centric Smart City.

MISSION:

To provide integrated, appropriate, cost-effective, accessible, efficient, reliable and innovative IT solutions and services to meet the service delivery mandate of the Municipality.

KEY PERFORMANCE AREAS:

The IT unit should provide the following Information Technology services:

-  **Corporate IT Governance and Strategy**- Ensure good IT Governance through the implementation of IT policies, strategies, plans, SLA's and Contracts that is aligned and cost effective to the business needs of the Municipality and train employees in all relevant Municipal systems to improve productivity and efficiency.
-  **E-Government services including website and intranet** - Implement E-Government 24/7 services to the community and various stakeholders.
-  **Servers, Network Systems & Desktop Maintenance and Services** - Support, Maintain, Manage and Provide excellent IT Server, Network and Desktop Services to all users and residents, Enterprise wide.
-  **Information technology Solutions & Systems including Research and Project Management** - Propose, Procure and Implement new innovative IT Solutions and Systems that will fast track and improve the quality of service delivery provided to the community.
-  **Disaster Recovery, Business Continuity and IT Security** -Ensure minimum to adequate business continuity in the provision of services to the community and ensure optimum level of IT security to equipment, information and related IT resources.
-  **Networking** - Build and Develop Partnerships with various stakeholders to exchange and share their knowledge and experience in implementing similar service delivery enhancement systems.

AIMS & OBJECTIVES:**Corporate IT Governance and Strategy:**

- ✚ Compile and review IT Policies, procedures and implement them.
- ✚ Compile and review IT strategy/plan, IDP, Sector plans – to align IT to meet business goals of the various Directorate's.
- ✚ Draft and Finalise IT division's organogram and job descriptions.
- ✚ Ensure appropriate personnel render required IT services.
- ✚ Review all IT Contracts and SLA's against performance of SP's.
- ✚ Implement ITIL as the de-facto standard for managing IT services.
- ✚ Project management of IT projects - Entire lifecycle.
- ✚ Work with Skills Development Unit to upskill IT personnel and users (including Councillors).

E-Government services including website and intranet:

- ✚ Redevelop and maintain the web solutions including the website and intranet to customer centric transactional services, business, economic and tourism needs, information dissemination to various tiers of Government and residents.
- ✚ Integrate with the Smart City project to provide all E-government services to the community.

Servers, Network Systems & Desktop Maintenance and Services:

- ✚ Procure, Upgrade, Deliver, Implement, Maintain, Repair all IT equipment, systems and services.
- ✚ Ensure timeous support to assist on required IT needs in line with ITIL standards.
- ✚ Ensure good level of uptime to servers and network systems by implementing good monitoring & preventative maintenance tools.
- ✚ Implement, maintain, upkeep IT technical asset management and call logging system in line with ITIL principles.

Infrastructure and IT Solutions & Systems including Research and Project Management

- ✚ Partner with various Directorates to help them from business analysis to automation, upgrading or reengineering existing business processes and business applications / Information systems.
- ✚ Assist to compile business/ project proposals with Technical specifications for innovative cost effective IT solutions to support the Directorates.
- ✚ Assist with tender / procurement and other processes throughout the IT /SCM lifecycle.
- ✚ Assist to evaluate and co-ordinate the implementation of the approved Information Systems.

- ✚ Assist with ICT capital projects from conception to implementation and management including but not limited to operationalisation and maintenance.
- ✚ Maintain, upgrade, implement, operationalise IT systems and databases in a virtual environment or as required.

Disaster Recovery, Business Continuity and ICT Security:

- ✚ Develop and implement Disaster recovery strategy and plan.
- ✚ Ensure that all data is backed-up on a daily basis.
- ✚ Review, improve and implement and manage all various types and levels of computer security.
- ✚ Ensure the UPS and generator can provide sustainable continuity of business.
- ✚ Ensure adequate security of systems and data, both physical and logical
- ✚ Establishment and maintenance of Secondary disaster recovery site including a cloud environment.
- ✚ Cross-skill IT staff to ensure business continuity in instances of a disaster scenario.

Networking:

- ✚ Collaborate with other municipalities, District and Province to share technologies and other resources.

High level IT Services

- Procurement of IT equipment and services.
- Projects co-ordination from start to completion including assisting with all aspects of the tender processes.
- IT Governance throughout the IT lifecycle in a municipal environment – quality assurance, Policy/procedures, IT Strategy/plan – monitoring, management and implementation.
- Assist with procure, deliver, setup, configure, repair, support, maintain, manage all IT equipment with emphasis on Network/server/desktop/Applications equipment/systems and services
- Database Installation, Maintenance and Support and operational administration.
- Knowledge and information strategy, plan, development, implementation, management, maintenance and support and operational administration.
- Business and system analysis and technical documentation.
- Applications support.
- IT security deployment, management, maintenance and operational support.
- IT cabling, deployment, management, maintenance and operational support.
- E-government services including website and intranet systems /applications development, management and administration including SharePoint
- Asset management and change management throughout its life cycle.
- Compile IT Strategy/plan and assist with its implementation.
- Assist with provision of reports as and when required on all IT systems and services and needs.
- Assist with project proposals and implementation, if necessary.
- Assist with the entire infrastructure and end user management of VoIP systems, and CCTV systems in specific and others in general.
- Assist with DRP/BC throughout its lifecycle through review, maintenance, management and administration.
- Integration of various systems through development and enhancement of systems of services.
- Conduct annual penetration testing and resolve all findings within the required period.
- Maintain the Sever room and keep it in a good operational state
- Conduct quarterly vulnerability testing and resolve findings
- Resolve all IT audit findings
- Implement robust IT network to interconnect all municipal sites.

IT OUTSOURCE ORGANOGRAM

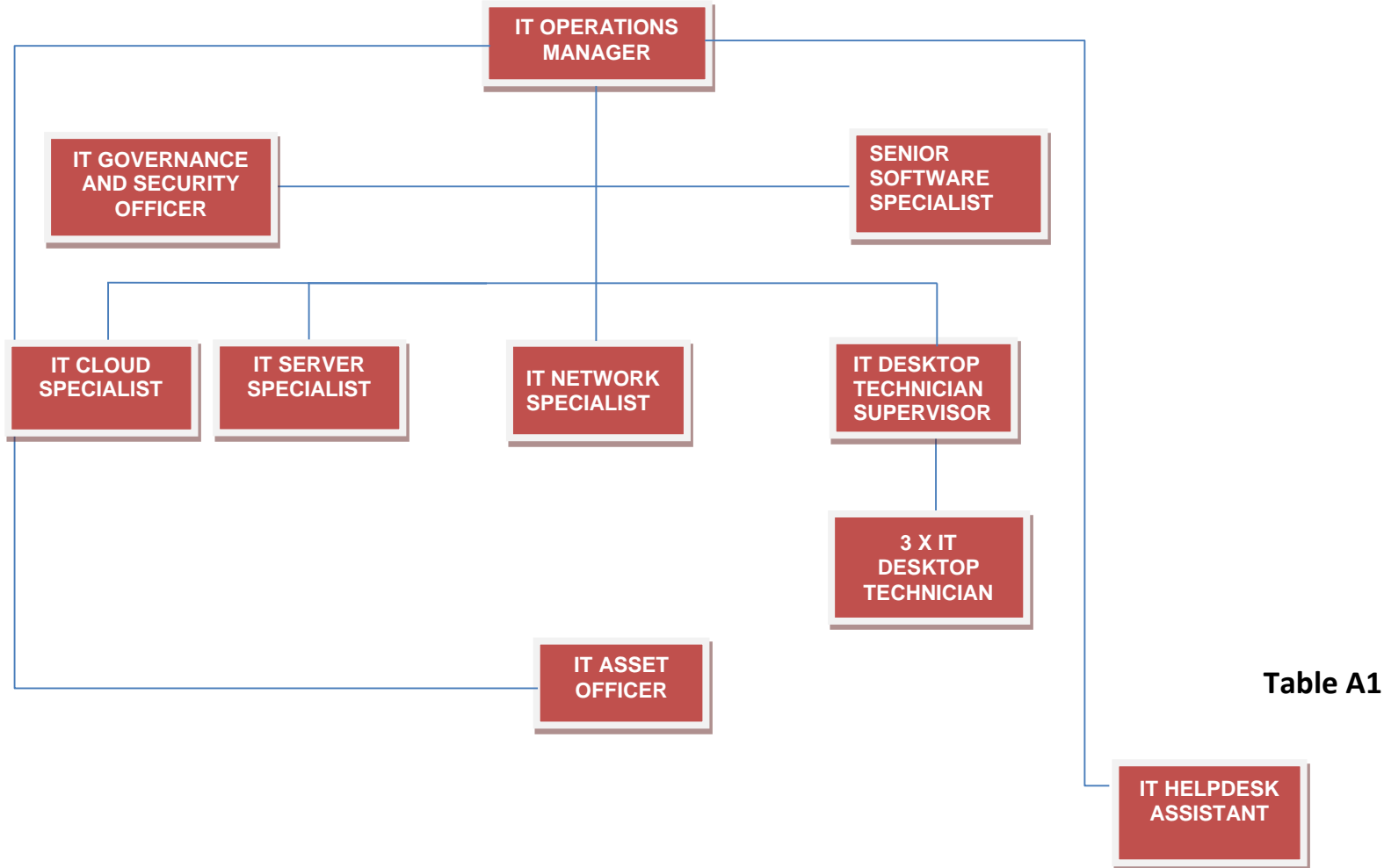


Table A1

ANNEXURE A

High Level Roles and Responsibilities:

The below functions provide a general guideline but a comprehensive site visit must be done by the bidders to acquaint themselves with the systems, solutions and services that need to be rendered as any successful bidder is compelled to ensure that the provision of existing services as a minimum requirement while new systems and services will become part of the ongoing contract.

IT Operations Manager

Activities:

- Ensure the SLA implementation and management between service Provider and the City of Mbombela which includes compliance, Billing, Procurement, Operations, Administration and services.
- Ensure monthly SLA meetings are held and attended.
- Ensure to liaise with and obtain client approval and implement all requested deliverables and projects.
- Oversee, manage and ensure implementation and completion of all requests and projects
- Manage and deliver projects according to agreed deliverables and time frames.
- Ensure the management of contract staff members as well as their respective duties and deliverables. This includes all aspects from tasks to disciplinary processes.
- Ensure 3rd party SMME communication, implementation and deliverables as well as compliance to SLA requirements.
- Ensure client policies, procedures, plans, strategies and requests are reviewed, changed, maintained and implemented.
- Provide guidance on contract matters to contract operational staff, including training to new employees in contracting practices and procedures.
- Advice on new Technologies, products and services which are offered with appropriate, competitive terms and conditions
- Manage on-going issues and change management
- Assist with vendor management on IT related systems and services.
- Assist with all aspects of the entire supply chain processes applicable to IT systems and services from start to finish.
- Assist with IT security in all forms relevant to the environment.
- Assist with all analysis, documentations and reports required in a IT municipal environment.
- Monitor and escalate client complaints / issues Mbombela IT manager/Senior manager.
- Monitor customer satisfaction and minimize SLA breaches.
- Ensure compliance in all functions agreed upon. Report / escalate possible breaches and/or issues to IT manager/senior manager.
- Co-Ordinate, discuss, monitor and evaluate IT solutions and options on projects / services
- Draft, monitor and co-ordinate vendor maintenance schedules and requirements. Initiate maintenance / review processes as and when required.
- Assist and co-ordinate financial system monthly billing and month end processes.

- Attend sectional IT meetings / sessions and provide input / feedback on challenges / issues
- Oversee, Co-Ordinate, monitor and enable inter sectional operational requirements
- Perform operational tasks as approved by Manager/Senior Manager IT
- Provide AG Audit, all committees, forums and management requested and related information and reports for compliancy and correctness.
- Assist with change requests throughout its lifecycle.
- Assist with DRP/BC implementation and compliance
- Supervise operational implementation of IT technical hardware and software systems and infrastructure both capital and operational projects including monitoring, evaluation, review, project management related to the post.
- Vendor liaison at supervisory level
- Ensure weekly time sheets, Weekly plans and supporting documentation for staff are submitted, signed off by sectional supervisors and presented to Manager IT for approval and subsequent review and approval by Senior Manager.
- Co-Ordinate and arrange 3rd party and back-end specialised remote or onsite support as and when required and on approval by Manager and Senior Manager. Ensure vendor tasks are completed and signed off by sectional supervisors. Provide feedback / report to Manager and Senior Manager IT
- Co-Ordinate and assist with procurement requests as approved by Manager and Senior Manager IT. Ensure specifications are obtained and verified by sectional supervisors / vendors / suppliers.
- Oversee and co-ordinate client assets register and requirements.
- Assist with IT Budget planning and monitoring of client approved budget deliverables.
- Assist / co-ordinate and enforce IT control forms and procedures
- Draft, monitor and co-ordinate systems and application license requirements. Initiate renewal / review processes as and when required.
- Attend to an intervention or request from a Senior manager IT(CIO) or manager IT so that the requested intervention is addressed immediately and a call is logged if necessary.
- Perform all tasks requested by the Senior Manager IT (CIO) and manager related to the functioning of the IT section.

Cloud Specialist

- Maintain & monitor on-premises data centers and cloud platforms (public/private cloud).
- Ensure seamless integration between legacy systems and cloud services.
- Manage compute, storage, networking, and virtualization resources.
- Provision, configure, and decommission cloud resources.
- Monitor system performance, uptime, and availability.
- Troubleshoot incidents, outages, and performance bottlenecks.
- Implement identity and access management (IAM).
- Enforce security policies across hybrid environments.
- Ensure compliance with government regulations and data protection laws.
- Manage backup systems and recovery processes.
- Test disaster recovery plans regularly.
- Ensure high availability and resilience of critical city services.
- Develop scripts and automation for deployments and maintenance.
- Support CI/CD pipelines for application teams.
- Use Infrastructure as Code (IaC) tools for consistency.
- Work with cloud providers and hardware vendors.
- Escalate and resolve vendor-related issues.
- Review design and evolve the city's hybrid cloud architecture.
- Monitor cloud spending and optimize resource usage.

- Assist with budgeting infrastructure costs.
- Establish cloud governance frameworks and standards.
- Define best practices for resource usage, tagging, and security.
- Ensure alignment with Municipal IT policies and other Government regulations.
- Evaluate new technologies (AI, IoT, smart city platforms).
- Lead modernization of legacy systems to cloud-native solutions.
- Identify infrastructure risks and implement mitigation strategies.
- Ensure resilience against cyber threats and system failures.
- Plan for scalability as city demands grow and implement relevant solutions.
- Ensure 24/7 uptime for critical infrastructure
- Attend to an intervention or request from a Senior manager IT(CIO) or manager IT so that the requested intervention is addressed immediately and a call is logged if necessary.
- Perform all tasks requested by the Senior Manager IT (CIO) and manager related to the IT section.

IT Governance Officer

- Ensure compliance in all functions related to governance and security. Report / escalate possible breaches and/or issues to Manager IT/Senior Manager IT.
- Co-Ordinate, discuss, monitor and evaluate Governance and security issues.
- Draft, monitor, review and co-ordinate policies, procedures, systems related to Governance and security.
- Attend sectional meetings / sessions and provide input / feedback on challenges / issues
- Oversee, Co-Ordinate, monitor and enable inter sectional operational requirements related to governance and security
- Perform the functions of ISO.
- Ensure clean audit in terms of governance and security and assist to monitor, manage and address all queries.
- Assist with change requests
- Assist with DRP/BC implementation and compliance
- Supervise strategic, tactical and operational implementation of IT security.
- Assist with compilation of tender specs, reports and all IT documentation.
- Vendor liaison at supervisory level.
- Ensure logs are managed and threats addressed daily.
- Ensure all security related systems both logical and physical are implemented and managed.
- Assist with IT Budget planning and monitoring of client approved budget deliverables.
- Assist / co-ordinate and enforce IT control forms and procedures
- Draft, monitor and co-ordinate systems and application license requirements. Initiate renewal / review processes as and when required.
- Perform administrative tasks as approved by Manager/Senior Manager IT
- Assist with AG reports.
- Assist to comply to ITIL, COBIT, ISO, SABS, King IV , Acts/ legislations, other prescripts and directives and guidelines and best practices applicable to the municipal environment.
- Assist with drafting, approval and dissemination of IT policies, procedures, and related information.
- Ensure the compliance to implementation of IT procedures, processes, mechanisms and controls.
- Assist with IT performance management and change management compliance.
- Ensure IT contingency plans are compiled, approved and enforced.
- Assist with needs analysis with users and departments on IT and the compilation and approval of related reports and processes including but not limited to IT strategy and plan.

- Assist with all the processes related to the establishment of the municipality's IT Ethical culture.
- Compile, manage the compliance to IT risk register.
- Providing all information in the required format for audit.
- Assist with training and capacity building on governance.
- Assist with amendment and management of DRP/BC policies, plans, systems and services.
- Assist with IT infrastructure documentation.
- Assist and ensure comprehensive project management to ensure value for money.
- Develop, monitor and manage change management and contingency plans.
- Ensure comprehensive security management from end to end with continuous review and implementation of best practices.
- Develop, implement and update IT Disaster recovery and Business Continuity Plan.
- Compile, assess, and mitigate IT risks and formulate an IT risk register.
- Attend to an intervention or request from a Senior manager IT(CIO) or manager IT so that the requested intervention is addressed immediately and a call is logged if necessary.
- Perform all tasks requested by the Senior Manager IT (CIO) and manager related to the IT section.

Senior Software Specialist

Activities:

- Identify application needs of various Directorates including business / technical analysis in consultation with the Manager/Senior manager IT.
- Research, planning, designing, performance, develop, upgrade, integrity testing, security and troubleshooting of applications and databases systems and solutions.
- Develop tender specs, reports on applications.
- Develop, implement and update IT Disaster recovery and Business Continuity Plan.
- Compile, assess, and mitigate IT risks and formulate an IT risk register.
- Capacity planning of applications personnel.
- Application systems budgeting.
- Assist with identification and Implementation of new applications projects.
- Manage Licenses for all applications.
- Renew licenses and liaise with vendors for installation and activation of all software licenses and certificates.
- Assist with the process of capital and operational projects.
- Provide IT training on applications.
- Coordinate and oversee knowledge and management strategy and systems.
- Assist with applications and integration to all other IT systems including reporting.
- Assist with Design and implement integrated spatial information system.
- Assist with Design and implement E-government services.
- Sharing of information with other Government entities and other stakeholders as instructed by the Manager/Senior manager IT.
- Implement knowledge management systems.
- Consolidate, Process, analyse and report - Business Information systems.
- Assist with Implementation and managing GIS systems/ information.
- Ensure implementation and management of E-Government systems and services.
- Implementation of middleware, interface and integration with all systems including third party systems.
- Virtualisation of systems and solutions.
- Ensure implementation of change management

- Assist Back-Office/Desktop Support with 1st Line support on all information systems such as Payday, ESS, cashdraw, suprema etc.
- Assist with Audit information and reports
- Create, develop, and manage municipal website and intranet web page
- Manage and update SharePoint system
- Attend to an intervention or request from a Senior manager IT(CIO) or manager IT so that the requested intervention is addressed immediately and a call is logged if necessary.
- Perform all tasks requested by the Senior Manager IT (CIO) and manager related to the IT section.

IT Server Specialist

Activities:

- Proactively monitor and manage the servers.
- Server infrastructure – Design, install, configure, implement, support, repair and administer systems and solutions
- Implementation and commission of IT technical hardware and software systems.
- Manage and implementation server projects.
- Monitor, update and assist with asset management.
- Vendor liaison and interaction on technical solution specifications and requirements.
- Compile sever infrastructure analysis, documentation and statistics.
- Research on client requests and find solutions on server infrastructure.
- Ensure SLA compliancy and adherence to client policies, rules and regulations.
- Perform skills transfer and in-house trainings on servers and related systems.
- Implement backup and restore of all severs
- Restore systems and produce restore certificates
- Ensure security support to Business applications and server environment.
- Plan and implement systems administration, software tools and protocols
- Maintain and manage systems and network connections
- Deploy antivirus software to all devices
- Deploy and manage windows updates to all devices
- Management of Active Directory
- Configure, maintain, support and oversee Windows and Linux based servers and SAN storage solutions.
- Troubleshoot server performance, network communication and routing issues.
- Ensure security support to business applications.
- Develop and implement long term strategic goals in systems administration.
- Coordinate with end-users, software professionals and third-party vendors to establish systems administrative procedures.
- Oversee and configure Web, SQL, Exchange, Active Directory, storage and SANS servers.
- Configure and maintain VM environment.
- Take backups of Linux, windows and SAN server, user data and other systems as required and as per policy.
- Handle routine technical, operational and analytical tasks to support customer data systems.
- Interact with users to answer questions and resolve problems.
- Monitor and report application licenses and oversee server load balances and disk space.
- Oversee and assess server efficiency and make associated suggestions.
- Manage users on network, assign application access and maintain workstation configurations as per system requirements
- Voice and Data System Administration functions

- Access control System Administration.
- Develop and update Server related IT policies
- Develop, implement and update IT Disaster recovery and Business Continuity Plan.
- Compile, assess, and mitigate IT risks and formulate an IT risk register.
- Develop and implement IT security management strategies, standards, guidelines, procedures and controls as required in a municipal environment.
- Protect all IT systems and IT related resources in line with IT security policies.
- Educate and train users to comply with IT security.
- Apply patches and updates to ensure all servers and computers are up to date.
- Renew all software licenses and certificates related to the server environment.
- Attend to an intervention or request from a Senior manager IT(CIO) or manager IT so that the requested intervention is addressed immediately and a call is logged if necessary.
- Perform all tasks requested by the Senior Manager IT (CIO) and manager related to the functioning of the IT section.

IT Network Specialist

Activities:

- Proactively monitor and manage the Network Infrastructure.
- Network infrastructure – Design, install, configure, implement, support, repair and administer systems and solutions
- Implementation of IT Network hardware and software systems.
- Manage implementation IT network projects.
- Monitor, update and assist with asset management.
- Vendor liaison and interaction on technical solution specifications and requirements.
- Compile Business and infrastructure analysis, documentation and statistics.
- Research and development on client requests / solutions.
- Ensure SLA compliancy and adherence to client policies, rules and regulations.
- Perform skills transfer and in-house trainings.
- Cisco specialist and solution implementation.
- Ensure security support to Business applications
- Plan and implement systems administration, software tools and protocols for IT networking systems.
- Maintain and manage systems and network connections
- Troubleshoot network performance, communication and routing issues.
- Ensure security support to business applications.
- Develop and implement long term strategic goals in IT network systems administration.
- Coordinate with end-users, software professionals and third-party vendors to establish systems administrative procedures.
- Handle routine technical, operational and analytical tasks to support customer data systems.
- Assist with technical documentation and reports related to the post including but not limited design, development and implementation of systems and services.
- Interact with users to answer questions and resolve problems.
- Oversee and assess network efficiency and make associated suggestions.
- Manage users on network, assign application access and maintain workstation configurations as per system requirements
- Voice and Data System Administration functions
- Access control System Administration.
- IT Security infrastructure- Design, install, configure, implement, support, administer and manage systems and solutions including all accessories.

- Manage all network resources and ensure uninterrupted communication between all municipal sites.
- Develop and implement IT security management strategies, standards, guidelines, procedures and controls as required in a municipal environment.
- Develop, implement and update IT Disaster recovery and Business Continuity Plan.
- Compile, assess, and mitigate IT risks and formulate an IT risk register.
- Protect all IT systems and IT related resources in line with IT security policies.
- Educate and train users to comply with IT security.
- Attend to an intervention or request from a Senior manager IT(CIO) or manager IT so that the requested intervention is addressed immediately and a call is logged if necessary.
- Perform all tasks requested by the Senior Manager IT (CIO) and manager related to the functioning of the IT section.

IT Desktop Technician Supervisor:

Activities:

- Proactively monitor and Manage the Desktop section
- Desktop/Laptop/ cable infrastructure –Install, configure, implement, support, repair and administer systems and solutions
- Supervise operational implementation of IT technical Desktop hardware and software systems.
- Manage implementation of Desktop projects.
- Monitor, update and assist with asset management.
- Compile specifications for end user computers
- Vendor liaison and interaction on technical solution specifications and requirements.
- Oversee and supervise Desktop Support staff and deliverables.
- Compile Business and infrastructure analysis, administrative documentation and statistics.
- Research and development on client requests / solutions.
- Ensure SLA compliancy and adherence to client policies, rules and regulations.
- Perform skills transfer and in-house trainings.
- Develop and implement long term strategic goals for the Desktop Section.
- Coordinate with end-users, software professionals and third-party vendors to establish systems administrative procedures.
- Oversee and configure Operating Systems, Client Applications and office automation applications.
- Handle routine technical, operational and analytical tasks to support customer data systems.
- Interact with users to answer questions and resolve problems.
- Escalate issues to IT Operations Manager with notification.
- Develop, implement and update IT Disaster recovery and Business Continuity Plan.
- Compile, assess, and mitigate IT risks and formulate an IT risk register.
- Send a technician immediately when Senior manager or manager requests intervention or assistance by reallocating the work of the technicians and making sure the requested intervention is addressed immediately.
- Attend to an intervention or request from a Senior manager IT(CIO) or manager IT so that the requested intervention is addressed immediately and a call is logged if necessary.
- Perform all tasks requested by the Senior Manager IT (CIO) and manager related to the functioning of the IT section.

IT Desktop Technician

Activities:

- Deploy, Monitor, Repair, Support and Manage Desktop & Notebook Hardware
- Deploy, Monitor, Repair, Support and Manage Windows Operating Systems [All Versions]
- Deploy, Monitor, Repair, Support and Manage Office Automation Software [MS-Office all versions]
- Deploy, Monitor, Repair, Support and Manage Printers, Scanners, Faxes
- Deploy, Monitor, Repair, Support and Manage Telephony and Data services
- Deploy, Monitor, Repair, Support and Manage Billing and backups [As and when required]
- Oversee and update assigned support service requests.
- Handle daily technical support activities on desktop support.
- Setup desktop computers and peripherals and test network connections.
- Install and test desktop software applications.
- Test computers to ensure proper functioning of computer systems.
- Train end users on usage of computer hardware and software.
- Train end users on cyber security.
- Develop and manage effective professional working relationships with contractor personnel, co-workers and clients.
- Adhere to policies as per corporate manuals and directives.
- Setup computers and install software for various applications and programs.
- Interact with end users on desktop problems and their resolution.
- Maintain computer peripheral devices like printers and resolve associated problems
- Comply and adherence to standard quality procedures.
- Escalate challenges to IT Desktop Technician Supervisor.
- Perform tasks as instructed by IT Desktop Technician Supervisor.
- Comply with SLA targets for Desktop Support.
- Travel to municipal remote sites as and when required.
- Attend to an intervention or request from a Senior manager IT(CIO) or manager IT so that the requested intervention is addressed immediately and a call is logged if necessary.
- Perform all tasks requested by the Senior Manager IT (CIO) and manager IT related to the functioning of the IT section.

IT Asset Officer

Activities:

- Manager inventory for IT assets
- Register and follow up on IT warranty claims
- Assist users with registration of insurance claim with the Municipal Insurance department
- Follow up on IT insurance claims with Municipal Insurance department
- Report progress on IT insurance and warranty claims to Manager IT/Senior manager
- Compile reports on IT assets
- Update asset forms and inform the Municipal Asset department on any movement of IT assets
- Keep stock of IT equipment and consumable and advise on restocking when necessary
- Ensure spare IT equipment is always available (laptops, computers, keyboards, mouse, monitors, RAMs, external hard drives, flash drives, HDD enclosures, switches, routers, cashier printers, projectors, spare projector bulbs, RJ 45 connectors, cables, etc.)
- Attend to an intervention or request from a Senior manager IT(CIO) or manager IT so that the requested intervention is addressed immediately and a call is logged if necessary.
- Perform all tasks requested by the Senior Manager IT (CIO) and manager related to the functioning of the IT section.

IT Helpdesk Assistant

Activities:

- Provide first line support to users
- Coordinate and record new incidents.
- Adhere to troubleshooting steps and escalation process.
- Serve as primary contact for IT issues.
- Handle recordkeeping and logging calls into the municipality's call logging system.
- Escalate problems to relevant section supervisors.
- Report unusual and recurring issues to relevant section supervisors.
- Assist users with relevant forms for their requests.
- Handle requests from multiple sources like email, telephone, voicemail and face to face.
- Present and explain computing support policies to clients and support staff.
- Report on Help Desk service usage and suggest technologies to enhance Help Desk functioning.
- Solicit user feedback of IT services to upgrade service quality
- Resolve helpdesk service calls using documented procedures.
- Support IT staff members on support work.
- Manage Help Desk responsibility and resource allocation to maintain end users.
- Report all challenges to Helpdesk Supervisor
- Solve routine issues and escalate complex issues based on priority.
- Ensure customer satisfaction through continuous status information.
- Attend to an intervention or request from a Senior manager IT(CIO) or manager IT so that the requested intervention is addressed immediately and a call is logged if necessary.
- Perform all tasks requested by the Senior Manager IT (CIO) and manager related to the functioning of the IT section.

Notes:

All personnel to support all 3rd party applications both 1st line and 2nd line support and assist with training and transfer of skills. Full support on all other systems, services and applications must be provided, if necessary, with the backend support from the head office of the successful bidder at no additional cost.

All resources must be vetted and the Municipality will have the right to request immediate termination and replacement of a resource violating security rules.

Additional resources can be procured under the contract as and when necessary, at the same or related costing for similar related services.

Any resource on leave or absent must be replaced with equally or more competent / qualified resource at all times at no additional cost.

DETAILED IT SERVICES

This document provides a comprehensive overview of the service delivery scope for **COM's IT Outsource** function. This document includes the specific details of service delivery. For purposes of this bid the IT Outsource functions are divided into the following functional areas:

- **IT Governance**

Assist with development and compliance to appropriate IT Governance framework and structure with all relevant strategy, plan, policies, procedures and standards to safeguard the business investment and to ensure compliance to legislation and global corporate governance compliance to ITIL, COBIT, ISO, SABS, King IV. All activities in relation to governance must be in relation to organisational structure, job descriptions, skills audit, planning, succession planning, transfer of skills. Other issues include meetings, reviews and engagement protocol.

Assist with compilation, amendment, monitoring, management and enforcement of all frameworks, strategies, policies, procedures and plans

- **IT Asset and Configuration Management**

Assist in tagging, capturing and maintaining information about comprehensive user profiles, products, software licences and services, installed hardware etc., throughout their life cycle and beyond, into a fully interfaced/integrated (with Service Desk, Incident/Problem Management, Release Management, IMACD, Change Control and COM's asset management and HR systems) asset and configuration management system.

Change Management - System to raise changes, record changes, assess impact of changes, develop business justifications for changes, obtaining approval for changes, management and co-ordination of changes, monitoring of implementations, reporting on implementation, closing and reviewing of change requests.

Release Management - Systems to control and document changes to and implementations of application programs (developed and purchased), utility software, systems software, hardware, hardware specifications, procedures, policies, User Manuals.

Asset Database - Create, maintain and manage an IT Configuration Management Database, including the functions of populating, change tracking, updates, data integrity and interface/integration to IMACD process, asset life and cycle tracking to the stage of retirement. Applies to H/W & S/W.

Asset Management Procedures & Processes - Develop, maintain, implement and monitor procedures and processes surrounding the asset management system and database which provides for pro-active (i.e. the system should whenever possible and commercially feasible recognise, flag and update the asset data base whenever asset movement and change take place including tracking of IT assets.

Interfaces - Define and implement interfaces with COM's financial, Service Desk and IT Procurement systems to assist the asset manager in his duties and relevant reporting.

Asset Reporting - Asset Management system to provide standard set of asset reports, plus allow for personalised searches and report generation via the intranet and other means as required by business.

- **IT Procurement**

IT Procurement Services comprises the procurement, management and delivery of IT equipment and supplies in line with municipal procurement processes. This includes research and advising the IT division on various options, obtaining quotations from Municipality's recommended service providers, assisting with evaluation, ensuring the delivery of the equipment/ services to agreed standards while reconciling and managing defective or damaged equipment, manage secure storage, assist the vendor with rollout/implementation, assist with vendor management on the Manager/Senior Manager's request, assist with compilation of reports including but not limited to budget, contract negotiation, manage warranties and agreements.

Assist with requisition processing, order processing and invoices processing. Assist with tracking orders, and compile relevant reports.

Assist with testing and signing off on the roll outs. Assist with asset management and monitoring and reporting as per requirements of the Municipality.

The municipality may procure IT equipment and systems and services from the appointed successful service provider, if necessary.

- **End User Support-** End User Support comprises support for workstation devices, including PC's, printers, scanners, mfp, voip equipment, cctv and laptops. This includes hardware support, software support, interface support, accessories support.

Hardware Support - Provide end user hardware tests, on-site and/or carry-in support up to and including installed network devices. Includes desktops, notebooks, monitors, portable devices, printers, scanners and other approved networked and standalone devices.

Software Support - Provide end user software support, loading and testing, based on number of seats not devices, covering IMACs, standards, maintenance, problem determination and rectification. Includes creation of standardised images. Support selectable from carry in to desk side or to suppliers. Software includes operating systems, office systems, utilities and business applications e.g. antivirus. Supply and apply antivirus updates, routine maintenance desktop activities eg; service packs, security patches, bios upgrades etc. Evaluate new hardware and software products through evaluating continuous monitoring of technical trends, impact analysis and proactive reporting of potential benefits to business. Data migration as necessary. Interfaces - Interface with Asset Management and Service Desk Management systems. Perform pre installation checks and configuration loading, asset tags to new installations of IMACD hardware, warranty management as required, testing of equipment and organising quotes. Installation of new or upgrade software. Utilise centralised electronic, automated software distribution and installation tools where necessary. Perform necessary tests. Provide user notifications /coordination of add/s moves/ changes. Documenting IMACD activity. User orientation erase data as per regulations, repairs and maintenance as necessary. Installation, refurbishment and de-installation of used and new equipment and peripherals. Change configuration settings, collection and managing of configuration settings, Asset disposal as required. Stock control and documentation of change processes and sign offs as necessary. Determine user requirements for new/add/moves/ changes/removal/ disposition and user acceptance testing and quality control as necessary. Updating of the calls as required. Virus eradication. Remote desktop support. Provide user training on hardware or software change or implementation. Report unauthorised software and place copies of approved software on servers, limiting number of concurrent users. Track, evaluate, manage license and maintenance agreements associated with assets and provide reports as necessary. Also provide management reports as necessary.

- **Service Desk**

Provision of a single point of contact for problem and incident logging, first line problem determination and rectification, service requests, escalations, problem/incident and request tracking, information provisioning and reporting. Includes on-going customer satisfaction ratings. Monitor and manage web logging of complaints by users, sms service on request and feedback.

Problems, Incidents, Requests, Information - Service Desk service covering all activities from initial logging through to call closure and customer satisfaction data gathering.

Full service from 07:30 to 16:00 workdays, with the understanding to log calls and initiate corrective action at all other times. Provide a 24 hour VIP service for identified users and/or agreed services such as Billing, electricity prepaid etc. General Standby services are 24x7x365days after-hours and over weekends and public holidays. After hours, weekends and public holiday calls will be automatically routed to standby resources.

Communication to IT management in event of outage etc via communication channels e.g.; SMS. Management of incident resolution within SLA targets. Monitor and enforce service levels with various departments and stakeholders. Assist with basic assistance in the form of training where necessary. Coordinate assistance with third party system vendors on first line support and on emergencies and manage 2nd and 3rd line supports to completion. Testing must be done to ensure optimal cost savings. Remote desktop management and backup recovery must be catered. Develop and implement scripts for users. Ensure corrective actions put in place to avoid repeat incident. Define and document call closure rules and parameters. Perform capacity monitoring and planning for service desk system and resources. Provide service desk, technical training and rollout user training on new hardware and software systems and applications. Produce root cause analysis reports. User profile management processes and accounts including administrative rights. Report and resolve security violations. Submit monthly reports. Do customer satisfaction surveys.

Provide trend analysis reports ,and management reports as and when necessary including statistical reports on various help desk related issues. Develop and document back-up procedures. Conduct regular disaster recovery tests including annual DR failover test. Document DR tests and results.

- **IT Training/workshops** - The provisioning of an end-to-end, managed IT training /workshop service including the scheduling of courses, venue management, presentation of courses, evaluation and reporting on training provisioning and service improvement.

Needs Analysis - Develop needs analysis. Utilise information from Service Desk statistics, applications development teams. Determine and recommend basic skill and knowledge requirements dependant on job requirements. Determine user training needs & maintain user skills database.

Sourcing - Sourcing of training material. Delivery - Delivery of training, including classroom, self-study and the numerous combinations thereof, utilising appropriate recognised adult learning techniques and tools. Provide input to WSP process. IT support staff training and certification. Develop & deliver new training courses for new / existing users. Develop & deliver "refresher" training courses for existing users. Assist with Shortlist and identify preferred vendor partners. Place and track orders in conformance with COM's procedures with vendors - report on order status. Co-

ordinate deliveries with users & make site preparations. Deliver training and provide training material. Develop appropriate tests and accreditation. Develop report formats and provide necessary reports. Report on training provided, success rates, recommended changes etc. Report per completed course, indicating learner satisfaction with course (summary from learner evaluations), number of learners, success rate of learners, recommendations for similar future courses etc.

Servers- For server support maintenance , repairs and services, the service provider will provide a managed baseline service including on-site support, installs, moves, adds, changes, deletes (IMACDs), software distribution, remote server monitoring, operational support and management including repair and maintenance, preventative maintenance, installation of management agents, maintain maintenance orders and requests, logical audit of all software, proactive management of redundancy of hardware and software, update service packs, bios upgrades, security patches. Hardware and software support will apply to in-scope servers including accessories, both current and future. Provide a pro-active managed service including on-site support, centralised software distribution, remote server monitoring and management via a centralised facility, and hardware maintenance according to supplier requirements and good industry practice. Applies to centrally and remotely located servers. Maintain warranty, maintenance, inventory data, and provide necessary linkages and interfaces to Assets tracking and Configuration Management systems. Manage third party hardware maintenance & warranty repairs, Monitoring of automated alerts (e.g. storage, availability) , webhosting, email hosting, Set-up of software on item to be monitored, Maintain warranty, maintenance, inventory data, and provide necessary linkages and interfaces to Assets tracking and Configuration Management systems. Maximum 36hrs downtime per weekend. 99.99% availability on a 24x7x365 schedule. Upgrade individual hardware components. monitor and control the Systems from a dashboard.

- **Hosting** – Physical hosting of COM hardware infrastructure including all servers. Establish and maintain a properly trained and adequately staffed datacentre population, including necessary management and support staff, security, fire protection and disaster recovery site. Setup and maintain DR hosting facilities. Assist with transitioning of existing infrastructure where required. monitor and control the Systems from a dashboard.

Restrict access to data centres to authorised personnel only on. Protect IT resources at all premises from unauthorised access. Conduct periodic reviews of the access logs for unusual occurrences and perform follow-up activities. Prepare and submit a Security Manual covering all required physical security procedures. Perform a baseline inventory of all existing data centre infrastructure. Provisioning of a complete (and discreet) primary hosting and data centre environment including the environmental control and monitoring for COM owned infrastructure. Commissioning and management of a secondary disaster recovery hosting and data centre environment on COM premises. Relocate servers to locations where necessary and reinstall all software and applications as and when necessary.

Support and maintain all municipal information including systems on third party servers, hosted on behalf of the Municipality, where applicable.

- **WAN Data Communications** - Management of the communications related equipment, software and connectivity to and between locations. Includes the equipment, software, circuits, network management platforms and the design required to deliver the WAN services. Support for current TCP/IP, voice, data and video-addressing standards is required. Support for installed and proposed wireless technology is required. Support and provision for remote dial-in access is required. Develop security policies, standards and procedures, assist with design and implementation of new sites and upgrading of existing sites with recognised good/best practice and agreed security policies and procedures., monitor and control the Systems from a dashboard, continually propose and implement connectivity solutions and on-going improvements. Develop and implement IP plan in relation to overall topology, develop and implement long term strategy and plans in line with business needs, Obtain and maintain site details plans, co-ordinates and diagrams. Assist in transitioning the WAN infrastructure to the City's preferred network as and when the service and capacity is available. This is envisaged to happen in a phased approach manner. Provide a full Configuration Management and Change service in accordance with the agreed Change Control process. Manage all activities across multiple suppliers. Implement contingency plans if necessary. Obtain COM acceptance of implemented changes. Perform capacity monitoring and planning, Design hardware system layout, Monitor system capacity requirements for software or hardware limitations. Procure agreed equipment and assist with the entire procurement processes, Development of Statements of Work within agreed timescale, procurement of equipment, propose, develop, implement and manage integration of voice, data and video, provide information and conduct investigations as required, Testing and installation of equipment. Perform quality control on test-to-production results, perform test-to-production tasks per instructions, perform roll-back plans in the event of failure, Update Service Desk details, continually update WAN documents (schematics, geographic) whenever changes occur. Arrange and install and/or manage installation of required connectivity equipment e.g., routers. Configure and test the installed communication links and equipment. Obtain user acceptance of successful installation. Arrange and install and/or manage installation of required connectivity equipment e.g., routers. Configure and test the installed communication links and equipment. Obtain user acceptance of successful installation. Order required and approved connectivity links and equipment from approved carrier equipment provider/s. Determine user hardware /software procurement needs and acceptance test criteria, Shortlist and identify preferred vendor partners as approved by the CIO in line with procurement processes, Place and track orders with vendors - report on o/s order status, Co-ordinate deliveries with users & make site preparations, Obtain and complete necessary licence documentation on behalf of COM, when required to do so. Interact with carrier and equipment suppliers and notify COM of any planned or known disruptions in service provision. Wherever possible notify COM well in advance of the service interruption and in the event of service disruptions due to maintenance obtain COM approval before disruption occurs. Provide day-to-day operational management of carrier and equipment suppliers.

Report, manage and escalate faults of local carrier and equipment suppliers. Perform tasks such as patching, or other manual interventions on hardware connecting to the service provider's network. Provide day-to-day operational management of devices connecting to the service provider's network, Provide on-site technical management whenever maintenance work is required on devices. Manage and implement any emergency changes to the network which are deemed necessary to avoid unplanned disruption to services. Inform COM as soon as possible of potential risk and actions taken to mitigate against the risk. Provide and install software maintenance upgrades whenever necessary and in accordance with agreed procedures. Respond to alerts and alarms issued by equipment and/or when detected by management systems. Provide full TCP/IP and IPX protocol support. Analyse data network trends, evaluate possible impact, and make recommendations for COM's approval to prevent service disruption or degradation. Perform full pro-active network monitoring and management from a central point. Monitor service level targets. Install diagnostic equipment e.g., sniffers as required in consultation and on approval of the Manager and Senior Manager IT. Monitoring of automated alerts (e.g., network failure, availability). Set-up of software on items to be monitored. Provide Service Desk and/or IT management with notification of service changes Inform service desk of service disruptions and the current status; this would include the need to inform the Service Desk when the system is 100%. Inform Service Desk of planned interruptions , test, install and tune system management software, Manage hardware and software to optimise service. Provide technical assistance as requested, Document service-level objectives and agreements, Develop improvement plans. Provide a full management service including managing, troubleshooting, performance monitoring, fault isolation and resolution for all in-scope voice and data services. WAN includes all equipment including internet lines, routers, switches, hubs, fibre lines, analogues lines, pabx, pbx, network related UPS and standby generators. Develop and submit a plan to rectify existing connectivity problems connected by new and technologies, Develop and submit a plan to implement stable connection using available technology to un-connected sites. Implement approved replacement and new site plans. Design, implement, test, monitor, repair and maintain all the wan networks with special references to radio wireless, fibre, etc

- **LAN Data Communications:** Design - Provision of LAN engineering functions including design, capacity and configuration management, optimisation, efficiency tuning, vendor coordination, ordering and installing circuits and equipment, coordinating site surveys and upgrading.

Provisioning of Services - Procurement and installation activities in support of the LAN equipment and circuits that are needed to provide the services. Includes recommendations for power and environmental conditions for such equipment and circuits. All laying and testing of cabling both fibre and copper especially, end to end solution.

Management - Support the operational functions for the LAN including pro-active real-time production monitoring, performance monitoring, tuning, and problem resolution. Includes equipment, cabling, external gateways, up to and including the router port where applicable. Implement performance management and monitoring tools to be used in conjunction with the Service Desk and the Asset database. Encompasses those activities required to continuously evaluate the performance indicators of LAN operations, verify Service Levels, identify actual and potential bottlenecks and establish and report on trends for decision making and planning. Identify future loads on the LAN that could impact performance and propose changes to improve performance in anticipation of future loads. Manage usage and access to LAN services for 3rd parties (e.g. UACs, banks). Support for wired and wireless technology is required.

Design and recommend initial infrastructures and on-going enhancements (if required). Identification of future loads on the LAN that could impact performance, with recommendations to improve performance in anticipation of such future loads. Recommend and implement appropriate operations, management, maintenance and service reporting of the devices deployed on the LAN. Develop and maintain and publish documentation which contains all hardware and software documentation, addressing schema, logical device assignments parameters, connectivity diagrams etc.

Provide connectivity for new and existing end users. Access requirements for new users as they relate to site configurations, overall network topology, network application, connectivity, projected traffic patterns and required performance. Implement services for agreed new users - Recommend connectivity parameters for new users. Tune network design as circumstances and performance trends and analysis dictate. Provide a full Configuration Management and Change service in accordance with the agreed Change Control process. Emergency configuration re-loads including but not limited to Maintenance of configuration records.

Maintenance of integrity of addressing schema. Implement agreed technology maintenance updates, including testing for compatibility with COM's applications. Configure network topologies, Perform capacity monitoring, and planning , Design hardware system layout, LAN bandwidth / response impact / needs analysis, Monitor system capacity requirements for software or hardware limitations , Provide necessary end user training regarding connectivity issues. Procure agreed equipment and assist with the entire procurement processes, Development of Statements of Work within agreed timescale. Assist with delivery and on-site preparations and implementation.

Setting standards / architecture for LAN (cabling, protocols, access security etc) technologies and systems. Provide information and conduct investigations as required. based on site and model configuration. Manage provisioning process involving suppliers and managed 3rd party vendors. Manage and maintain installed equipment. vendors - report on o/s order status , Co-ordinate deliveries with users & make site preparations, Install and implement components according to agreed Change Control and Procurement processes. Manage and maintain installed equipment. Set up addresses & filters , Perform quality control on test-to-production results, Perform test-to-production tasks per instructions, New user set-up, Update Service Desk details. Provide users and Service Desk with basic training regarding connectivity.

Provide a full management service including managing, troubleshooting, performance monitoring, fault isolation and resolution data services. LAN includes from switch port up to and including fly-leads. Provide timely notification regarding scheduled interruptions via the agreed Change Control process. Record faults via agreed Service Desk procedures and track until resolved. Manage LAN environments in a proactive manner via real-time systems if required. Isolate, diagnose and rectify reported and detected faults. Submit to COM root cause analysis reports of faults. Monitor, measure and report on resource usage. Identify capacity thresholds. Recommend techniques and processes to improve performance and reduce faults. Provide on-site technicians as necessary. Develop and implement schedules and procedures for preventative maintenance. Recommend and implement agreed escalation procedures, Manage to resolution 3rd party faults. Recommend and implement agreed Scheduled maintenance procedures. Investigate security breaches. Administer IDs, passwords, and addresses associated with access to the managed networks in accordance with agreed security standards and procedures. Provide all services in compliance with industry standard and government legislated security policies and procedures as advised and agreed with the Municipality at no additional cost. Develop and maintain and LAN maintenance tasks , Responsibility for regular configuration backup of centrally

managed servers (e.g. radius servers), Perform roll-back plans in the event of failure , Manage third party hardware maintenance & warranty repairs , Provide user base with notification of service changes, Maintain automated information distribution requirements , Responsibility for internal and 3rd party repair personnel to maintain service , Test, install and tune system management software , Manage hardware and software to optimise service , Provide technical assistance as requested, Document service-level objectives and agreements , Develop improvement plans , Implement improvement plans. Develop report requirements. Measure and analyse performance relative to objectives and agreements , Report on service-level results , required reports. Provide COM with access to the agreed range of standard defined reports.

Implement approved security policies and procedures. Deleting end user accounts. Modifying user accounts (access rights etc.), Maintain logical security of assets. Conduct periodic security checks per requirements, Report and resolve security violations. Review, recommend and apply latest security standards. Provide and maintain virus avoidance, detection and elimination for IT systems. Assist COM with virus attack response. Manage and maintain all firewalls and gateway devices that connect the service provider's data network to the COM data network that the service provider requires to provide the services. Manage and maintain security controls for internal and enterprise gateway and dialing services and add, change, and delete user access to dial-in services as advised by COM. COM will authorize and approve logon / security level access of COM employees, agent and all contractors including IT services contractor. Maintain physical security of assets. maintaining and update Virus Signature Files for all IT equipment. COM will identify all dial-in services and inter-enterprise gateway services and the authorised users of such services.

- **IT Security Management** - Define, develop, set-up, implement and manage security processes, procedures and systems which will protect COM's physical and logical assets. Provide adequate scheduled reports including changes to policies and procedures, intrusion detection and virus activity with IPS/IDS/NIDS in place.

Management and maintenance of security policies and procedures, reviews of procedures, recommendations regarding changes. auditing, recommending and where appropriate and agreed provision of physical security at identified sites. Review security policies and procedures for effectiveness and recommend improvements. Maintain, update and distribute the security documentation as necessary. Provide physical security controls at all COM facilities. Restrict access to data centres to authorised personnel only. Conduct periodic reviews of the data centre access logs for unusual occurrences and perform follow-up activities. Protect LAN servers and infrastructure devices at all premises from unauthorised access. Implement controls which protect printed output from unauthorised access while under service provider's control.

During the initial period, develop and implement security strategy, plan, policies and procedures with best industry practice for this type of environment especially policies and procedures and recommend improvements.

Review changes made or requested by COM to its security policies and standards and advise COM whether or not such changes can be implemented and if implemented, will be considered a New Service. During the initial period, with COM's assistance, perform a baseline inventory of removable storage media (for example, tapes, disks) for which the service provider has security responsibility.

If requested by COM, restrict access to data processing areas, whether at service providers premises or at COM's facilities, for which service provider has security responsibility to authorised personnel only. Conduct periodic reviews of the data

processing areas for which the service provider has security responsibility including reviews of access logs for unusual occurrences and perform follow-up activities in accordance with documented procedures or as requested by the Manager/Senior Manager :IT). Provide secure storage for removable storage media under service provider's control.

Perform an annual audit and reconciliation of the tapes under service providers control and promptly notify the appropriate COM and service provider personnel if discrepancies are discovered. All backups and restores must be done as per audit requirements, best practices and relevant systems requirements, policies and procedures.

Resolve discrepancies annual tape audit and inform COM of the resolution. Implement controls for and provide effective elimination of residual information on removable storage media before disposal or reuse outside of COM. New user set-up , Deleting end user accounts , Modifying user accounts (access rights etc.), During the initial period, perform a baseline inventory of access IDs for the systems for which the service provider has security responsibility. Provide annually to COM for review (i.e., re-verification) a list of existing COM system logon IDs. Review and verify annually the system logon IDs for the service provider personnel (i.e., re-verification) and delete the IDs of those individuals who no longer have a business need and/or are no longer authorised by management to access the system. Based on information provided by COM, delete the system logon IDs of those individuals who no longer have a business need and/or are no longer authorised by management to access the system. Install, maintain and upgrade new or existing data access control software as deemed necessary by the service provider to provide the services. Implement the functions and features of the access control software that will satisfy COM's security practices as defined in the security procedures documents. - Identify the protection requirements for operating system resources. Implement the protection requirements for operating system resources via the access control software with all changes being scheduled and performed in accordance with the change management process. Capture and maintain audit records for a mutually agreed retention period, and provide record retention reports to COM upon request. Promptly inform COM of any security issues as the service provider becomes aware and recommend possible remedial action. Schedule and notify COM through the change management process of security or integrity software fixes that must be applied to the systems for which the service provider has security responsibility. Establish, change, deactivate, and remove logon IDs and associated access authorities for COM and the service provider personnel. Reset logon ID passwords for COM and the service provider personnel and disclose such passwords to authorised personnel. Review, approve, and grant requests for privileged user authorities. Periodically review privileged user authorities and remove those for which management authorisation no longer exists. Control and be responsible for the security officer/security administrator user profiles on those systems for which the service provider has security responsibility. Perform periodic security health checks to validate, access control settings, authorised privileged users, operating system resource protection installation and operation of virus control programs on the appropriate platforms. Install, manage, recommend firewalls, gateways and other applicable devices and software to provide detection and protection against intrusion and damage from unauthorised external and internal sources. Provide adequate scheduled reports including changes to policies and procedures, intrusion detection, virus activity etc.

- **Applications Support** –application Support, maintenance and projects, as well as interfaces to the Service Desk, IT strategy team, server teams , internal users, integration /interfaces and security. Also included will be project management and third-party management. Includes comprehensive management to allow for remote management and review of software versions and comprehensive SDLC compliance.

Support & Maintenance - Maintenance of existing Applications (existing applications, existing skills etc), bug fixing Enhancement of existing applications - Additional functionality (business requirements, functional specification, technical specification, development, test, implement). New Application Development - Reactive Design & Development catering for new requirements.

Migration of existing applications to newer platforms as required by the Municipality. Maintenance of existing applications, including problem resolution and the application of supplier patches and implementation of new releases - Log problem, assign severity levels and route problem to appropriate area. Investigate problem, define cause, develop or obtain necessary fix. Manage 3rd parties, Implement a workaround if necessary. Test fix in testing environment. Organise and conduct users testing as appropriate. Obtain user sign-off to migrate to production. Plan and migrate from test to production environment. Develop new procedures as necessary to prevent reoccurrence of problem. Submit root cause analysis to COM. Obtain user sign-off for fix. Close incident. Perform quality control on test-to-production results Perform test-to-production tasks per instructions, Document service-level objectives and agreements. Measure and analyse performance relative to objectives and agreements ,Vendor management -coordination of day-to-day services.

Definition and review of user training requirements. Organisation and delivery of developer training courses. Follow-up on developer training quality and effectiveness. Create applications program code, inquiry add-ons and interfaces/integration programs. Conduct testing of module/program & integration. Transfer programs to Quality Assurance. Conduct user test for system conformance to functional requirements & usability standards.

Enhancements- Design, development, testing and implementation of required enhancements resulting from user requirements or pro-active recommendations- Conduct detailed analysis of request. Develop detailed requirements and project plans. Submit analysis, requirements and plans to COM for approval. Develop appropriate training material. Delivery of user training Define and develop appropriate support procedures. Complete development within agreed project timescales and budget. Develop testing plans and submit to COM for approval. Manage and conduct all system testing. Establish user acceptance test environment. With assistance from COM develop user acceptance test scripts and conduct tests. Conduct and conclude required operations testing. Obtain required user acceptance signatures. Develop and plan live implementation. Submit plans for approval. Run pilot tests where applicable. Implement system per approved implementation plan. Conduct required training for users and conduct "train the trainer" courses where applicable. Train the service desk as appropriate. Implement agree enhanced support Obtain final user acceptance of enhanced system, Formally close the project. Perform quality control on test-to-production results , Perform test-to-production tasks per instructions. Document service-level objectives and agreements ,Measure and analyse performance relative to objectives and agreements, Develop improvement plans, Implement improvement plans. Vendor management - coordination of day-to-day services. Definition and review of user training requirements. Organisation of user training courses. Delivery of user training. Definition and review of developer training requirements. Determine detailed functional requirements. Develop functional specifications. Approve functional specifications ,Design data structures and program modules. Create applications program code, inquiry add-ons and interfaces/integration programs. Conduct testing of module/program & integration. Transfer programs to Quality Assurance. Conduct user test for system conformance to functional requirements & usability standards. Ensure system conformance to naming/operational conventions. Install local system components as needed. Provide in-person assistance during initial implementation

period. Provide system and user documentation. Ensure system integration. Perform migration of data. Provide second-level telephone assistance for system in production.

New Systems - Recommendations, functional specifications, design, development, testing, documentation and implementation of new systems and applications, primarily as a result of identified business needs. Perform quality control on test-to-production results. Document service-level objectives and agreements. Measure and analyse performance relative to objectives and agreements. Shortlist and identify preferred vendor partners. Vendor management - coordination of day-to-day services. Establish security requirements. Definition and review of user training requirements. Organisation of user training courses. Delivery of user training.

Definition and review of training requirements. Organisation and delivery of training courses. Follow-up on developer training quality and effectiveness. Define documentation requirements and formats. Provide output in format specified by the COM for support of activities throughout the life cycle of services. Recommend technology platform that best meets business needs, expense & service levels. Identify and recommend development tools according to COM architecture standards in consultation with the CIO. Authorise technology platform and development tools. Determine detailed functional requirements. Develop functional specifications in consultation.

Design data structures and program modules. Create applications program code, inquiry add-ons and interfaces/integration programs. Conduct testing of module/program & integration. Transfer programs to Quality Assurance, Conduct user test for system conformance to functional requirements & usability standards.

Ensure system conformance to naming/operational conventions. Install local system components as needed, Provide in-person assistance during initial implementation period, Provide system and user documentation. Ensure system integration. Perform migration of data. Provide second-level telephone assistance for system in production. Develop package selection process. Check hardware and software standard compliance. Prepare customisation project plan. Perform impact analysis Install package, Test installation Parameterise as appropriate, Test functionality, Post implementation audit and report.

Design, Develop, maintain, upgrade, monitor, test databases and database /web on a 2 or 3 tier applications.

- **Projects** – All IT Projects are managed internally from the IT division and, therefore, will not form part of the pricing for the Outsource Contract Proposal submission, however, resources and services will be from the service provider(s) to support the in-house team in the entire project management processes including conception, design, specifications, bill of quantities, documentation, implementation and rollout and taking over of the management and maintenance of the system at no additional cost.
- **AG reports** – Comply, monitor, report on all AG related information. Resolve all AG queries and findings within stipulated timelines.

IT security: Act as the Municipality's Security design authority, managing the design and documentation of the Municipality's IT securities, encompassing IT organisation and processes, Applications, Network and application services, Operating systems, Network, Establishing IT Security Policy in line with the Municipality's Information Security requirements, Work closely with the Information Governance Group and acts as the main point of contact and expert advice for information security for the Municipality, assuring the provision of

information security management in accordance with the municipality requirements, relevant standards and best practice, Take responsibility for the day to day operational effectiveness of the Municipality's IT security and compliance with responsibility for Assuring the confidentiality, integrity and availability of the Municipality's electronic information, Development of policies and procedures , Security incident management and reporting, Investigation of security breaches, Investigation of unauthorised access and the initiation of risk control measures, Provide expert advice and related information governance matters, representing the Municipality regarding IT security at various external forums and reporting to the corporate information governance board on information security matters, Drives the strategic development of the IT security function, by the development, maintenance, promotion and stewardship of the IT Security Policy, in accordance with Members' requirements and legislation including policies and procedures. Conducts an annual review of the IT Security Policy, Formulates guidelines and standards in liaison with Municipal staff and external organisations at all levels, Manages the selection, design, justification, implementation and operation of information security controls, management strategies and standards, enabling effective assessment of risks to information integrity, authentication, and confidentiality, combating virus attacks, network hacking and system misuse, Advises all functions in Service Development and Service Delivery on the application of security controls, Promotes and assists in the implementation, where practicable, of procedures designed to attain compliance of the ISO27001, ISO20000 (ITIL) and other relevant ICT standards. This will involve establishing security processes that can ensure compliance and accreditation with ICT security best practice, Monitor international and vendor sites for security updates, Advises on the potential impact on existing access security mechanisms of specific planned technical changes, in order to help ensure that potential compromise or weakening of existing security controls is minimised. Also assists in the evaluation, testing and ensures implementation of such changes, Ensures that processes for starters, leavers, changes, password resets, remote and wireless access authorisation, VPN, etc provide robust and timely assurance of the Municipal's information, advising IT colleagues and others on best practice in the day-to-day operation of security related software and hardware, Negotiates with 3rd party suppliers in liaison with the Supplier Relationship Manager in relation to security requirements including confidentiality agreements and compliance with internal policies, Ensures the protection of systems and information in storage, processing, or transit from unauthorised access or modification through the denial of service to unauthorised users, Acts as a Registration Authority under the Municipal's procedures including the liaison with the Municipal's Certifying Authority with regard to the issuing, suspension, revocation and archiving of digital certificates, Advises users on risk reduction and promotes awareness of policies and procedures. Ensures that users are aware of obligations such as protecting the secrecy of passwords and accounts access details, Provides advice regarding training courses in relation to new IT related legislation and compliance with the Municipal's Corporate IT Security Policy working towards ISO27001. Conducts information security awareness sessions, Manages monitoring compliance with the Municipal's Information Security Policy and adherence to legal and regulatory requirements. Liaises with internal and external service providers to obtain reports in order to check entitlement of those accessing information and providing support, Manages monitoring system and other monitoring logs to identify potential anomalies or breaches of security or policy and similarly to discover and report potential issues that need control action. Investigates security breaches, including offensive or indecent material, and reports such incidents immediately to the appropriate authority, Conducts security risk assessments for business applications and computer installation and provides authoritative advice and guidance on security strategies to manage the identified risks, Manages the security incident process, reviewing security incidents, weaknesses and malfunctions relating to the Municipal's systems, taking appropriate remedial action. Liaises with service delivery staff on IT forensic investigations. Perform vulnerability assessments and penetration tests. Resolve all issues from vulnerability assessments and penetrations tests. Provides evidence and advice to senior officers in disciplinary investigations, liaising with the SAPS as appropriate, Takes the measures necessary to detect, document and counter threats to the integrity of stored information. Assesses the effectiveness of firewalls, SMIs (Smart Managed

Interfaces), Gateways, IDS (Intruder Detection Systems) and IPS (Intrusion Prevention Systems) to improve network/system resilience. Seeks to assure integrity of system interconnectivity, Monitors the effectiveness of security installations and investigates those not achieving design aim or business requirement, making appropriate recommendations for change or remedial action as described within the Work Commissioning Framework, Produces procedural advice to those involved in investigations involving IT security abuse; ensure that disks or archives are imaged and managed in a method that is forensically sound, collate information and carry out related tasks and to provide information when necessary, Ensures consistency between information security strategy with Data Protection and other relevant legislation. Assists the municipal with Information Governance initiatives including legislative compliance, records management and the appropriate use and storage of data, and also information security aspects of disaster recovery and business continuity, Contributes to Disaster Recovery and Business Continuity planning, testing and maintaining documentation as required. Provides feedback to enable improvement of such plan, Assists in the execution of and managed responses to various internal and external audit activities of information security for the whole of IT and other areas of the business as required. Responds to all enquiries relating to information security and contingency planning, Manages the creation and maintenance of auditable records, user documentation and security awareness literature for the IT security management function, ensuring that the records provide a comprehensive history of violations, resolutions and corrective action, Ensures that inventories of hardware, software and information holdings are available and kept up to date and are reflected in or incorporated in the Configuration Management Database (CMDB), Ensures the comprehensiveness of information provided on incident records. Contributes to knowledge bases (including Frequently Asked Questions) in undertaking duties., Analyses work in progress, takes action to ensure time-to-fix targets are met within safety and quality procedures, including hand-over to client where appropriate, Represents the Municipal at various inter-organisational forums, user groups, external IT seminars and meetings with third party suppliers regarding information security as required, Acts as a specialist advisor writing reports and presenting findings to the Information Governance group and IT Management Team on information security issues and advises on new initiatives, technologies and compliance issues, Serves as a member of the Change Advisory Board to provide security specialist input when necessary, Contributes to the work of the Service Development section and the overall IT service working in collaboration with peers and, Delivers the priorities set out in the IT Team Plan and overall targets and aspirations of the Department as defined in SDBIP by implementing designated objectives, Ensures compliance with standards, Provides performance data in a timely and accurate manner using appropriate tools, Implements the Municipal's Core Values and Leadership and Management Framework, Motivates, trains and empowers staff to optimise their skills and output, Complies with responsibilities under the Information Security standard and any other standards that the Municipality adopts, As directed, undertakes such additional duties and responsibilities that may arise from time to time and are commensurate with the grade of the post.

N.B.: IT MUST BE NOTED THAT SOME OF THE FUNCTIONS MAY BE PART OF MORE THAN ONE PERSON'S JOB DESCRIPTION AND ALL ABOVE FUNCTIONS ARE A MINIMUM REQUIREMENT AND IT WILL BE EXPECTED OF THE SUCCESSFUL BIDDER TO INCLUDE ADDITIONAL FUNCTIONS NECESSARY TO ENSURE OPTIMUM LEVEL OF SERVICES FOLLOWING THEIR ASSESSMENT AND SITE VISIT.

OTHER APPLICATIONS / SYSTEMS WILL BE ADDED AS AND WHEN REQUIRED DURING THE CONTRACT PERIOD FOR SUPPORT AND MAINTENANCE.