POLICY : INFORMATION TECHNOLOGY

ITEM CL 129-2001
MC 4.5.2001

DEPARTMENT: CORPORATE AND LEGAL SERVICES -INFORMATION TECHNOLOGY DIVISION: PROPOSED POLICY DOCUMENT FOR THE EKURHULENI METRO

RESOLVED:

(a) **That** the proposed Information Technology policy document for the Greater East Rand Metro (Ekurhuleni Metropolitan Council) as set out in **ANNEXURE "A"** attached to the report, **BE NOTED**.

(b) **That** the proposed policy mentioned in (a) **BE IMPLEMENTED** with effect from July 2001.

(c) That the Chairperson of the Corporate and Legal Services Portfolio Committee, Councillor N A Hassan and the Chairperson of the Finance Portfolio Committee. Oft M K Sambo meet on a date and time to **BE DETERMINED** by the Interim Head: Corporate and Legal Services.

EKURHULENI METROPOLITAN COUNCIL

ANNEXURE 'A'

EKURHULENI INFORMATION TECHNOLOGY POLICY

(1) IT EQUIPMENT AND HARDWARE

(2) IT NETWORK SECURITY

(3) IT CENTRE ACCESS SECURITY

(4) IT HUMAN RESOURCES DEVELOPMENT

(5) IT SUPPLIES

(6) IT SYSTEMS DEVELOPMENT IN HOUSE

(7) IT SERVICE PROVIDERS AND CONTRACTS

(8) SYSTEMS SECURITY

(9) DECLARATION OF ALL GIFTS RECEIVED

(10) SOFTWARE PURCHASED

(1) IT EQUIPMENT AND HARDWARE

1.1 (a) Gradually phase out all generic or clone machines.
- (i) Machines assembled with many different parts from various suppliers.

(b) Purchase machines from well recognized suppliers and good brands.
- (i) Machines assembled with one-type supplier parts.

(c) Adapt to purchase one uniform capacity machines.
- (i) All machine workstations should be 128 MB RAM, compared to currently being between 15-21 MB RAMS.
- (ii) All workstations motherboards should be at least 133 MhZ speed, compared to 66 MhZ.
- (iii) Hard drives must be at least the minimum size available at that period, compared to 500 MB – 1 GB.
- (iv) All network cards should have a speed of at least 10-100 MB and from a selected brand, e.g. 3COM, and not 10 MB RAM.
- (v) VGA and sound cards optional extras.

1.2 (a) All rooters and switches should be purchased from well recognized companies, e.g. 3COM, to maintain uniformed product.
(b) Capacity should be from 10-100MB speed.
(c) LAN connection should be made from UTP cable.
(d) All LAN or WAN should be derived from uniformed topology.

1.3 Printers should be bought from efficient companies.

(2) IT NETWORK SECURITY

Develop policy on network security:

(a) Authentication of users to network.
(b) Group users, according to departmental work and accessibility.
(c) Installation of firewall.
(d) Policy on modems connection:
- (i) All modems used by external developers should be kept off.
- (ii) Switched on only as per request for control sheet changes.
- (iii) IT administrator must record periods of switch on occasions.

(e) N.B. Specifics to PQ-Africa dial up line.

PQ Africa dial up line:
- (i) Modem has to be switched off all times.
- (ii) PQ-Africa has to phone for any connection, and indicate the following:
  - Change control request number.
  - The person who requested that change control sheet.
  - Indicate changed to be effected.
  - Record the name of a person to effect those changes, e.g. PQ programmer.

(iii) Logbook has to be kept in place to record the above details.
- Date of phone request from PQ-Africa.
- Person who made request from EGSC and related department.
- Type of changes to be effected.
- Change control number.
- Completion date of changes.

(iv) All change control sheets have to be certified by requested person when completed.

(v) All departments should select one person to be responsible for change control sheets.

(vi) All change controls must be sent to the IT department for payment verification, for recording and completion monthly.

(vii) All change control sheets has to be compared to monthly billing and payments, to PQ-Africa.

(3) IT CENTRE ACCESS SECURITY

(a) Installation of combination locks.
(b) Combination locks numbers to be known by IT personnel only.
(c) Always have one IT staff member in the data centre.
(d) Data centre should not be left unattended during working hours.
(e) All visitors should wait at reception centre.
(f) Only IT staff should be allowed in the data centre.

(g) All visitors that are engineers, technicians or post office workers, should work under supervision of IT staff.

(4) IT HUMAN RESOURCES DEVELOPMENT

(a) IT staff should attend at least 2 courses a year.
(b) A program of mentoring staff members should be in place.
(c) Outsource all staff mentoring and training to efficient and well-established companies.
(d) Students should be romped in for practical knowledge once a year, e.g. for community development.
(e) IT to adopt community development.
  (i) Get staff engaged on community education.
  (ii) Get staff engaged on student development from community.
  (iii) Above to be done in order to address staff shortage.

(5) IT SUPPLIES

(a) Supplies should be derived from more disadvantaged companies.
(b) Supplied hardware should be verified according to the specifications.
(c) All supplied hardware should be checked against lively wood expectancy.

(6) IT SYSTEMS DEVELOPMENT IN HOUSE

All in house systems developed by staff should remain the Metro property.

(a) These systems should not belong to certain individuals.
(b) Systems developed should be documented for verification and be accessible by all software developers.
(d) Uniformity of systems should be maintained:
    (i) Systems used in one area, should be available to the whole Ekurhuleni Metropolitan Council.
    (ii) Developers should not be permitted to use the Metro resources in order to create their own scripts for private use.
(e) All developed software should remain the property of the Ekurhuleni Metropolitan Council.

(7) IT SERVICE PROVIDERS AND CONTRACTS

(a) For Finance policy purposes, all contracts must be in writing.
(b) Contract scripts should be filed and accessible to senior officials, e.g. Departmental H.O.D.
(c) Service providers requests:
    (i) All change control requests should be verified by the administrator in the IT department.
    (ii) All change control requests should be logged down and used as a reference on payments to the service provider.
    (iii) No change controls should by pass the IT department in order to meet payments demand.
    (iv) Change controls executed via modem, should be notified at the IT department, because the modem is always off until a request comes forward.

(8) SYSTEMS SECURITY

8.1 Select NT 5 - Windows 2000 Professional to avoid security violation.

(a) No logging into systems without authentication, if network can't recognize you, machine will halt.
(b) Users can't move around offices to login on somebody else's machine. This will keep users working at their own desks.
(c) Users won't be able to run any unauthorized jobs.
(d) Users won't work offline on machines because they won't be able to use cancel button. They will be forced to login.
(e) Users will be disabled to use stiffy and CD drivers. This will stop users from copying sensitive information and from loading illegal software.
(g) Users won't be able to access unauthorized function, e.g. e-mail (unless loaded), pornography.
(h) All software purchased for Ekurhuleni, should first be approved by IT department. This will result in uniformity of software in the whole Metro.

8.2 Copy information from systems.

All stiffy drivers should be disabled. To avoid the following:
(i) Copying of sensitive information.
(ii) Loading illegal, software.
(iii) Playing games from stiffy.
(iv) Viruses from spreading.

8.3 Anti-Virus

(a) Should be loaded on every server, and run from servers to workstations.
(b) All e-mail servers should have anti-virus running.
(c) All other servers to have anti-virus running.

8.4 Firewalls

All IT centres should have firewalls, to prevent hackers from accessing the IT department.

8.5 UPS

All IT centres has to be linked to UPS.
(i) To prevent data loss.
(ii) To prevent hardware damage on power dip.

(9) DECLARATION OF ALL GIFTS RECEIVED

All gifts received from suppliers has to be declared to the Metro:
(i) Stop officials being corrupted.
(ii) Stop suppliers notion that if they give a gift, they would be the sole supplier to the Metro.
(iii) Prevent low quality of hardware in the Metro, supplied because of special favour.

(10) SOFTWARE PURCHASED

(a) All software has to be purchased through the IT department, to avoid Duplication.
(b) Software should be uniformed, no different software should be allowed in the Metro.
(c) Uniformed software is cheap to maintain, easy to train and adopt.
(d) For security reasons Ekurhuleni should use Windows 2000 Professional.
(e) All software should be compatible to all business partners, e.g. Government, Gauteng Province and Receiver of Revenue.
(f) No Ekurhuleni Metro official should be allowed to create software which would render the Metro depending on one specific official.
(g) All software development should be done by well recognized companies who can maintain and perform innovations on that particular software.
(h) Officials should not be permitted to create software and keep the Metro at ransom if they are not happy.

ITEM IT 1-2002 **INFORMATION TECHNOLOGY MANAGEMENT POLICY 2002-2003**
MC 4.4.2002

RESOLVED

(1) **That** the proposed IT Management Plan 2002-2003 for the Ekurhuleni Metropolitan Municipality, attached to the report as **Annexure 'A'**, **BE NOTED**.

(2) **That** a further report on an implementation programme for the plan referred to in (1) above, **BE SUBMITTED** to the Mayoral Committee.

ANNEXURE 'A'

TABLE OF CONTENTS

POLICY RESPONSIBILITY PER COUNCIL:

	POLICY:	PERSON RESPONSIBLE:
1	Introduction and Compilation of Policy	N. Mathabathe
2	IT Management/Strategy and Support Policy	S. Ngwenya
3	Information use Policy	A. Hofer
4	IT Architecture Policy	N. Arnoldi
5	User Access Policy	J. Reis
6	IT Development Policy	G. Ramashala
7	IT Tender and Evaluation Policy	R. Baljeko
8	IT Standards Policy	M. Vorster
9	IT Backup and Disaster Recovery Policy	T. Kotze
10	IT Helpdesk Policy	B. Muller
11	IT Asset and License Policy	L. De Jager / B. Linde

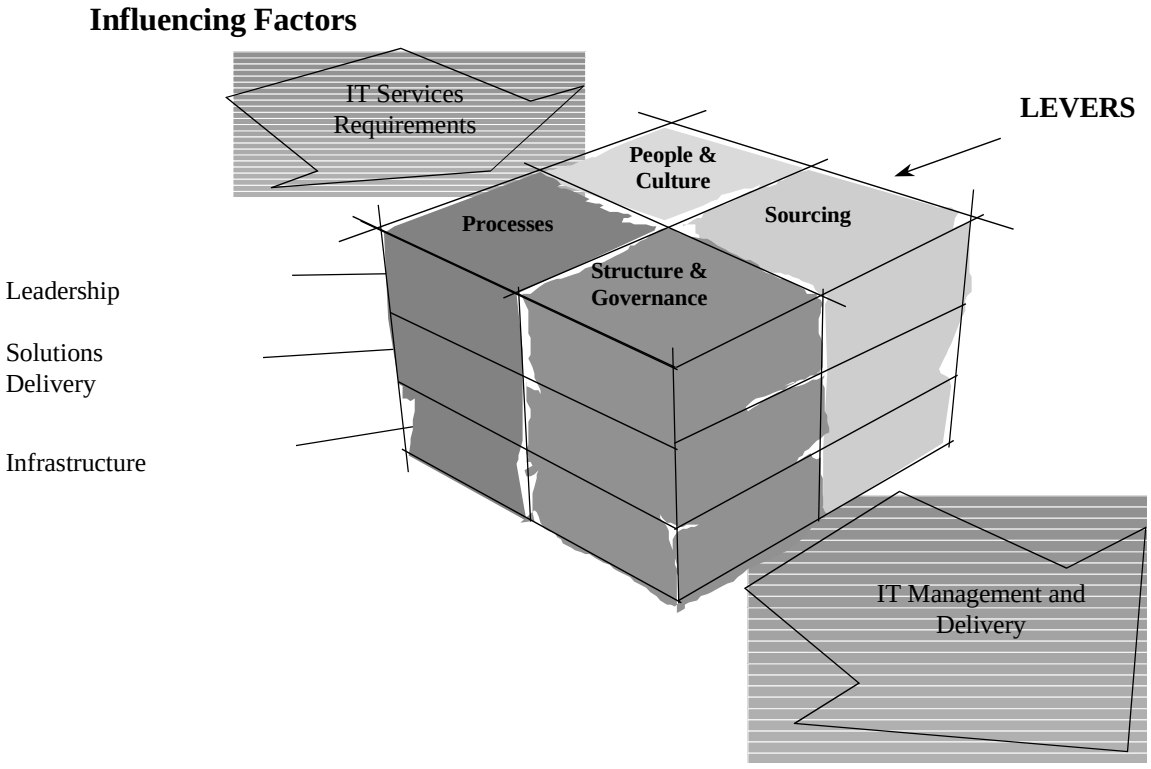
THE IT POLICY AND IT VALUE DISCIPLINE

Introduction

Advances and innovations caused by information technology have and will continue to dramatically change the competitive landscape over the next 10 years. Traditional value chains and business models for all market segments and industries will be impacted. New competitors will possess unique infonomics capabilities and skills enabled by being connected to their customers and suppliers. Forces of globalisation, industry consolidation and regulation, together with the more direct political and social economic demands imposed by national, provincial or local players are paramount in understanding the impact and importance that they may have on a business. Business leaders will be compelled to employ revolutionary techniques for calculating business valuation (e.g. collaborative coefficients) based on informational assets. Hence, information is emerging as the critical factor of production in competitive markets.

However you cannot change the IT solutions or infrastructure every time the business has to change. Therefore enterprises must increasingly subsume non-differentiating business processes and establish information source capabilities that will facilitate concepts of data warehousing, data mining, geographical information systems, and any other type of information mechanisms that will span the next business chasm. Paramount is the ability of the IT function to position itself strategically and structurally with the business functions.

The Ekurhuleni Metropolitan IT Managers (IT Steering Committee) have developed and compiled an IT POLICY document with the aim to focus and amalgamate the current different IT technologies and standards deployed in the separate Councils that make up the new Ekurhuleni Metropolitan. Additionally, the IT policy aims to enable and support the metropolitan's strategic business plan and to accommodate the integration of technology and commerce.



As can be seen several factors influence IT's ability to undertake an efficient, effective and an enabling IT Management and Service delivery. The IT policy documents endeavours to address initially some of these factors.

This IT policy document must be seen as the first version of an ongoing work document to be updated as and when it is deemed to be necessary. The IT policy does not therefore try to prescribe or enforce specific aspects of information technology issues, but should be seen as an attempt to ensure tenable, working IT solutions spanning across the metropolitan, the service regions and respective departments.

Purpose and Importance of the IT Policy

The IT policy documents hopes to achieve the following objectives:

- Refocus information technology management to support directly the metropolitan strategic objectives

- Determine co-operation in the use of information technology across all departments and sub-structures, to improve the productivity of metropolitan resources and to promote a co-ordinated, interoperable, secure, and shared metropolitan infrastructure
- Significantly improve the management of information systems
- Significantly improve the acquisition of information technology equipment and software solutions

It is important that this policy requires support from both the executive and functional management structures without which this policy can neither be implemented nor used effectively.

Structure of the IT Policy

The IT policy addresses various aspects of the information technology and has been subdivided into the following more manageable sub-sections, namely:

1. IT Management/Strategy and Support policy
2. Information Use policy
3. IT Architecture policy
4. IT User Access policy
5. IT Development policy
6. IT Tender and Evaluation policy
7. IT Standards policy
8. IT Backup and Disaster Recovery policy
9. IT Helpdesk policy
10. IT Asset and License policy

Each of these policies are discussed in more detail below.

IT MANAGEMENT/STRATEGY AND SUPPORT POLICY

Policy name:	IT MANAGEMENT
Reference number:	
Date of last update:	29/05/2001
Circulation to:	All IT Management and personnel
Brief description:	Converge all IT resources, e.g. Hardware, Application, Networks in alignment with Metropolitan Business Strategy
Scope:	All Ekurhuleni Metropolitan Council areas
Objective:	Unify all IT Admin Units

IT MANAGEMENT/STRATEGY AND SUPPORT POLICY	
Detail Description:	1.1 IT has to converge all the IT components, namely Hardware, Software, Networks, Human Resources, Data and Utilities. 1.1.1 Converging of all the IT resources would fulfill the notion of achieving saving in the output of IT results. 1.1.2 IT has to compliment the Ekurhuleni Business strategy, to achieve the main National Governments plan of service delivery. 1.1.3 IT must continue growth and development on interpretation of Ekurhuleni Metropolitan Council business strategy. 1.2 IT has to adopt the three service delivery areas of the Metropolitan business plan identified by the Council. 1.2.1 Setup and determine functions in SDR's according to the Council business plan. 1.2.2 Organize key performance functions. 1.2.3 Allocate Human Resources according to skills function requirements. 1.2.4 Acquire and put in place peripherals as per function requirements. 2. Determine and maintain short-term achievable strategy 2.1 Applications have to be standardized. 2.1.1 All eleven admin units must agree on one software application, namely : Windows, Financial System, Library, Health, Engineering, etc. 3.1 Streamlining all applications and hardware. 3.2. Streamlining all resources and peripherals to achieve the ultimate goal of delivery for the Ekurhuleni Metropolitan Council. 3.3 Meet the demand of Business, and enable the capability to provide Metropolitan wide payments. 4. Scale up infrastructure (spend increase). 4.1 Infrastructure should be checked against deficiency in order to produce efficient results. 4.2 Reduce redundancy by examining every peripheral performance standard. 4.3 Always work in conjunction with the Council business strategy, aligning IT functions to Ekurhuleni Metropolitan Council community delivery strategy.

IT MANAGEMENT/STRATEGY AND SUPPORT POLICY	
Detail Description	4.4 Immediate goal should be to obtain best equipment in IT in order to Achieve service delivery. 4.5 All peripherals should be gradually standardized and phase out all generic or clone machines. 4.6 Machines assembled with different components should be gradually discarded. 4.7 Network connection components should be of a good grade, to fulfill the E-Government objective from Local Government through out to National Government. 4.8 Rooters and network cards should comply with standards and follow the scope of procurement policy. 5. Determine long-term achievable strategy. 5.1 Rationalize IT assets and resources. 5.1.1 Make all IT assets and resources equally as per function requirement 5.2 Obtain details of National Government policy for Local Government IT and work within the mainframe. 6. IT Management. 6.1 Must provide guidance for the future, and set a broad framework that will promote the progressive convergence in technology and management practices, of the individual founding municipalities. 6.2 Should devise staff organogram. 6.3 Determine overall IT functions. 6.4 Ascertain skill requirement. 6.5 Acquire suitable skills. 6.6 Determine future skills requirements. 6.7 Train staff in designed programs. 6.8 Determine short, medium and long-term goals of IT. 6.9 Consider costs, benefits, risks and constraints of these goals. 6.10 Examine results of not adhering to ultimate strategies. 7. Human Resources 7.1 Develop IT related staff development program. 7.1.1 Implement compulsory training development for all IT staff, within the Budget limit. 7.1.2 Implement public participation of staff training and institutions.

IT MANAGEMENT/STRATEGY AND SUPPORT POLICY	
Detail Description	7.1.3 Allow internship of students from public institution. (a) Determine the scope of internship in conjunction with educational Institution. (b) IT to adopt students from selected educational institutions indiscriminately. (c) IT Management has to endorse impart skills or perform mentor program. (d) Policy of transparency has to be adopted by every IT Managerial person to support and enhance IT staff in Performing their duties. 8 System processing 8.1 Procedures and standards should be documented and safely kept by the IT Manager. 8.2 Execution of daily and monthly procedures should be scheduled and constantly evaluated by Management to retain stability of IT data integrity. 8.2.1 Execution of daily and monthly procedures should be scheduled and constantly evaluated by Management to retain stability of IT data integrity. 8.2.2 Operational processing should follow standardized roaster, designed by IT Management, as per job schedule according to application requirement. 8.2.3 Approach implemented in IT operational areas should always complement the Business strategy of Ekurhuleni Metropolitan Council. 8.2.4 Daily procedures must be determined according to key performance areas requirements. 8.2.5 Monitor and scrutinise service delivery to all departments and any other entities receiving services from IT. 8.2.6 Identify areas where service levels are not according to agreed service levels or service objectives and improve services to desired service levels. 9. Budgets 9.1 CIO department has to co-ordinate IT budget. 9.2 Formulation of IT budget committee has to be done including IT Management. 9.2.1 Budget committee should be derived from all departments, to achieve all-inclusive participation of department. 9.2.2 Departments should be assisted to construct a good and efficient budget. 9.2.3 IT Workshop Budget with various sections on the following items, Hardware, Software and Training. 9.2.4 Final analysis of current expenditure and projected budget should be implemented on budget strategy.

IT MANAGEMENT/STRATEGY AND SUPPORT POLICY	
Detail description	9.2.5 Budget to be derived from users and IT requirements. 9.2.6 Users should be permitted to retain their Departmental IT Budget. 9.2.7 Budget draft should be started at an early stage to allow amendment period. 9.2.8 Before the Council approves the IT budget, the IT budget committee should verify it. 9.2.9 IT budget committee should approve all purchases of IT equipment. 9.2.10 Standardized format must be applicable to all IT equipment purchases.

INFORMATION USE POLICY

Policy name:	INFORMATION USE POLICY
Reference number:	
Responsible person:	André Hofer
Date of last update:	22/05/2001
Circulation to:	All IT and user personnel employed or otherwise contracted to the Ekurhuleni Metropolitan Council
Brief description:	The Information Use Policy provides a framework for giving guidance and understanding in the use of business resources made available to Personnel in their execution of business duties
Scope:	Applicable to all Personnel and Information Systems in the Ekurhuleni Metropolitan Council
Objective:	The following objectives are applicable: • To lay down a regulatory framework regarding the purpose of the IUP • To ensure that individual and group behaviour is consistent with the Council's expectations and with the requirements of any applicable legislation and regulations • To ensure adequate use of the Council's systems, equipment and resources, so that the Council's activities are carried on in a manner consistent with its mission and tend to constantly maintain, enhance, and promote its image and reputation • To provide, encourage and maintain within the Council an environment which is healthy, peaceful, safe and respectful of collective and individual rights • To encourage positive participation by those affected by the IUP during the planning, design and execution of the Council's operations • To provide those who are affected by this IUP with the means and tools to fulfil their task, to perform their activities and to assume their responsibilities in a fully effective manner

INFORMATION USE POLICY	

Detail description:	• Compilation and review of Information Use Policy
	  • This Policy is created by the current incumbent Information Technology (IT) steering committee representatives from each local council under the auspices of the Ekurhuleni Metropolitan Council
	  • The Policy will be reviewed on an annual basis by the IT steering committee, or any such designated committee, or as otherwise requested by the Council
	• Applicability of the IUP to Information Systems by Personnel
	  • The Policy is applicable to all Personnel and Information Systems at all times as defined in the definitions
	• Usage of the Information Systems is governed by the following principles, as defined in the definitions:
	  • Non violation of Copyright
	  • Non violation and protection of Intellectual property
	  • Non violation and protection of Confidentiality
	  • Adherence to Security
	  • Awareness of Public image
	  • Warranty of Data integrity
	  • Non violation of Usage Rules
	• Notification to Personnel of IUP and obtaining signed undertakings from Personnel of IUP
	  • All current Personnel will be requested to sign individual undertakings in favour of the Council agreeing to the terms of the Policy
	  • Procedures must ensure that all new Personnel are requested to sign individual undertakings in favour of the Council agreeing to the terms of the Policy
	• Usage rules of Information Systems by Personnel:
	  • **General use** – The use of Information Systems or resources requiring no formal authorisation or approval but adhering to the following principles:
	  • Information Systems or resources provide will remain the property of the Council.
	  • Information Systems or resources will in principle only be used for business purposes and are deemed in all events to be business orientated.
	  • Personnel must adhere to all Information Systems security policies and processes.
	  • Personnel are to conduct themselves in a professional and responsible manner, which do not detract from the Council's public image.

INFORMATION USE POLICY	
Detail description (Cont):	• All correspondence, in written, electronic or voice media, must contain the originator and sender details and where originated by Personnel, but not authorised as per Council policy, must indicate appropriate Council disclaimers. • No messages disclosing sensitive, confidential, restricted, non-public, or proprietary information involving trade secrets will be transmitted electronically unless otherwise secured or encrypted. • Personnel will maintain a clean-desk policy and must ensure that cupboards or offices containing sensitive, confidential, restricted, non-public, or proprietary information are locked when not being used. • All personal computers or notebooks must be switched off when no longer in use or before leaving the office for protracted periods, e.g. leave, over night, business trips, etc. • Personnel must ensure that all CD-Rom disks or Stiffy drive diskettes containing sensitive information must be locked away when not in use. • All information or files on CD-Rom disks or Stiffy drive diskettes imported into the Metropolitan Council's Information Systems must be subjected to virus protection software prior to being made available for general use. • Personnel may not de-activate, switch-off or remove software from their personal computers pertaining to virus protection, license or asset detection purposes.
	Authorised use – Access to Information Systems or resources require specific authorisation with agreed, pre-determined processes and procedures of obtaining approval • Personnel will not share their user-id's with other Personnel for any specific Information Systems access provided to them and are solely responsible for any illegal access by other Personnel. • All electronic mail will be restricted with a 2MGb attachment capacity. • All electronic mail will be scanned and protected with up to date virus tools. • Web sites containing sexual, defamatory, racist or sexist information will be blocked.

INFORMATION USE POLICY	

Detail description (Cont):	• **Prohibited use** - Specific usage rules determine the prohibition of either the engaging, using, sending, creating thereof of Information Systems functions or logic:
	  • Information Systems or resources may not be used for transmitting, retrieving, printing or storage of any communications of a derogatory or inflammatory or sexually harassing remarks about a person's race, colour, sex, age, disability, religion, national origin, physical attributes and sexual preference, discriminatory or harassing nature or materials that are obscene or X- rated.
	  • The use of e-mail / fax / letters / telephones / mobile phones to participate in political activities, to solicit political support or propagate political views, to solicit non-council business or for personal gain is prohibited.
	  • The illegal copying, downloading, storing, distributing, forwarding or printing of either Council or any other copyrighted materials including but not limited to messages, e-mail, fax, letters, text files, program files, image files, database files, sound files and music files or recordings, the cutting or pasting of graphics or other creative work is prohibited.

	▪ All business information material of the Council must not violate, plagiarise or infringe upon the right of any third party, including copyright, trademark or proprietary rights ▪ The act of spamming or spoofing of e-mail, and the automatically forwarding of e-mail to an Internet site is prohibited ▪ The act of designing, writing or executing of malicious code, and the act of hacking or tampering with Information Systems is prohibited. ▪ The act of downloading files, executable code email message and/ or attachments such that they bypass any inherent virus checking software is prohibited.
	Out of office use – Specific usage rules that govern the use of Information Systems outside the work place environment: ▪ Information Systems or resources used via dial-up mechanisms must ensure dial-up user profiles and passwords before allowing access to such systems or resources. ▪ Personnel must ensure that Information Systems or resources used outside the Council's premises are either secured when not in use or not available to non-authorised people. **Personal use** - Usage rules that govern the manner in which Information Systems or resources can be used in a personal capacity: ▪ Policies or processes dealing with the usage of Information Systems or resources for personal use must be enforced. ▪ Requests to derogate from IUP • Personnel can make requests to deviate or derogate from UIP in writing to the incumbent IT Manager who will table such requests with the relevant IT governance committee ▪ Disciplinary process/sanctions • Disciplinary steps, as determined and laid down within the council, can be initiated against Personnel who violate the Policy ▪ General provisions of IUP:

INFORMATION USE POLICY	
Detail description (Cont):	• **Force Majeure** - No one shall be considered to be in default pursuant to this Policy if the fulfilment of all or part of its obligations is delayed or prevented due to "force majeure". "Force majeure" is an external unforeseeable and irresistible event, making it absolutely impossible to fulfil an obligation. • **Severability -**If all or part of any section, paragraph, or provision of this Policy is held invalid or unenforceable, it shall not have any effect whatsoever on any other section, paragraph or provision of this Policy, or on the remainder of the said section, paragraph or provision, unless otherwise expressly provided for in this Policy. • **Headings -** The headings in this Policy have been inserted solely for ease of reference and shall not modify, in any manner whatsoever, the meaning or scope of the provisions hereof. • **No Waiver –** Under no circumstances shall the failure, negligence or tardiness of a person as regards the exercise of a right or a recourse provided for in this Policy be considered to be a waiver of such right or recourse. • **Cumulative Rights -** All rights set forth in this Policy shall be cumulative and not alternative. The waiver of a right shall not be interpreted as the waiver of any other right. • **Amendment or Cancellation of the Policy** - This Policy may be modified or cancelled at any time and without notice, at the Council's discretion.
	▪ All correspondence, in written, electronic or voice media, must contain the originator and sender details and where originated by Personnel, but not authorised as per Council policy, must indicate appropriate Council disclaimers. ▪ No messages disclosing sensitive, confidential, restricted, non-public, or proprietary information involving trade secrets will be transmitted electronically unless otherwise secured or encrypted. ▪ Personnel will maintain a clean-desk policy and must ensure that cupboards or offices containing sensitive, confidential, restricted, non-public, or proprietary information are locked when not being used. ▪ All personal computers or notebooks must be switched off when no longer in use or before leaving the office for protracted periods, e.g. leave, over night, business trips, etc. ▪ Personnel must ensure that all CD-Rom disks or Stiffy drive diskettes containing sensitive information must be locked away when not in use. ▪ All information or files on CD-Rom disks or Stiffy drive diskettes imported into the Metropolitan Council's Information Systems must be subjected to virus protection software prior to being made available for general use. ▪ Personnel may not de-activate, switch-off or remove software from their personal computers pertaining to virus protection, license or asset detection purposes.

INFORMATION USE POLICY	
Detail description (Cont):	• **Authorised use –** Access to Information Systems or resources require specific authorisation with agreed, pre-determined processes and procedures of obtaining approval ▪ Personnel will not share their user-id's with other Personnel for any specific Information Systems access provided to them and are solely responsible for any illegal access by other Personnel. ▪ All electronic mail will be restricted with a 2MGb attachment capacity. ▪ All electronic mail will be scanned and protected with up to date virus tools. ▪ Web sites containing sexual, defamatory, racist or sexist information will be blocked. • **Prohibited use -** Specific usage rules determine the prohibition of either the engaging, using, sending, creating thereof of Information Systems functions or logic: ▪ Information Systems or resources may not be used for transmitting, retrieving, printing or storage of any communications of a derogatory or inflammatory or sexually harassing remarks about a person's race, colour, sex, age, disability, religion, national origin, physical attributes and sexual preference, discriminatory or harassing nature or materials that are obscene or X- rated. The use of e-mail / fax / letters / telephones / mobile phones to participate in political activities, to solicit political support or propagate political views, to solicit non-council business or for personal gain is prohibited. ▪ The illegal copying, downloading, storing, distributing, forwarding or printing of either Council or any other copyrighted materials including but not limited to messages, e-mail, fax, letters, text files, program files, image files, database files, sound files and music files or recordings, the cutting or pasting of graphics or other creative work is prohibited.
	▪ All business information material of the Council must not violate, plagiarise or infringe upon the right of any third party, including copyright, trademark or proprietary rights ▪ The act of spamming or spoofing of e-mail, and the automatically forwarding of e-mail to an Internet site is prohibited ▪ The act of designing, writing or executing of malicious code, and the act of hacking or tampering with Information Systems is prohibited. ▪ The act of downloading files, executable code email message and/ or attachments such that they bypass any inherent virus checking software is prohibited. **Out of office use –** Specific usage rules that govern the use of Information Systems outside the work place environment: ▪ Information Systems or resources used via dial-up mechanisms must ensure dial-up user profiles and passwords before allowing access to such systems or resources. • Personnel must ensure that Information Systems or resources used outside the Council's premises are either secured when not in use or not available to non-authorised people.

INFORMATION USE POLICY	
Detail description (Cont):	• **Personal use** - Usage rules that govern the manner in which Information Systems or resources can be used in a personal capacity: ▪ Policies or processes dealing with the usage of Information Systems or resources for personal use must be enforced. ▪ Requests to derogate from IUP • Personnel can make requests to deviate or derogate from UIP in writing to the incumbent IT Manager who will table such requests with the relevant IT governance committee ▪ Disciplinary process/sanctions • Disciplinary steps, as determined and laid down within the council, can be initiated against Personnel who violate the Policy • General provisions of IUP: • **Force Majeure** - No one shall be considered to be in default pursuant to this Policy if the fulfilment of all or part of its obligations is delayed or prevented due to "force majeure". "Force majeure" is an external unforeseeable and irresistible event, making it absolutely impossible to fulfil an obligation. • **Severability -**If all or part of any section, paragraph, or provision of this Policy is held invalid or unenforceable, it shall not have any effect whatsoever on any other section, paragraph or provision of this Policy, or on the remainder of the said section, paragraph or provision, unless otherwise expressly provided for in this Policy. • **Headings -** The headings in this Policy have been inserted solely for ease of reference and shall not modify, in any manner whatsoever, the meaning or scope of the provisions hereof. • **No Waiver –** Under no circumstances shall the failure, negligence or tardiness of a person as regards the exercise of a right or a recourse provided for in this Policy be considered to be a waiver of such right or recourse. • **Cumulative Rights -** All rights set forth in this Policy shall be cumulative and not alternative. The waiver of a right shall not be interpreted as the waiver of any other right. ▪ **Amendment or Cancellation of the Policy -** This Policy may be modified or cancelled at any time and without notice, at the Council's discretion.
	• **Number and Gender -** Where appropriate, a singular number set forth in this Policy shall be interpreted as a plural number, and the gender shall be interpreted as masculine, feminine or neuter, as the context dictates. • **Other Applicable Policies -** This Policy is in addition to all other company policies, and to all guidelines, standards and methods issued by the Council. It is not in any way intended to replace or supersede one or more such policies, guidelines, standards and methods, unless otherwise specified in this Policy.
Applicable forms:	To be designed
Input documents:	To be designed
Reports ("D,E,F:):	
Approval:	
Other matters 1:	
Other matters 2:	
Attachments:	

INFORMATION USE POLICY	
Definitions:	**Attachment –** A file attached to an e-mail message. Many e-mail systems only support sending text files as e-mail. If the attachment is a binary file or formatted text file (such as an MS-Word document), it must be encoded before it is sent and decoded once it is received. There are a number of encoding schemes, the two most prevalent being Uuencode and MIME.
	Browser – Short for Web browser, a software application used to locate and display Web pages. The two most popular browsers are Netscape Navigator and Microsoft Internet Explorer. Both of these are graphical browsers, which means that they can display graphics as well as text. In addition, most modern browsers can present multimedia information, including sound and video, though they require plug-ins for some formats.
	Copyright – the legal right to control every way of producing a version of an original piece of work, such as a book, play, film, photograph or piece of music.
	Data Integrity - Refers to the validity of data. Data integrity can be compromised in a number of ways: Human errors when data is entered • Errors that occur when data is transmitted from one computer to another • Software bugs or viruses • Hardware malfunctions, such as disk crashes • Natural disasters, such as fires and floods There are many ways to minimize these treats to data integrity: These include : • Backing up data regularly • Controlling access to data via security mechanisms • Designing user interfaces that prevent the input of invalid data • Using error detection and correction software when transmitting data.
	Information Systems – are deemed to be any and all systems, tools, devices, data, information, or practices provided by the Council to Personnel in their execution of their duties as indicated but not limited to telephones, mobile phones, facsimile machines, Internet, e-Mail, Application systems, policies, procedures, standards and practices, etc. **Intellectual property –** is an original idea which can be used to earn money. The person or group who is recognized as having the idea can use the law to prevent other people from earning money by copying it. **e-Mail -** Short for electronic mail, the transmission of messages over communications networks. The messages can be notes entered from the keyboard or electronic files stored on disk. Encryption - **Encryption is the transformation of data into a form unreadable by anyone without a secret decryption key. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended.** **Network -** A group of two or more computer systems linked together. There are many types of computer networks, including: • local-area networks (LANs) : The computers are geographically close together (that is, in the same building). • wide-area networks (WANs) : The computers are farther apart and are connected by telephone lines or radio waves.

INFORMATION USE POLICY	
Definitions (Cont 1):	**Ownership –** for the purpose of this policy, the Information System or any part thereof that is made available to Personnel shall be deemed to be the exclusive property of the Ekurhuleni Metropolitan Council. Consequently Personnel shall not have any right (real or assumed) of ownership, confidentiality or privacy while using the Information System. Further, the Council shall be deemed to be the exclusive owner of all information, messages, data and files in the Information System or emanating there from, in any form whatsoever (electronic, digital, printed, audio, video, or other), whether or not such information, messages, data and files have been created, received or stored with the help of such system. Consequently, Personnel shall not have any right (real or presumed) of property, confidentiality or privacy as regards such information, messages, data and files. Personnel – **are deemed to be any and all officers, employees (full-time and part-time) consultants, agents, contractors, sub-contractors, independent contractors or other representatives of the Council, and any end-users given discretionary access to the Information Systems provided by the Council** **Security –** Techniques, processes, policies, tools, or software for ensuring that data stored in a computer cannot be read or compromised. Most security measures involve systems access, data encryption and passwords. Systems access involves user and function access hierarchies or templates requiring users to be set-up against specific systems and/or functions. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system. **Spamming -** An inappropriate attempt to use a mailing list or other networked communications facility as if it was a broadcast medium by sending the same message to a large number of people who did not ask for it. **Spoofing -** A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted port. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted port and then modify the packet headers so that it appears that the packets are coming from that port. **Trade Secret** - For purposes of this Agreement, "Proprietary Information" and "Trade Secrets" is any information, including, but not limited to: • The operation of Ekurhuleni Metropolitan Council, consisting, for example, and not intending to be inclusive, of its lists or other identifications of clients or prospective clients of Council (and key individuals employed or engaged by such clients or prospective clients), the nature and type of services rendered to such clients (or proposed to be rendered to prospective clients), fee charged or to be charged, proposals, inventions, methodologies, algorithms, formulae, processes, compilations of information, form and content of data bases, designs, drawings, models, equipment, results of research proposals, technical or non technical data, patterns, programs, devices, techniques, product plans, job notes, reports, records, specifications, software, firmware and procedures used in, or related to, the Council relations with its employees including without limitation, salaries, job classifications and skill levels;

INFORMATION USE POLICY	
Definitions (Cont 2):	• Financial, sales and marketing data compiled by the Council as well as Council`s financial, sales and marketing plans and strategies, lists of actual or potential customers or suppliers and non-public pricing that derive economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from their disclosure or use; • All ideas, concepts, information and written material about a client disclosed to an employee by Council or acquired from a client of the Council, and all financial, accounting, statistical, personnel and business data and plans of clients, are and shall remain the sole and exclusive property and proprietary information of the Council or said client;

IT ARCHITECTURE POLICY

Policy name:	IT Architecture policy
Reference number:	
Date of last update:	17/05/2001
Circulation to:	
Brief description:	Addressing the open standards architecture that must be conformed to for Information Technology in Ekurhuleni.
Scope:	Applicable to the procurement of all Hardware, Software, Middleware and Applications in the Metropolitan Council.
Objective:	To ensure that whatever Hardware, Software or Applications is acquired for the Council, conforms to open standards and that no part of the IT environment is locked into proprietary systems.

IT ARCHITECTURE POLICY	
Detail description:	Standards are based on the 7 layers **OSI** Reference Model. # Application protocols. **ODBC** for accessing databases. **SMTP** to deliver messages between e-mail applications. **EDI** to facilitate flow of transaction tasks between businesses. # Presentation protocols. **ASN.1** for transmitting numerical data. **TIFF** the graphics format for high-resolution bitmapped images. **JPEG** for photographic images **MPEG** for the compression of video and CD's. # Session protocols. **NFS** used with TCP/IP and Unix w/stations to allow transparent access to remote resources. **SQL** to provide users with a simpler way to define their information requirements. **RPC** as a broad client/server redirection tool for disparate service environments. **X-WINDOW** is used by intelligent terminals for communicating with remote Unix computers. # Transport protocols. **TCP/IP** # Network protocols. **TCP/IP** # Data Link protocols. **802.11b** for wireless lans at 11 Mbps **802.3** for standard lans **LAPB** for Frame control when X.25 is used **SLIP** for low speed interfacing with Unix **PPP** as SLIP but with added logins, passwords and error correction **ISDN** for transmitting voice and data **100BaseFX** for Ethernet over fibre at 100Mbps **100Base4 using 802.3** specs for 100Mbps over cat 3,4,5 cable **100BaseTX** for fast Ethernet over cat 5 cabling # Physical protocols. **EIA/TAI-232** **EIA/TAI- 449** **V.24** **V.25** **X.21** **G.703** **EIA-530** **HSSI** (high speed serial interface)

IT ARCHITECTURE POLICY CONT.

Applicable forms:	To be stated in all tenders/quotations being put forward.
C Input documents:	None
Reports (“D,E,F:):	None
Approval:	
Other matters 1:	
Other matters 2:	
Attachments:	None

USER ACCESS POLICY

Policy name:	User access policy – password protection procedure
Reference number:	
Responsible person:	
Date of last update:	29/05/2001
Circulation to:	All IT and user personnel
Brief description:	Password related matters – setting and changing, size and construction rules, display, violation reporting.
Scope:	Applicable to every terminal/PC having access to networks and servers.
Objective:	To ensure that security and confidentiality is maintained and that authorized personnel (both internal and external) are denied access to applications and data.

USER ACCESS POLICY	
Detail description:	▪ Set-up of rights. HR will complete section 1 of form USER ACCESS on commencement of employee and forward it to the relevant department head/superior for confirmation of access rights and for authorization. Department head will forward form USER ACCESS to system/network administrator who will set up the appropriate rights. ▪ Change of rights. Department head/superior will complete section 2 of form USER ACCESS, will authorize and will forward to system/network administrator who will amend access rights. ▪ Withdrawal of rights. Department head/superior will complete section 3 of form USER ACCESS, will authorize and will forward to system/network administrator who will withdraw access rights. ▪ Password length and construction. Passwords comprise a mixture of six alphanumeric characters. The chosen sequence should have no meaning. (Avoid date of birth; dogs name etc) ▪ Password expiry. Passwords expire ever 30 days and must be changed by the user. The system requires that a different password be used each time. Five days warning is given to allow for user to change password. ▪ Number of attempts. Three attempts at the password are allowed before the user is locked out of the system ▪ Display. Keyed in passwords will not be displayed on the screen. ▪ User log-off. User must log out of system when they leave their workstation for any reason. ▪ Inactive terminals. After a terminal/pc has been inactive for a predetermined period (15 minutes) the user will be automatically logged out of the system or the screen saver with password will be activated. ▪ The “superuser” password. The “superuser” password will be known to the system administrator. The password will be recorded in the password book, which will be locked in the fireproof safe of the treasurer. ▪ System consoles. All system consoles on Unix, Windows NT and Novell must be at all times secured with password authentication. ▪ Network resources. Where possible, all network resources eg. Print servers, routers, switches and storage area networks, should be accessed by password authentication. Configuring network devices. Where possible, all network devices that can be configured must be password protected in compliance with set policy.
Applicable forms:	Form user access is used for: ▪ Taking users on to the system. ▪ Determining of the user profile – applications to which access is allowed, type of access (view, update), and time of access. ▪ Deleting users from the system. ▪ Changing user access profiles.
Input documents:	Form USER ACCESS. To be filed in numerical order by the system administrator.

USER ACCESS POLICY	
Reports ("D,F,F"):	Two reports are available from the system: ▪ Audit log of password amendments. Report of passwords added to, deleted from and changed on the system. (**D**istributed to the system administrator. **F**requency is monthly. **F**iling is in date sequence.) ▪ Register of password input failures. (**D**istributed to the system administrator. **F**requency is monthly. **F**iling is in reverse date sequence.)
Approval:	Form USER ACCESS will be approved by the department manager/superior of the employee. The two reports will be scrutinized by the system administrator for reasonableness on a monthly basis. Internal audit will periodically check that entries on the report "audit log of password amendments" are supported by correctly authorized copies of form USER ACCESS.
Other matters 1:	
Other matters 2:	
Attachments:	Form USER ACCESS; Audit log of password amendments; register of password input failures.

IT DEVELOPMENT POLICY

Subject	INFORMATION TECHNOLOGY METHODOLOGY FOR SYSTEM DESIGN
Procedure number	
Policy number	
Accompanying policy	None
Enquiries	André Hofer
Department	Finance
Division	IT&S
Telephone	921 2175
Reference number	
Annexures	None
Purpose	To describe the basic methodology of designing systems
Introduction	
Scope	All IT&S issues pertaining to the Kempton Park Tembisa Administrative Unit

IT DEVELOPMENT POLICY	
Detail description:	DEVELOPMENT METHODOLOGY **1. BASIC METHODOLOGY – SYSTEM DESIGN** This procedure must be applied to all information technology projects initiated in the Council. The purpose of all new information technology projects must first be established and should adhere the methodology as set out below. 1.1 SYSTEM DESIGN REQUESTS Proposals are received from management or users. These requests must be evaluated for validity and relevance within the context of the proposed project. At a high level, the analysis stage confirms the vision for the application, and establishes the details and boundaries for its construction. This is typically accomplished by the preparation of the requirements definition document and three subsequent design documents: a.1. Systems design document. a.2. User interface design. a.3. object design. 1.2 FEASIBILITY STUDY A feasibility study must be conducted. This study will entail a high level analysis of the current business area, to determine whether a system can cost effectively support the new requirements. The study must reflect estimates on cost, manpower resources required, hardware or software required, as well as time frame estimates of the various stages of the proposed project. A full report of the feasibility study must be provided back to the project initiator / sponsor for final approval. 1.3 DESIGN AND PROTOTYPING Where appropriate a prototype should be designed based on the requirement of the project initiator or sponsor for approval. The prototype should be able to demonstrate the salient features required by the project initiator in such a way to obtain approval to take the project to its proper analysis and design state.

IT DEVELOPMENT POLICY	
Detail description:	1.4 PROJECT PLAN A relevant and commensurate project plan, as related to the scope of the project, incorporating details from the feasibility study and the prototyping, must be created. The project should be divided in logical phases with relevant checkpoints at the end of each phase. The project plan should address the different resource requirements, constraints, costs and time flow. Where appropriate milestones and checkpoints must be included for reference and feedback purposes. Each checkpoint should be associated with a further approval from the project initiator or sponsor. 1.5 SYSTEMS ANALYSIS SPECIFICATION The following aspects should be incorporated in the System Design and project plan. First identify current business processes that are carried out and the data structures involved, and then identify system requirements for the new proposal. After this step requirement specification must be detailed, functional and non-functional requirements identified and any new techniques introduced if necessary, for required processing and data structures. Technical system options must be identified for development and implementation environments. (hardware and software platforms). The logical design of update and enquiry processing and system dialogues (menus) must be carried out. Finally the project plan must be updated stating proposed actions and methods to be used to incorporate new requirements, with time frames and costs involved. 1.6 EVALUATION OF SYSTEMS SPECIFICATIONS The project leader must together with the user community evaluate the specification. The various assumptions must be evaluated for relevance, accuracy and impact. Preferably, a business dry run of the proposed system specification should be undertaken to ensure validity and correctness in the work environment. The project sponsor must authorise the next phase of the project. 1.7 DETAILED SYSTEMS DESIGN The system design phase translates the logical and technical specifications into program specifications, database design criteria and anticipated test criteria. The test data created should cater for program, component and system testing.

IT DEVELOPMENT POLICY	
Detail description:	1.8 PROGRAM CODING The necessary program coding must now be done. 1.9 SYSTEM TESTING The system testing comprises several types of testing. Firstly, individual programs or design creations are tested individually for correctness and stability. Once these tests have been completed components of systems and or whole systems can be tested to ensure overall system coherency. Each testing phase should be managed separately before proceeding to the next test. It is recommended that the user community is involved in the creation of test data as well as the testing of the different scenarios. Each possible business scenario should be tested for data storage, updating and output correctness. Reports or online queries to indicate program and logic correctness should be written provided and used during the testing phases. 1.10 SYSTEM IMPLEMENTATION System implementation must only take place after the user community are happy with all system testing as per the system specifications. The project sponsor must sign off the development and testing phases before implementation is started. The following aspects must be considered prior to implementing the changes: • The synchronisation of the new programs or systems with existing systems • The timing of the implementation of the new programs or systems in relation to existing systems • The training of users prior to the implementation • The updating of system and user documentation. 1.11 SYSTEM SIGN OFF Upon final implementation the new programs or system must be bedded down to ensure no problems. Once a sufficient period has been allowed the entire project should be reviewed and signed off by the originating user.
Applicable forms:	System dependant
Input documents:	
Reports (“D,E,F:):	System dependant
Approval:	The approval of the Policy is the responsibility of the Mayoral Committee or its delegated assignee.
Other matters 1:	
Other matters 2:	
Attachments:	

IT TENDER AND EVALUATION POLICY

Policy name:	IT Tender & Procurement Policy
Reference number:	
Date of last update:	May 2001
Circulation to:	All It Management / Assets Management
Brief description:	To lay down minimum conditions / standards concerning the procurement
Scope:	
Objective:	

IT TENDER AND EVALUATION POLICY	
Detail description: **Section 1** **General Conditions / Requirements:**	1. Tenderers must ascertain the Metropolitan's current and future requirements and submit tenders accordingly. 2. The lowest or any tender will not necessarily be accepted. Any tender submitted which does not comply with the conditions stated in these documents may be rejected. 3. Preference will be given to tenderers with XYZ Gold and Silver partnership status. 4. The proposed solutions must be able to be managed by XYZ Software. 5. If any solutions are proposed without the use of cable, the tenderer must produce a certificate from the local distributor accrediting the solution. 6. The awarding of the respective projects may possibly be awarded to different tenderers, however, preference will be given to the tenderer with a total solution. 7. The Metropolitan reserves the right to change the quantities of materials and equipment included in this document, within a period of three months from the date of placing an order for the contract works. 8. The proposed hardware and software must be made available, at the supplier's cost, to run a benchmark to be determined by the Metro. 9. The proposed hardware must have seamless connectivity to the Metropolitan's existing Novell and Unix and Microsoft networks. Seamless connectivity implies the ability to address any installed computer platform or printer from any workstation on the networks. The hardware supplier must prove such connectivity. 10. Only original OEM manufactured or supplied hardware and software shall be used. No alternatives shall be used. 11. The tenderers company name and date of installation must be placed on the bottom of all hardware. 12. The successful tenderer must guarantee that the hardware and software are sized correctly based on the tender specifications, failing which, the undersized hardware and software will be upgraded to the required specifications at the tenderer's expense. 13. The successful tenderer must guarantee that the proposed hardware and software are year 2000 complaint. 14. The successful tenderer must accept responsibility for the installation of all the necessary communications for the proposed equipment (electrical, data etc.). 15. Lightning protection, as necessary, must be included in the solutions. 16. All existing hardware and software which are not used in the proposed upgrades remain the property of the Metro.

IT TENDER AND EVALUATION POLICY	
Detail description:	17. Tenderers must supply on site maintenance (site of installation) for the proposed hardware and software. In addition, on site maintenance must be provided for all existing connectivity hardware on the LAN that is upgraded, relocated and/or left in service. Copies of the Maintenance Contracts must be submitted with your response. 18. The Metropolitan will not be responsible for the accepting, handling and storing of materials and equipment. 19. Training must be given by the successful tenderer to (Amount) Metropolitan employees covering the proposed hardware and software. (Details of the proposed courses to be submitted with the tender). 20. Tenderers must hold good for 120 days from the closing date stated herein, or extension thereof, during which, tender prices will remain firm, save only such price variations as are subject to statutory price variations. 21. Tenderers must submit schedules for the proposed hardware and software indicating: (all costs are to be stated in South African currency and all prices must include VAT) a) hardware b) hardware costs c) duties, exchange rates and taxes payable d) delivery, installation and commissioning costs e) cabling costs f) warranty periods g) as equipment has warranty periods, indicate from when maintenance is payable h) maintenance costs i) software j) software costs k) training costs l) professional support etc costs m) travelling costs n) installation and commissioning dates for both hardware and software

IT TENDER AND EVALUATION POLICY	
Detail description:	22. It is acknowledged that all responding tenderers submit full and complete costs for this tender. Should there be any omissions on behalf of the tenderer, these omissions will be for the tenderers account. 23. Tenderers must state the number of working days after the date of order so that they would be able to guarantee completion of the various undertakings. 24. Tenderers shall guarantee the tender completion date and shall accept responsibility for the penalties as specified below: 24.1 Penalties shall be paid by the Contractor to the Employer, or the amount shall be withheld by the Employer from the Contractor, as penalties for defaults on the part of the Contractor to complete the contract in the agreed time. 24.2 The penalty shall be ½(half percent) per week or part of a week, calculated on the total value of the contract works, to a maximum of 15% (fifteen percent) of the value of the contract works. 25. Payment will only be made after completion of tender. No part payments will be considered.

IT TENDER AND EVALUATION POLICY	
Detail description: **Section 2** **Hardware:**	1. What is your company involvement in defining and implementing Open Systems? 2. State the country of origin/manufacture of the proposed hardware. 3. What is the growth potential of the proposed hardware assuming that the operating, drivers and utility software are not changed? 4. What assurance can you give that the proposed hardware will be fully compatible with any future announced hardware so as to protect the Metropolitan's intended investment as per this tender? 5. Can connectivity hardware upgrades be done on site and what is the down time to affect these upgrades? 6. Explain in full detail the upgradeability of the proposed hardware. 7. Explain in full detail how the proposed system can be run on a decentralised basis. (eg. power failure, communication failure etc.) 8. Explain in full detail what securities are built-in to ensure privacy and security of data. 9. For how many years is the supplier prepared to guarantee spares and maintenance for the proposed hardware? 10. Can the proposed hardware be run 24 hours per day, 7 days a week without additional costs? 11. Which units of the proposed hardware require air-conditioning? 12. Specify environmental requirements for all hardware. 13. What is the guaranteed response time on callout? Give details. 14. In the event of a hardware failure, what is the guaranteed maximum downtime? Give details. 15. Does your hardware support remote diagnostic facilities? If yes, give details. 16. Can your proposed hardware communicate with other manufacturer's hardware? Give details. 17. Indicate how often, when and at what rate maintenance and other charges are reviewed. 18. Can the maintenance increase be contracted to a fixed or maximum amount/percentage? If yes, give details. 19. If you are an agent for the proposed hardware, give details of how you intend supplying the after sales service.

IT TENDER AND EVALUATION POLICY

Detail description: **Section 3** **SOFTWARE :** **OPERATING, DRIVERS AND UTILITIES**	1. Supply full details of the proposed operating, drivers and utility software 2. What is your Company involvement in defining and implementing Open Systems? 3. Do you comply with the C2 Security Rating as set by the U.S. Department of Defence? Explain in full detail. 4. Indicate how often, when and at what rate software and other charges are reviewed? 5. Can the software increases be contracted to a fixed or maximum amount/percentage? If yes, give details.
Detail description: **Section 4** **Requirements:**	Refer Annexure A for a diagram of the existing network. The following preferences should be kept in mind: 1. The XYZ ranges of products are preferred. 2. The protection of current investment must be kept in mind. 3. Both current and future Ethernet standards must be maintained. 4. Continue with tender required specifics……..
Detail description: **Section 5** **Training:**	Supply a detailed schedule of courses for both the hardware and software relevant to this proposal including duration and costs i.e.: a) Course name b) Course synopsis c) Duration d) Cost per delegate e) Venue f) Who presents the course g) Who should attend the course

IT TENDER AND EVALUATION POLICY	
Detail description: **Section 6** **Support & Reference Manuals**	1. Supply a structure list and numbers of support personnel who are proficient in the support and maintenance of the proposed systems. 2. Specify the number of Ekurhuleni employees and the level of their expertise, that will be required to manage the technical operation of the system. 3. Manuals: 4. Two sets of manuals relating to the proposed hardware and its software are to be supplied by the successful tenderer. Modifications or enhancements to the manuals or completely revised manuals shall be provided on a continuing basis for the duration of the contract.
Detail description: **Section 7** **License & Maintenance Agreements**	1. Specify all conditions in terms of licence and maintenance agreements. 2. Specify conditions re upgrades and additional developments of the proposed hardware and software. 3. Supply a sample of the relevant contracts.

IT STANDARDS POLICY

Policy name:	Standards Policy: High Level
Reference number:	
Responsible person:	H.J. Vorster
Date of last update:	08/05/2001
Circulation to:	All IT personnel and Admin Units
Brief description:	Software, hardware, network
Scope:	Applicable to all IT related matters
Objective:	To increase efficiency. Develop standards to reduce costs for hardware, software, peripherals, training and other factors and make for better sharing of information.

IT STANDARDS POLICY	
Detail description:	**Software:** Where available, network versions of standard software should be considered for purchase. With the Internet evolving as the preferred method of information and data exchange. Worldwide, the broadest "standards" are SGML (Standards General Mark-up Language) and the more popular HTML (Hypertext Mark-up Language). All products chosen should be evaluated for their capabilities of writing HTML formatted files. Word Processing - Microsoft Word is the defacto standard and all users should convert to Microsoft Word as soon as possible. A further goal should be to upgrade computer systems to be able to run Word 2000 or greater as soon as is practical. Non-standard word processing packages will be phased out as soon as possible. Spreadsheets - Microsoft Excel is the defacto standard and all users should convert to Microsoft Excel as soon as possible. A further goal should be to upgrade computer systems to be able to run Word 2000 or greater as soon as is practical. Non-standard word processing packages will be phased out as soon as possible. Database Management Systems - Three RDMS systems namely, Oracle, SQL and Adabas C. Programs using ODBC formats are acceptable alternatives especially when dealing with GIS data. A goal is for all systems to upgrade to current versions capable of accessing above-mentioned databases and meeting ODBC requirements. Operating Systems - 1) MS Windows 3.1x, 95, 98 are the defacto standards on Personal Computers. 2) Windows NT, Novell and Unix are the defacto standards on servers. E-Mail - By using Simple Mail Transport Protocol (SMTP) as a common language Microsoft Exchange is the defacto standard. All other E-Mail packages must be phased out. CAD - No standards are recommended at this stage. GIS - No standards are recommended at this stage. Project Management - MS-Project is the defacto standard and all users should convert to MS-Project as soon as possible. Terminal Emulation - No standards are set at this stage. An investigation will be done to select a package for the long term. Anti-Virus - The anti-virus package must be able to resolve the following platforms or solutions: - Desktops - Servers - WEB - E-Mail

IT STANDARDS POLICY CONT.

Detail description:	Trend and Mcafee are the current defacto standards and an investigation will be done for a long-term selection. Access Content Analysis – Internet misuse leads to productivity declines, legal liability and excessive demands on band-with and network resources. To control Internet usage, Websense as a server-based software solution is the defacto standard. Websense allows you to transparently monitor, report and manage traffic from the internal networks to the Internet. Firewall - Firewalls create barriers in order to prevent unauthorised access to the network. Firewalls are the security doors through which some people (i.e data) may pass and others may not. MS-ISA is the defacto standard and all service delivery areas should convert to MS-ISA as soon as possible. Fax Software - No standards recommended at this stage. **Hardware:** All systems will meet EPA Energy Star standards where available. Personal Computers - It should be the goal of Ekurhuleni to purchase or upgrade to systems that can run the recommended standard software listed above. Some programs listed above need the top-of-the-line computer Hardware (Tier 1) because of speed, data capacity and graphics handling capabilities. The standard for personal computers is as follows: Tier 1 - Compaq, HP, Dell, IBM Tier 2 - Mecer, Acer, Mustek The minimum specifications for the above are: Intel Motherboard, Intel Processor (entry level), Seagate Hard-drive (entry level), 128mb SDRAM 133 (minimum) TEAC Stiffy-drive, Network Interface Card, (3COM 10/100 mb autocensing), 14" Monitor, PS^2 Keyboard and mouse. Terminals - Terminals should be used where users only need to access the financial systems. Terminals must have the capability to emulate the VT100 emulations. Graphic terminals should meet the X-Windows standards. Notebooks - Should be capable of running the standard software listed above. The standard for notebooks are as follows: Tier 1 - Compaq, HP, Dell Tier 2 - Mecer, Acer, Mustek The minimum specifications for the above are: Intel motherboard - PIII Intel Processor (entry level). 128MB SDRAM. Seagate harddrive (entry level). 12.1" Active screen. 10/100MB. 3COM PCMCIA Network Card. Stiffy and CD Rom. Palmtops - The defacto standard for Palmtops is 3COM.

IT STANDARDS POLICY CONT.

Detail description:	Printers - When sharing documents, incompatibility among printers can cause frustrating formatting problems. Printers should be demonstrated to be well supported by the applications to be used. Performance and compatibility with applications should be the prime considerations in their selections. Printers must be as far as possible directly connected to the network rather than to a computer. The defacto standard for printers are as follows: Laser Printers: Hewlett Packard Dot Matrix: Seikosha, Epson Line Printers: Mannesman Tally, Printtronix Deskjets: Hewlett Packard, Canon Plotters(pen,raster) - Plotters should be selected for performance and compatibility with applications. Plotters should be as far as possible, directly connected to the network. The defacto standard for plotters is Hewlett Packard. Scanners - Scanners should be selected for performance and compatibility with applications. The standard for scanners are as follows: Hewlett Packard and Fujitsu Modems - The defacto standard on dial-up modems are US-Robotic and leased modems Penil and Nokia. UPS - A full investigation is required to select a certain product. The UPS at this stage must be a full-synchronized unit. Servers - Servers should be selected for high performance in work groups (departmental and enterprises), maximum uptime and compatible with operating systems (Novell,NT) and databases (Oracle,SQL). In selecting server Tier 1 servers must be chosen to handle mission critical workloads and Tier 2 servers to handle non-mission critical workloads. <u>Tier 1 Servers (Novell, NT)</u> Dell Compaq Hewlett Packard IBM <u>Tier 2 Servers (Novell, NT)</u> Mecer Acer Fugitech Mustek Intel SC5000 Intel motherboard dual capacity (minimum entry level Intel Processor) 1Gig RAM expandable to 2Gig (minimum) Raid 5 Entry level harddrives - 10Gig Ultra 160 HDD (minimum) CD Rom, stiffy and Intel I9660 network card with onboard risk processor <u>Unix Servers (Sun)</u> The specifications of Sun servers will depend on how many users will access these servers.

Detail description:	**Networks:** This part of the standards document explores the needs for networking, e-mail file transfer and remote log-on. We consider Local Area Network (LAN) as being one ore mor servers connected by cabling to several personal workstations and specially configured to work together. A Wide Area Network (WAN) will be defined as being the inter networking of LAN's as well as their connections to regional officers and remote users. The standards for LAN/WAN are as follows: Network Cards - 3COM (auto-censing) Cabling - UTP Cat 5 (minimum) HUBS - 3COM (auto-censing) Switches - 3COM and Cisco Printers - Intel print servers and Jet Direct network card File transfer protocol - Open at present Remote access - MS-RAS Network protocol - IP Protocols - TCP/IP is the only protocol that is capable of communication across the Internet and the only one that is supported by all computers. TCP/IP is the defacto standard for network communications.
Applicable forms:	
Input documents:	
Reports ("D,E,F:):	
Approval:	
Other matters 1:	
Other matters 2:	
Attachments:	

IT BACKUP AND DISASTER RECOVERY POLICY

Policy name:	Disaster Recovery Policy For Ekurhuleni Metro
Reference number:	
Date of last update:	23/05/2001
Circulation to:	All IT Managers and Operations Managers
Brief description:	Backup and disaster recovery matters, such as frequency of backups to be taken Storage and control of backup media, testing of recovery procedures. Areas that need such procedures
Scope:	Applicable to all IT sites that have file servers which are critical to Metropolitan activities
Objective:	To ensure that all critical data is securely backed up on a regular basis and stored In a safe environment so that it can be successfully restored, as and when required.

IT BACKUP AND DISASTER RECOVERY POLICY

Detail description:	• **Areas that require backup** All file servers are to be backed up • **Frequency** Daily • **Storage of backup** All backup media is to be stored off-site in a fire proof safe. The latest Version should be transferred to the off-site facility on a daily basis. Backup that is kept on site (older copies) must also be kept in a fire proof safe. All movements are to be recorded in a register and signed for. • **Backup Register** A register must be kept, to record the following: Date on which backup was made Time that backup was made What was backed up (eg. Full data base, system, PayDay etc.) The tape number on which the backup was made. Name of operator. Tape location(on site/off-site) • **Number of Backup sets** At least three full sets of backups should be kept. Month end and year end backups should be kept for longer periods as per individual requirement. • **Backup of critical data on desktops** Space should be made available on one of the servers for individuals to save critical information such as big spreadsheets etc.(these servers are to be backed up daily.) • **Uninterruptible Power Supply Units(UPS'S)** All file servers are to be linked to UPS'S which will allow at least enough time to do proper shutdowns of the systems. • **Testing of restore procedures** Restore procedures should be tested on a regular basis to assure that backed up information can be restored from the backup media. This should be done once every three months and the results should be recorded in a register. • **Disaster Recovery Plan** A formal disaster recovery plan must be put in place, and should include the network infrastructure as well as all other relevant computer systems.

IT HELPDESK POLICY

Policy name:	HELPDESK POLICY
Reference number:	
Date of last update:	28/05/2001
Circulation to:	All users of IT equipment and systems
Brief description:	Policy deals with the setup of a helpdesk to log, manage and resolve It hardware and software problems including the supply of information on assets, software licenses, warrantees and movement of IT equipment.
Scope:	Applicable to every user of IT equipment that experience a problem with the equipment or software in use.
Objective:	To provide a fast, reliable service to IT users to solve problems experienced by them as to achieve business and operational benefits such as: • Accessibility through a single point of contact for communication and • Information. • Improved usages of IT support resources. • Increased productivity of business personnel. • Improved customer service and satisfaction. • Better-managed infrastructure. • More meaningful management information for decision support.

IT HELPDESK POLICY	
Detail description:	1. GENERAL All references to the HelpDesk will mean the IT HelpDesk. HelpDesk will be setup to address the Metropolitan Head Office and the three Services region. It is anticipated that in the longo form the SDR Helpdesk be connected together and replicated to provide redundancy and consolidated information on all problems All incidents, problems or requests pertaining to any IT related product, item or system must be logged at the HelpDesk. NO IT personnel are allowed to attend to any problem or incident without it being logged BEFORE being attended to. The HelpDesk Procedures Manual will contain all the day to day functions and procedures to be followed and must be seen as an extension of this Policy. The extent of the contents of this manual is described later in this Policy document. 2. INCIDENT MANAGEMENT An incident is a single occurrence of an issue, which affects the delivery, or normal or expected level or service. Incident Management provides the interface between the users of those services and those operating the services when an incident arises. Incident management would constitute: - Receiving incidents from users - Logging of those incidents for later reference and ensuring that it do not get lost when passed around support teams - Informing users of known workarounds - Ensuring that support personnel are working on the incident - Keeping users informed on the resolution progress - Informing users when incidents have been resolved and ensuring that Resolution is complete and to the satisfaction of the user - Ensuring that all outstanding incidents are resolved in a timely Manner. The method of achieving all the above mentioned goals is described in the Helpdesk Operations Manual. Incident management also means that all business and product knowledge together with known problem checklists and other diagnostic aids will be used to solve the incidents prior to passing them on to support teams.

IT HELPDESK POLICY

Detail description:

3. PROBLEM MANAGEMENT

A problem is the underlying cause of one or more incidents. The policy of Problem Management is to utilize the skills of experts and Support groups to fix and prevent recurring incidents by determining and Fixing the underlying problem/problems causing the incidents. Problem Management would constitute:

- tracking and logging of problems
- correlate related incidents to identify problems
- solve problems by logging change requests or determining workarounds
- supply solutions to all user communities and appropriate support personnel.

4. REQUEST MANAGEMENT

Request Management can be defined as the process whereby requests from users, vendors or developers are controlled by accepting, logging and channeling of the requests. The function of Request Management forms part of the HelpDesk Policy.

The procedures to fulfill the Request Management function are defined in the HelpDesk Procedures Manual.

5. IT HELPDESK CONTACT

The helpdesk will be setup such that users can contact the Helpdesk via telephone, facsimile and e-mail.

The contact details will be determined shortly.

6. SUPPLIER HELPDESK CONTACT

As no IT user should contact any supplier, vendor or software company directly the telephone numbers to contact all the above mentioned entities are listed in the HelpDesk Procedures Manual available at the HelpDesk centre.

7. SERVICE LEVEL DEFINITION

The following HelpDesk functions must be measured to determine the level of service. Targets set to compare the service levels are also stipulated (where applicable), where:
(I = Incident R = Request P = Problem)

- Effectiveness of resolutions of I/P's:

Priority	Type of call	Measurement	Target
1	Production down	Time in hours	2 hours
2	Serious problem	"	4 hours
3	Normal user fault	Time in days	2 days
4	Upgrade/Request	"	5 days
5	Change control	"	5 days
6	Question/Quote	"	5 days

IT HELPDESK POLICY	
Detail description:	• Percentage of I P's wrongly assigned 1 % - Call responsiveness: - speed of response to a call 5 rings - percentage of calls lost (due to not getting answer before user gave up) 2 % - average call time 5 min. - User satisfaction (by survey): 98 % • Effectiveness of Service level: - I,P,R's closed - no comeback 9 8 % - I,P,R's re-opened (nor properly solved) 1 % - Number of I,P's associated with top 5 I P's 5 % • Correctness of Asset/License Info: - assets incorrectly coded 1 % - (established during verification audit or logging of I, P calls) - illegal software licenses discovered 0 % • Repair cycle time: - time taken to repair equipment - to be determined at each Regional office - to be determined at each Regional office 8. CALL ESCALATION Calls that are not closed within the specified Service Level Targets will be escalated as follows: Priority Escalation Response 1 Mail notification to IT Manager. Mail notification to support team head. Repeated every 1-hour until call is closed. 2 Mail notification to support team head. Mail notification to IT Manager and support team head after another 2 hours and call escalated to a priority 1 call. 3 Mail notification to support team head. Mail notification to IT Manager after another 4 hours. Repeat mail notification to IT Manager and support Team head every 4 hours until call is closed. 4 Mail notification to support team head. Mail notification to IT Manager and support team Head after another 1 day. Repeat mail notification to IT Manager and support Team head every day until call is closed. 5 Same as priority 4. 6 No escalation will be used.

IT HELPDESK POLICY	
Detail description:	9. CALL STATUS The status of a call will indicate what is happening with that call at that particular moment. The status of a call will change as it moves along the path of being resolved. CALL STATUS — OPERATION PERFORMED OPEN — Received at call centre ACTIVE — Opened by support group for investigation and being resolved PENDING — Call cannot be resolved due to: • Repair • Awaiting spares • Awaiting quote • Pending an install • Pending an upgrade etc. COMPLETE — Call resolved. HelpDesk will phone user to confirm satisfaction with resolution of call. CLOSED — Call resolved satisfactory. 10. PROCEDURES MANUAL The Procedures Manual defines the day-to-day operation details and procedures to be followed by the HelpDesk personnel. The Procedures Manual must include all the following headings and give full details as to the procedures to be followed. All requirements mentioned must be seen as a compulsory necessity and part of the HelpDesk Policy. (I = Incident R = Request P = Problem) Process Definition Incident, Request and Problem Logging of I R P Processing of I R P Linking incidents and problems Assign workarounds Re-assign I R's Closing of I P's Auto logging of I R's Data Requirements: User information Incident/Request/Problem Categorization Status definition Responsibility Priority Escalation history Location

IT HELPDESK POLICY	
Detail description:	Reporting Requirements: Query facility Reporting on: Time taken to repair Cause type Call type Current status Call analysis Group statistics Audit trails Call statistics Integration requirements: Asset management Change management License management Repair management 11. HELPDESK SYSTEM SOFTWARE The HelpDesk system software must be a customisable system for automated call tracking, problem resolution and management, messaging, reporting and trend tracking. The system to be used is still to be determine.
Applicable forms: **Input documents:**	No handwritten documents will be handled at the HelpDesk as the operators will log all calls on-line and notification will be sent through e-mail. The only exception is for new users requiring user access with user access forms. No input documents are applicable
Reports ("D,E,F:):	Daily reports on: Calls logged: Showing status, priorities, escalation history, call type, etc. Reports to be distributed to HelpDesk manager. Reports to be filed in date sequence. Reports to be signed by HelpDesk manager prior to filing. Weekly reports on: Escalation history of all calls not resolved. Time taken to repair on all calls. Call analysis per support team. Reports to be distributed to HelpDesk manager and support team heads where applicable. Reports to be filed in date sequence. Monthly reports on: Audit trails Call statistics

IT HELPDESK POLICY	
	Reports to be distributed to HelpDesk manager. Reports to be filed in date sequence.
Approval: **Other matters 1:** **Other matters 2:** **Attachments:**	The approval of the Policy is the responsibility of the Mayoral Committee or its delegated assignee.

IT ASSET AND LICENSE POLICY

Policy name:	IT Assets and License Policy
Reference number:	
Date of last update:	29/05/2001
Circulation to:	All IT and personnel involved in Assets.
Brief description:	Maintaining records for all IT Assets, Licenses and Software
Scope:	Applicable to all SDR's (All Departments and Sections) Hardware and Software
Objective:	To keep track of all licenses, assets. To keep track of all cost per lifecycle of a specific asset.

IT ASSET AND LICENSE POLICY

Detail description:	Asset Tracking with Configuration: Includes all Components per Hardware Add, Change, Delete and Repair Functions as part of Asset System. The system must have the necessary functions to add, delete ,change and to update any repairs Forms for Asset logging and Tracking (Movements and Repairs) All Asset details must be reflected on all System Forms Unique Numbering System Each main Asset must have a unique Number. All components including software relating to that asset must be connected to the unique asset number. Repair History To keep track of the cost of repairs and maintenance of the asset. Warranty Details Must be reflected on all associated forms. License Tracking: Software will be reflected under the unique asset number Network Software Hardware Software Purchase of Hardware without Licenses If there is an existing open license agreement it must be reflected on the requisition of Hardware. Scrapping of licenses of obsolete Hardware Licenses must be scrapped with the Hardware where applicable. E.g. Unix Server plus Software. Asset Acquisition and Management Responsibilities and controls Refer to Standards in “Standards Policy” Recording and Storage of Licenses and Media Copies of Licenses off-site, record of licenses on asset system. All media must be stored per unique asset number where applicable (e.g. MOLP).

IT ASSET AND LICENSE POLICY

Applicable forms:	Must be developed, depend on specific Asset Tracking System Form from Stores for Updating of Assets Forms for Movement of assets Forms for Repair of Assets Forms redundant Hardware
Input documents:	Above Mentioned Form to be Filed by Asset Management Administrator
Reports ("D,E,F:):	Must be developed, depend on specific Asset Tracking System
Approval:	
Other matters 1:	
Other matters 2:	
Attachments:	

ACTS:

The following governmental acts either have a direct or an indirect bearing on the Information Use Policy, and are included here for completeness.

1. **Interception and Monitoring Prohibition Act 127 of 1992, and as amended Act 77 of 1995.**

   To prohibit the interception of certain communications and the monitoring of certain conversations or communications; to provide for the interception of postal articles and communications and for the monitoring of conversations or communications in the case of a serious offence or if the security of the Republic of South Africa is threatened; and to provide for matters connected therewith.

2. **Companies Act 61 of 1973, and as amended Act 37 of 1999.**

   To consolidate and amend the law relating to companies; and to provide for matters incidental.

3. **Copyright Act 98 of 1978, and as amended Act 125 of 1992.**

   To amend the Copyright Act, 1978, so as to amend or insert certain definitions; to make provision that computer programs be eligible for copyright as a separate category of work; to further provide for the conditions to be met before works become eligible for copyright; to further regulate copyright in broadcasts and programme-carrying signals; to further provide for the protection of the moral rights of the author of a work; to further provide for dealing with the infringement of copyright and for the remedies available upon such infringement: to further provide for presumptions in proceedings relating to infringement of copyright; to further prescribe penalties for the infringements of copyright; to further provide for the seizure of imported infringing copies; to further regulate the procedure relating to applications of the Copyright Tribunal: to extend the powers of the Copyright Tribunal regarding the granting of licenses; and to make provisions for the appeal against decisions of the Copyright Tribunal; and to provide for matters connected therewith.

4. **Intellectual Property Laws Amendment Act 38 of 1997**

   To amend the Merchandise Marks Act, 1941, so as to substitute, to delete or to amend certain definitions; to define certain expressions; to repeal the provisions relating to the unlawful trading in counterfeit goods in so far as these provisions are to be superseded by other envisaged legislation regarding the counterfeiting of goods; to adjust the powers of inspectors to enter and search premises and attach goods; to substitute or delete certain obsolete provisions and references; to delete a provision imposing a burden of proof on an accused; to provide for a presumption with respect to the offence of offering for sale or hire goods to which any false trade description is applied; and to adjust the provisions regarding penalties for offences; to amend the Performers' Protection Act, 1967, so as to delete or to amend certain definitions; to define certain expressions; to protect performances in countries which are members of the World Trade Organization; to lengthen the term of protection for performances to fifty years; to provide for all broadcasters; to adjust the provisions regarding penalties for offences: and to extend the application of the Act to performances which took place before its commencement to correspond with the Agreement on Trade Related Aspects of Intellectual Property Rights (the TRIPS Agreement); to amend the Patents Act, 1978, so as to define certain expressions; to amend or to substitute certain definitions; to clarity the provisions with respect to the payment of renewal fees, the priority dates of matter as opposed to patent claims, the principle of privilege regarding communications by or to patent agents and the assessment of damages; to bring the Act in line with the Trade Marks Act, 1993, the Designs Act, 1993, and the TRIPS Agreement; to provide for the implementation of the Patent Cooperation Treaty in the event of South Africa's accession thereto; to effect a correction in the Afrikaans text; to repeal or amend certain obsolete provisions and references; and to amend the long title; to amend the Copyright Act, 1978, so as to substitute, to amend or to delete certain definitions; to elaborate the requirement that a work must exist in a material form to qualify for copyright; to adjust the term of copyright in a cinematograph film and to extend the scope of copyright in computer programs in view of the TRIPS Agreement; to provide for all broadcasters; to amend the provisions relating to damages and other compensation for the infringement of copyright in order that it corresponds with the Trade Marks Act, 1993, and the Designs Act, 1993; and to substitute a certain word in the Afrikaans text; to amend the Trade Marks Act, 1993, so as to amend the provisions regarding marks that may not be registered as trade marks and those regarding the protection of well-known trade marks to ensure compliance with the TRIPS Agreement and Article 6ter of the Paris Convention; to effect a correction in the English text; to further regulate the relief for the infringement of registered trade marks; to provide that the registrar must keep a list of emblems of convention countries and international organisations; and to replace an incorrect reference; to amend the Designs Act, 1993, so as to define an expression; to delete a definition; to adjust the requirements for the registration of a design; to amend the provisions regarding the notification of registration and the certificate of registration; to adjust the provisions regarding compulsory licences in respect of certain registered designs and to further regulate the effect of the registration of a design and the amendment of an application for registration, and of a registration of

a design, to ensure compliance with the TRIPS Agreement; and to correct or to clarify certain provisions; and to provide for matters connected therewith.

5. Labour Relations Act 66 of 1995, and as amended Act 127 of 1998.

The 1995 Labour Relations Act ('the Act') includes workers in most areas of economic activity, the only exclusions being 'soldiers and spies'. The Act is an attempt to move away from the traditional adversarial system of labour relations to a more co-operative and inclusive one. It affords extensive organisational rights to trade unions, including comprehensive disclosure of information provisions. Also introduced are workplace forums, which compel consultation and joint decision-making between workers and management under certain conditions. However, a workplace forum must be initiated by a representative (majority) trade union and can only be requested in a workplace consisting of more than 100 employees. The 1995 LRA firmly promotes centralised bargaining through bargaining councils whose jurisdiction may be demarcated by NEDLAC. Where there are no existing bargaining councils the Act provides for statutory councils which the Minister of Labour may create and to which the Minister may appoint representatives even without agreement of the parties in that particular industry. Employees have the right to strike under the Act provided they comply with the fairly simple, legislated procedures. Failure to hold a ballot does not affect the legality of the strike. Moreover, strikes are protected if the procedures laid down in collective agreements or bargaining council constitutions (in the case of parties to the council) are followed as an alternative to the statutory procedure. The Act codifies many of the principles that were developed by the Industrial Court and the old Labour Appeal Court 2000 in respect of unfair dismissal. All employees have the right not to be dismissed unfairly. In addition, a residual unfair labour practice definition remains in the transitional provisions section and includes the prohibition against discrimination on any arbitrary basis, e.g. race, gender, age, etc. These provisions apply to applicants for employment and it appears that they are being utilised increasingly by applicants. The residual unfair labour practice section dealing with discrimination will fall away when the discrimination provisions of the Employment Equity Act come into operation. Subsequently a number of additional Codes of Good Practice have been published under the provisions of the Act including a Code of Good Practice on dismissals based on operational requirements, on picketing and on handling of sexual harassment cases. In addition, guidelines have been published on conciliation proceedings and on balloting for closed shop agreements.

6. Employment Equity Act 55 of 1998

The Employment Equity Act focuses essentially on discrimination, past and present. Its stated objectives include the elimination of employment discrimination, ensuring employment equity to redress the effects of discrimination and to achieve a representative workforce. The Act broadly contains two parts. The first, which is Chapter II, concerns prohibition of discrimination. The second, which is contained mainly in Chapters III, IV and V, concerns affirmative action and the ways in which it is to be implemented and enforced in practice. The part dealing with discrimination proceeds from the premise that all citizens are equal before the law and that any unfair discrimination against any employee on any ground is prohibited. What is prohibited is not discrimination, but discrimination that is unfair. Having said that, the Act further specifically authorises discrimination that amounts to affirmative action, and discrimination on the basis of the inherent requirements of the job.

7. Computer Evidence Act 57 of 1983, and as amended Act 5 of 1992.

To provide for the admissibility in civil proceedings of evidence generated by computers; and for matters connected therewith.

8. National Economic, Development and Labour Council Act 35 of 1994 NEDLAC may -

(a) prepare and issue codes of good practice;
(b) change or replace any code of good practice
(c) demarcate the jurisdiction of bargaining councils.

9. Government Gazette, No. 16047, 28 October 1994.

This Government Gazette deals with the provisions of the Labour Relations Act, 1956, made and entered into by and between the Municipal Employers' Organisation and the Employers' Organisation for Local Authorities.

The scope of application agreement refers to the terms of this agreement shall be observed in the Local Government Undertaking by the employers and the employees who are members of the employers' organisations and the trade union respectively in the Province of the Transvaal as it existed immediately prior to the date of coming into operation of the Constitution of the Republic of South Africa, 1993 (Act No. 200 of 1993), excluding the Municipal areas of Pretoria and Johannesburg.