XHARIEP DISTRICT MUNICIPALITY ICT POLICIES & PROCEDURES

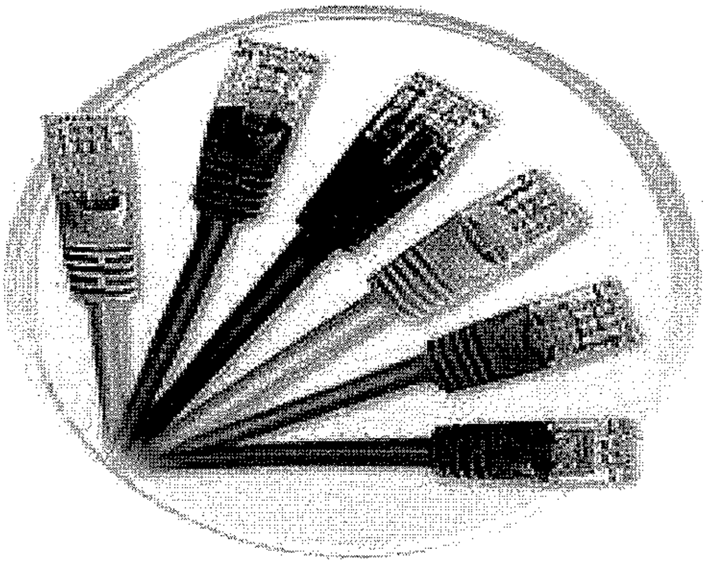


TABLE OF CONTENTS

OVERVIEW OF INFORMATION COMMUNICATION TECHNOLOGY POLICIES AND PROCEDURES 4

SECTION 01 - GENERAL INFORMATION COMMUNICATION TECHNOLOGY USAGE POLICIES AND PROCEDURES 7

SECTION 02 - SOFTWARE LICENSING POLICY 12

SECTION 03 - NETWORK AND INTERNET USE POLICY 15

SECTION 04 – E-MAIL POLICY 21

SECTION 05 – WEB SITE USE POLICY 26

SECTION 06 – ICT PROCUREMENT POLICIES AND PROCEDURES 30

SECTION 07 – COMPUTER SECURITY AND USAGE POLICY 33

SECTION 08 – INCIDENT HANDLING POLICY ..... [illegible]

SECTION 09 – CHANGE MANAGEMENT POLICY 48

SECTION 10 – PASSWORD POLICY 53

SECTION 11 – COMPUTER WORKSTATION USAGE POLICY 55

SECTION 12 – INFORMATION PROTECTION POLICY 57

SECTION 13 – INTERNAL NETWORKING POLICY 59

SECTION 14 – EXTERNAL NETWORKING POLICY 60

SECTION 15 – REQUEST FOR SERVICE (RFS) POLICY 62

SECTION 16 – NOTEBOOK (LAPTOP) COMPUTERS AND OTHER HANDHELD (E.G. PDA) DEVICES POLICY 67

SECTION 17 – STANDARDS POLICY 69

SECTION 18 – INSURANCE POLICY 71

SECTION 19 – EMPLOYEE SEPARATION POLICY 72

i) Incident Handling Policy – Section 08

j) ICT Change Management Policy – Section 09

k) Password Policy – Section 10

l) Computer Workstation Usage Policy – Section 11

m) Information Protection Policy – Section 12

n) Internal Networking Policy – Section 13

o) External Networking Policy – Section 14

p) Request for Service (RFS) Policy – Section 15

q) Notebook (Laptop) Computers and other Handheld (e.g. PDA) Devices Policy – Section 16

r) Standards Policy – Section 17

s) Insurance Policy – Section 18

t) Employee Separation Policy – Section 19

u) Software Usage Policy – Section 20

v) Network Copiers Policy – Section 21

PROTOCOL FOR INFORMATION COMMUNICATION TECHNOLOGY POLICY DOCUMENTS

ICT Policy documents shall be based as close as is practical on the ICT Policy Document Template and shall consist of five sections:

w) Introduction – will be a concise summary of the policy area and details.

x) Policy – is a section of clear and concise statements that will guide decision-making.

y) Procedures - (where applicable) are guides to actions that must be undertaken in order to deal with a particular situation consistent with the policy.

z) Definitions - (where applicable) are explanatory notes designed to assist people, not familiar with the terminology, in interpreting a policy document.

aa) References - will include documentation on the approval of the original and revised policy versions. Also to be included is the permitted Access Level. Related policies, procedures and documents are to be listed for cross-referencing.

SUBMISSION AND APPROVAL PROCESS FOR NEW AND AMENDED POLICIES AND PROCEDURES

Submissions of new and amended ICT policy material may be made, by any XHARIEP DISTRICT MUNICIPALITY employee, to the ICT Division utilising the following process:

bb) Use the policy document template and detail the proposed policy and justification, together with all reference documents, comments on guidelines, procedures and objectives and any other supporting material.

cc) The draft policy will then be presented, in complete form, to the next convenient meeting of the ICT Committee, where it will either be ratified or amended on the basis of submissions. If the policy is significantly amended then it will be published on the XDM intranet for a period of one week, with comments to be received. This process shall continue until the policy is approved with no significant amendments.

dd) The ratified policy and all details will then be published on the ICT Policy pages on the intranet.

Amendments and reviews of the policy and the guidelines shall be submitted for approval in line with the above. The entire policy document, including procedures (if applicable), shall be included in the documentation so that the material can be considered as a whole.

Additional policies and procedures may be included in the current document, or referenced separately.

Section 01 - GENERAL INFORMATION COMMUNICATION TECHNOLOGY USAGE POLICIES AND PROCEDURES

The ICT Policy and procedures (ICTPPs) set out the principles and standards, which determine acceptable use of the computing resources of the XHARIEP DISTRICT MUNICIPALITY. The primary aim of this ICTPP document is to balance the proper and efficient business use of the computing resources against the need for protection of the systems, services and information that make up those resources..

This document describes the basic computer policies and procedures that all of the XDM's employees, contractors and Users of the XDM's computer facilities are required to follow. This includes councillors, third party contractors, vendors, and others authorised by the XDM's management to use the XDM's computer systems.

The use of XDM's Information Communication Technology facilities in connection with municipal business and limited personal use is a privilege but not a right, extended to various municipal employees. The XHARIEP DISTRICT MUNICIPALITY's information and computing assets are critical to the XDM's success, and must be protected from loss, modification or destruction. Users of XDM's computing facilities are required to comply with all policies and procedures referred to in this document.

Users also agree to comply with applicable country, province and local laws and to refrain from engaging in any activity that would subject XDM to any liability. XDM reserves the right to amend these policies, procedures and practices at any time without prior notice and to take such further actions as may be necessary or appropriate to comply with applicable country, province and local laws.

To protect the integrity of XDM's computing facilities and its Users against unauthorised or improper use of those facilities, and to investigate possible use of those facilities in violation of XDM rules, policies and procedures, XDM reserves the right, without notice, to limit or restrict any individual's use, and to inspect, copy, remove, or otherwise alter any data, file, or system resource which may undermine the authorised use of any computing facility or which is used in violation of XDM rules or policies. XDM also reserves the right periodically to examine any system and other usage and authorisation history as necessary to protect its computing facilities.

XDM disclaims any responsibility for loss of data or interference with files resulting from its efforts to maintain the privacy and security of those computing facilities or from system malfunction or any other cause. Therefore employees are advised to maintain regular backups of their critical data.

XHARIEP DISTRICT MUNICIPALITY's information is defined as any information within its purview, including information that the XDM may not own but which is governed by laws and regulations to which the XDM is held accountable. It includes data in any form, that is owned and used by the XDM to conduct its business, and which is captured, stored, maintained, and accessed in the XDM's systems and on the XDM's equipment. All information stored on the XDM's computers and equipment, or travelling over computer networks, which has not specifically been identified as the property of other parties, will be treated as though it is a XDM asset.

Technology changes at a rapid rate and it is necessary for the policies and procedures to be regularly updated. Accordingly the IT Division of the XDM will authorise updates to the document as and when required. The latest version of the ICTPP document will be sent to the XDM Municipal Manager's Office for council review and approval on an annual basis.

SCOPE

This policy applies to all XDM employees throughout the XHARIEP DISTRICT MUNICIPALITY which includes, in alphabetical order, the following:

ee) XHARIEP DISTRICT MUNICIPALITY Sec 57 managers, and officials.

ff) It is the responsibility of all Head Of Departments and their operating units to ensure that these policies and procedures are clearly communicated, understood and followed.

This ICT Policies and Procedures' document describes the basic computer standards, policies and procedures that all of the XDM's employees, interns, contractors and controllable Users of the XDM's computer facilities are required to follow. This includes employees of utilities, contractors, vendors, and others authorised by the XDM's management to use the XDM's internal and external computer systems. The XDM employee who contracts for these services is responsible to provide the contractor/intern/vendor/supplier with a copy of these policies and procedures before any access is given.

These policies and procedures cover the usage of all of XDM's Information Communication Technology and communication resources, including, but not limited to:

gg) All computer-related equipment, including desktop personal computers (PCs), portable PCs, terminals, workstations, Personal Digital Devices (PDAs), wireless computing devices, telecomm equipment, networks, databases, printers, servers and shared computers, and all networks and hardware to which this equipment is connected.

hh) All electronic communications equipment, including telephones, pagers, radio communicators, voice-mail, e-mail, fax machines, multifunctional devices (MFDs), PDAs, wired or wireless communications devices and services, Internet and intranet and other on-line services.

ii) All software including purchased or licensed business software applications, municipal-written applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on municipal-owned equipment.

jj) All intellectual property and other data stored on municipal equipment.

kk) All of the above are included whether they are owned or leased by XDM or are under XDM's possession, custody, or control.

ll) These policies and procedures also apply to all Users, whether on municipal property, connected from remote via any networked connection (dialup, 3g, etc) or using municipal equipment.

ROLES AND RESPONSIBILITIES

There are a few key roles and responsibilities to be executed by XDM in order to ensure that the ICT Policies and Procedures are correctly implemented and adhered to, these being:

mm) *Users* - responsible for reading, understanding and adhering to this policy.

nn) *Managers* - are responsible for the effective utilisation of technology by subordinates and compliance with policy standards. Reports of misconduct will be brought to the attention of the appropriate XDM and Human Resources authority(ies) for corrective action. Minor transgressions will be handled at the lowest possible level. Incidents that involve ethical, security or privacy issues or are disruptive to a large User-group must be reported to Human Resources Division.

oo) *Human Resources Division* - responsible for the overall communication and enforcement of this policy, and subsequent revisions, to municipal employees. Also responsible for ensuring that the policy is consistent with other personnel policies and procedures adopted by the district and for recommending revisions to the policy as changes in working conditions may warrant.

pp) *Information Communication Technology Division* - responsible for the components of this policy that pertain to the efficient use of Information Communication Technology and resources. Also responsible for assisting the Human Resources Division staff with the effective communication and enforcement of the policy.

TERMS AND DEFINITIONS

Manual: System of approved policy statements and corresponding procedural guidelines and supporting forms that direct an organisation toward its operational goals.

Policy: Stated course of action with a defined purpose and scope to guide decision-making under a given set of circumstances within the framework of corporate objectives, goals and management philosophies.

Procedure: Series of prescribed steps followed in a definite regular order which ensure adherence to the guidelines set forth in the Policy to which the Procedure applies.

Activity: Action, element or decision representing a prescribed step in a Procedure process.

Task: Detailed component of an Activity specifying required behaviour to complete the activity.

Form: Pre-formatted document containing instructions and place-holders for data entry to monitor progress through a particular Procedure and to ensure proper record-keeping.

Information Communication Technology (ICT): Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving e-mail, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, PDA, pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Communication Technology Officer (ICTO): Responsible to the XDM for management of the District's information resources. The designation of an Information Communication Officer is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the XDM's information activities, and ensure greater visibility of such activities within and between local authorities. The ICTO has been given the authority and the accountability by XDM to implement policies, procedures, practice standards and guidelines to protect the Information Resources of the District.

Information Communication Technology (ICT): The name of the department responsible for computers, networking, telephone and data management.

Vendor: Someone who exchanges goods or services for money.

LEGAL AND CONSTITUTIONAL IMPLICATIONS

Non-compliance with the principles described in this ICTPP document may result in disciplinary action, possibly including dismissal. It is therefore vital that all employees and contractors to the XHARIEP DISTRICT MUNICIPALITY who utilise the XDM's systems are made aware of the Information Communication Technology Policies and procedures.

To achieve this, regular e-mails will be sent out advising people about the existence of the ICTPPs, and of any relevant updates or additions to the document. The document itself will be freely available in paper (hardcopy) and will be available electronically, on the XDM's Intranet. First time Users of the XDM's systems are required to agree that they will conform to these standards and codes of practice.

The XDM's computer systems and equipment (which includes telephones and cell phones) must only be used for conducting the XDM's business or for purposes authorised by the XDM's management. All electronic documents created, stored, or communicated using the XDM's computer systems and equipment are and remain the property of the XDM. The XDM's management may access documents or communications stored on its property or in its systems whenever warranted by business needs, legal requirements or authorised forensic investigations. The XDM's management reserves the right to monitor its systems for accounting and audit purposes, to ensure proper use, and to detect security violations. Employees should not expect that their communications using the XDM's systems are private. Use is subject to authorised audit by the XDM's management at any time and without prior notification.

Personal use of the XDM's computing equipment and facilities may be approved by the XDM's management if use is clearly insignificant compared to business use and it complies with the XDM's ICTPPs. Personal use will not be approved if it:

qq) Interferes or competes with the XDM's business.

rr) Interferes with an employee's duties or the duties of other XDM employees.

ss). Involves any incremental cost to the XDM.

tt) Provides information about, or lists of, the XDM's employees to others.

uu) Involves commercial or personal distribution lists.

Access to the Internet and the use of the XDM's e-mail systems are intended to be for the XDM's business related activities. However, incidental and infrequent personal use of the XDM's e-mail systems and access to the Internet for personal use during or outside your normal work hours are allowed without management approval provided none of the above prohibitions are violated and provided other ICTPPs contained in this document are not violated. Access to the Internet is however not a right of any employee.

Non-compliance with the principles described in these ICTPP documents may result in disciplinary action, possibly including dismissal.

Independent contractors who breach these ICTPPs may have their contracts terminated with immediate effect, and may be the subject of criminal or civil proceedings instituted against them by the XDM.

ASSISTANCE AND SUPPORT

Throughout this document reference is made to the ICT Unit. Whenever a new service is required, or a problem is being experienced or further information is required always in the first instance contact the ICT Unit on 051 713 9330/44. In most cases the ICT staff member taking your call will be able to immediately provide you with the necessary information or assistance.

SIGNATORIES

The appended signatories have accepted this document as the official XHARIEP DISTRICT MUNICIPALITY Information Communication Technology Policies and procedures Document.

Section 02 - SOFTWARE LICENSING POLICY

INTRODUCTION

End-User license agreements are used by software and other Information Communication Technology companies to protect their valuable intellectual assets and to advise technology Users of their rights and responsibilities under intellectual property and other applicable laws.

The XDM Software Licensing Policy applies equally to all individuals that use any XDM Information Resources.

2.1 SOFTWARE LICENSING POLICY OBJECTIVES

There are two main objectives that will be achieved by having an underpinning software licensing policy in place:

2.1.1 Ensure licensing compliance

2.1.2 Prevent piracy

2.2 POLICY STATEMENTS

The Software Licensing policy will take effect under different circumstances, namely:

a) Approval of new purchases

b) Manage installations

c) Monitor licensing

d) Physically secure disks/licenses

2.2.1 New Software

a) Units purchasing Software must consult with XDM ICT Office and verify that the product is compatible and appropriate before the purchase. New software must be approved by the relevant supervisor of XDM. This approval must be verifiable via a filed MEMO signed by all parties. New software is to be shipped to XDM when possible. XDM will retain all setup mediums, licenses and manuals, excluding end-User manuals. Any setup disks and/or licenses not currently stored in XDM must be relinquished to XDM upon approval of this policy.

2.2.2 Software Installations

a) All software installations will be performed by XDM ICT Office or vendors under supervision of the XDM ICT office, with XDM approval via instructions, or automatically via Active Directory. Software will not be installed without a proper license.

2.2.3 License Control

a) All licenses must be stored centrally within XDM. XDM ICT office will maintain a license inventory of all restricted licenses. This includes all purchased, granted, "free" for educational use, shareware, or any other restricted license.

2.2.4 Setup Medium Control

a) All mobile setup mediums (disks, CDs, floppies, tapes, etc) must be stored centrally within XDM's ICT office.

b) Licensed Software without a setup medium (direct download) will be stored and managed by XDM. XDM ICT unit is responsible for maintaining backups of licensed software.

2.2.5 General

a) XDM provides a sufficient number of licensed copies of software such that workers can get their work done in an expedient and effective manner. Management must make appropriate arrangements with the involved vendor(s) for additional licensed copies if and when additional copies are needed for business activities.

b) Third party copyrighted information or software, that XDM does not have specific approval to store and/or use, must not be stored on XDM systems or networks. Systems administrators will remove such information and software unless the involved Users can provide proof of authorisation from the rightful owner(s).

c) Third party software in the possession of XDM must not be copied unless such copying is consistent with relevant license agreements and prior management approval of such copying has been obtained, or copies are being made for contingency planning purposes.

d) All personnel are responsible for managing their use of ICT and are accountable for their actions relating to ICT security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.

e) All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected as it is government property.

f) On termination of the relationship with XDM Users must surrender all property and ICT managed by XDM. All security policies and procedures for ICT apply to and remain in force in the event of a terminated relationship until such surrender is made. Further, this policy survives the terminated relationship.

g) All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licensed software. The ICTO through ICT reserves the right to remove any unlicensed software from any computer system.

2.2.6 Disciplinary Actions

a) Violation of this policy may result in disciplinary action in alignment with XDM Human Resource disciplinary procedure.

Section 03 - NETWORK AND INTERNET USE POLICY

INTRODUCTION

Electronic communication is an indispensable business tool within the XHARIEP DISTRICT MUNICIPALITY. However, despite its benefits, unrestrained and uncontrolled electronic usage can cause a serious business liability. It is also understood that Users of the XDM's electronic communication system can intentionally or unintentionally infringe copyrights, violate trade secrets and trade marks, defame other people and businesses/institutions, harass individual/s, and commit the XDM to contracts. This can ultimately cause damage to the XDM, as it is generally liable for the acts of its Users. Therefore, in order to protect both the XDM and its Users' interests, it is important that employees are made aware of the limitations placed on their access to the XDM's electronic communication systems.

3.1 OBJECTIVES OF THE POLICY

The objectives of this policy are:

3.1.1 To ensure proper and sound management of the network and security systems.

3.1.2 To set responsibilities and limitations of the PC Users.

3.1.3 To foster discipline with regards to the XDM's confidential database.

3.1.4 To give effect to the general protection of the XDM's interests in respect of use of the electronic communication systems.

3.2 APPLICATION OF THE POLICY

The policy shall apply to:

3.2.1 All Municipal employees who are supplied with PC's and other ICT gadgets as a tool to enable them to perform their functions.

3.2.2 Full-time Councillors for the period of their tenure as full-time Councillors.

3.2.3 Individuals working for the associates of the District Municipality.

DEFINITIONS

Associate: A person or an organisation having partial rights or subordinate status whilst doing business with or for the XDM.

Browse: Read computer data files.

Chain letter: One of a sequence of letters, each recipient in the sequence being requested to send copies to a specific number of other people.

Computer: An electronic device that processes data according to a set of instructions.

Copyright: An exclusive legal right, given to the originator or his/her assignee for a fixed number of years.

Disclaimer: Renunciation of responsibility.

Employee: For the purpose of this policy, the meaning of an employee shall include Users who are not employees of the XDM.

Etiquette: Unwritten code governing behaviour.

Hardware: The mechanical and electronic components of a computer.

H.O.D: For the purpose of this policy, the meaning of the HOD shall include the Municipal Manager, and any Section 57 employee.

Megs (Megabytes): A measure of data capacity.

Network: A chain of interconnected computers.

Quantum: A sudden large increase or advance.

Software: The programs and other operating information used by a computer.

Users: Any authorised person who is given an access to a Computer Set (PC) of the XDM, including any person to whom the Computer set is allocated to for the purpose of executing official duties.

Web: Complete network of inter-connected series.

3.3 ACQUISITION OF NEW EQUIPMENT

The ICT Officer shall verify and approve specifications for all new electronic information equipment and software prior to purchase by each department.

After new software and hardware purchases, the ICT Division shall install, and allocate an IP address and other related services to them.

3.4 NETWORK USERS' REGULATIONS, LIMITATIONS, RESPONSIBILITIES AND SECURITY POLICY

The use of the Internet, e-mail and software facilities (hereafter "facilities") must be consistent with the business goals and objectives of XHARIEP DISTRICT MUNICIPALITY. Notwithstanding the above, the facilities may also be used for private matters, on condition that such use complies with the criteria as set out below, and would be considered by XHARIEP DISTRICT MUNICIPALITY to be reasonable and acceptable. In respect of this reasonable use, staff will be expected to exercise responsible, ethical behaviour when using the facilities. Inappropriate or illegal use of the facilities will result in the loss of privileges, disciplinary action and possible dismissal.

Use of the facilities is a privilege and not a right; consequently, staff members and/or agents of XHARIEP DISTRICT MUNICIPALITY are expected to strictly adhere to the following User guidelines:

3.5 Authorisation

3.5.1 Only Users, authorised by their HOD or authorised by the Municipal Manager (MM), will be allowed access to Internet and / or e-mail.

3.6 Network and Hardware

3.6.1 No User shall be allowed to attach any equipment to the network or computers without prior authorisation by the HOD in consultation with the ICT Division

3.6.2 Users shall not be permitted to provide User accounts to any other person.

3.6.3 The User shall not switch off the computer at the ON / OFF switch or at the wall plug as this can corrupt the Operating System.

3.6.4 Users should not engage in activities to damage hardware or software, disrupt communications, waste system resources, or overload networks with excessive data.

3.6.4 Users shall leave their computers switched on at all times as far as possible; but: the User must reboot their PC at least once a week during working hours.

3.7 Access and Data

3.7.1 Access for one User to another User's PC can only be authorised by the HOD or the User's superior and must be done in consultation with the ICT Division.

3.7.2 Each User shall be responsible for using his/her common sense and real world ethics to take precautionary measures to avoid violation of the objectives of the Network Policy.

3.7.3 Users shall not be allowed to give out their login and password to ANYONE.

3.7.4 Users shall not be allowed to use any other User's login and password to obtain unauthorised access to network resources.

3.7.5 Financial and Payroll system Users must not leave their systems unattended, the User shall either log out of the program before leaving his office or lock the office.

3.7.6 Users shall not write down or store their passwords in any physical form.

3.7.7 Users shall not be allowed to monitor another User's data communication, nor read, copy, change or delete another User's files or software, without the owner's permission.

3.7.8 Users shall not circumvent data protection schemes or exploit security loopholes.

3.7.9 XDM licenses the use of computer software from a variety of outside companies. XDM does not own this software or its related documentation, and unless authorised by the software developer, does not have the right to reproduce it except for back-up purposes.

3.8 Software

3.8.1 XDM employees shall use the software only in accordance with the license agreements and will not install unauthorised copies of commercial software.

3.8.2 XDM employees shall not download or upload unauthorised software over the Internet.

3.8.3 XDM employees learning of any misuse of software or related documentation within the Company shall notify the department manager or XDM's legal council.

3.8.4 According to applicable copyright law, persons involved in the illegal reproduction of software can be subject to civil damages and criminal penalties including fines and imprisonment. XDM does not condone the illegal duplication of software. XDM employees who make, acquire, or use unauthorised copies of computer software shall be disciplined as appropriate under the circumstances. Such discipline may include termination.

3.8.5 Any doubts concerning whether any employee may copy or use a given software program should be raised with a responsible manager.

3.9 General

3.9.1 Users should not create, access, display, download, save or transmit any text, file picture, graphic, or sound clip or engage in any conference that includes material which is obscene, libellous, indecent, vulgar, profane, or which advertises any product or service not permitted to minors by law.

3.9.2 Users members should not create, access, display, download, save or transmit threatening, racist, sexist, obscene, offensive, annoying or harassing language and / or materials such as broadcasting unsolicited messages or sending unwanted mail.

3.9.3 Use of the facilities for private commercial related activities is prohibited.

3.9.4 Users should adhere to all copyright, trademark, and licensing agreements and laws including seeking permission when required. In particular any use of software must strictly adhere to the terms and conditions of the license. Any unauthorised reproduction and/or use of proprietary software are strictly prohibited.

3.9.5 Users should not access chat rooms and under no circumstances must information of a confidential or proprietary nature be sent over the Internet.

3.9.6 Users should be aware of computer viruses and other destructive computer programs, and take steps to avoid being a victim or unwitting distributor of these processes.

3.9.7 XDM Administrators may deem it necessary to search any computer drive or file system for alleged violations of this policy. In particular, XDM retains the right to randomly monitor and intercept all employee communications, regardless of whether they are of a business or personal nature, including but not limited to e-mail and Internet usage. The monitoring of communications on XDM's communication infrastructures (whether it be Information Communication Technology or any other communication infrastructures operated by XDM) is necessary for the support and maintenance of XDM's communication infrastructures.

3.9.8 Users must use their best endeavours to ensure that the content of all authorised communications are accurate and concise. Users should use the same care in drafting and sending electronic communications as that afforded to traditional written communication.

3.9.9 All communications generated, sent, received or stored by electronic means, by Staff are prima facie deemed to be of a business nature and subject to monitoring and interception in terms of the provisions of the Regulation of Interception of Communication and Provision of Communication-Related Information Act 75 of 2002.

3.9.10 Any information available on XDM Information Communication Technology infrastructures may only be used at the sole discretion of XDM. Users may not disseminate any proprietary information belonging to XDM to third parties by means of the Internet or e-mail system.

Any use of the facilities in direct contravention of the above guidelines will be considered to be a misuse of the facilities. Acts of violations against this policy will be dealt with in terms of the disciplinary procedure of the XDM.

3.10 DISCLAIMER

Not all sources on the Internet provide accurate, complete or current information. Staff members need to be good information consumers, questioning the validity of the information.

Ultimate responsibility for resolution of problems related to the invasion of an employees privacy or loss of data rests with that specific employee. XDM assumes no liability for loss or damage to data or for any damage or injury arising from invasion of the employee privacy, or misuse of the facilities.

3.11 ACKNOWLEDGEMENT

I understand that all e-mail and Internet facilities are a resource operated and managed by XDM. I understand that any misuse of the facilities, may result in XDM taking appropriate disciplinary action against me. All disciplinary actions instituted for misuse of the facilities, shall be consistent with current Human Resource disciplinary procedure. Irrespective of internal disciplinary proceedings, XDM reserves the right to proceed with legal action, both civil and criminal, against me for any alleged violations of current laws.

I hereby state that I have read and will abide by this policy:

Signature______________________ Date ______/____/_______

Name: ________________________ Department: ____________________

XHARIEP DISTRICT MUNICIPALITY reserves the right to revise this policy, as it deems necessary.

NATURE OF MISCONDUCT AND POSSIBLE DISCIPLINARY ACTION PENALTIES

Nature of Misconduct	First Offence	Second Offence
1. Causing Disruptions	Disciplinary Action in Accordance with Disciplinary Procedure	Disciplinary Action in Accordance with Disciplinary Policy
2. Disclosure: unauthorised information; either personal or confidential	Disciplinary Action in Accordance with Disciplinary Policy	Disciplinary Action in Accordance with Disciplinary Policy
3. Illegal activities	Disciplinary Action in Accordance with Disciplinary Policy	Disciplinary Action in Accordance with Disciplinary Policy
4. Illegal attachments and installations on PCs	Disciplinary Action in Accordance with Disciplinary Policy	Disciplinary Action in Accordance with Disciplinary Policy
5. Leaving Financial and Payroll System on PC Unattended	Disciplinary Action in Accordance with Disciplinary Policy	Disciplinary Action in Accordance with Disciplinary Policy
6. Misrepresentation	Disciplinary Action in Accordance with Disciplinary Policy	Disciplinary Action in Accordance with Disciplinary Policy
7. Electronic vandalism	Disciplinary Action in Accordance with Disciplinary Policy	Disciplinary Action in Accordance with Disciplinary Policy

Section 04 – E-MAIL POLICY

4.1 INTRODUCTION

Electronic Mail (e-mail) functions much like ordinary mail. The sender writes an electronic letter and may add, if needed, attachments such as text documents, graphics or spreadsheets. The sender then 'posts' the message by adding the recipient's e-mail address, often selected from an electronic address book. These e-mail addresses may be people, departments or functions and include names and some indication of location.

E-mail uses resources that can be distributed over several data networks. The User's conduct contributes to whether or not the availability and confidentiality of the system is ensured.

4.2 RISKS OF E-MAIL

Since e-mail includes both the transmission and handling of sometimes sensitive information, care must be taken to protect the message from unauthorised access.

Threats can include the ability of individuals to change and copy information, or to distribute information to unauthorised parties. Users can also act anonymously, or with a fake identity, and spread information under an assumed name.

The use of e-mail is therefore open to a number of risks, including:

4.2.1 Inadvertent change or distribution of messages through error or negligence.

4.2.2 Unauthorised use, processing or distribution of messages.

4.2.3 Distortion, interruption or unwanted disclosure of messages.

4.2.4 Unwanted infection with, and distribution of, viruses or other harmful programs.

4.2.5 Unauthorised disclosure of confidential, proprietary or secret information.

4.2.6 Copyright infringement.

4.3 E-MAIL NAMING STANDARDS

The following naming standards have been agreed to and will apply for all XHARIEP DISTRICT MUNICIPALITY employees:

Category	Format
First Name:	Use only lowercase characters. Use the full first name, i.e., no nicknames, and do not use any middle names.
Initials:	Add the first initial of the surname.
Conflicts:	When defining a new User name, if such a name already exists, then the surname plus the first initial will be the users email username.

4.4 SIZE LIMITS OF MAILBOXES AND ATTACHMENTS

4.4.1 Users will avoid sending messages with attachments larger than 1MB to external emails. Users can use the following procedures to reduce the file size:

- Compress large attachments to make them smaller..

4.5 E-MAIL POLICY STATEMENTS

4.5.1 Incidental private use is permitted but this is subject to strict control. Abuse of this privilege may be regarded as misconduct.

4.5.2 From time to time the use of the e-mail system may be audited. This audits may be triggered by the following events:

4.5.2.1 XDM suspects the messaging infrastructure is abused or over utilized by private email;

4.5.2.2 Messaging irregularities are suspected;

4.5.2.3 Messaging virus attacks are suspected;

4.5.2.4 Messaging system warnings.

4.5.3 All e-mails created, sent, forwarded, stored or printed are the XDM's property but this excludes any e-mail where a copyright applies. The XDM reserves the right to inspect the XDM's e-mail at any time without notice.

4.5.3.1 Through using e-mail you will have been deemed to have read, understood and agreed to the policies and procedures relating to e-mail systems contained within these documents.

4.5.3.2 Do not, as a matter of course, forward confidential, secret or proprietary information to third parties. Delete any you receive from the e-mail system after having been read.

4.5.3.3 Only forward classified/confidential messages to other staff within the same work group and retain them on the e-mail system for a maximum of one month.

4.5.3.4 Do not send all messages as confidential as this negates the purpose and adds unnecessary overheads to the e-mail systems.

4.5.3.5 Check any e-mail enclosures for viruses, BEFORE opening, particularly if documents containing executable programs are sent. If you open a message and are prompted to "Enable or Disable macros" you should select "Disable" and scan for viruses. If any are found then notify the ICT Unit (051 713 9330). If none are found you may utilise the attachment.

4.5.3.6 If you get an attachment via e-mail which is unsolicited or of unknown origin, detach it and scan the file using your installed anti virus software. Alternatively delete it.

4.5.3.7 Employees are responsible for ensuring that they are utilising the most up-to-date anti-virus software. Employees must apply updates sent via e-mail as soon as they are received. The ICT Unit should be contacted if any update message is unclear or if you are unsure as to how to apply the update.

4.5.3.8 Make sure that the intended recipient of your message has suitable tools to work on any enclosed document(s).

4.5.3.9 Transmission of any material in violation of any laws, regulation, or management policy is prohibited. Avoid unnecessarily large distribution lists.

4.5.3.10 Check your mailbox regularly for received mail.

4.5.3.11Ensure that the content of your message cannot be misconstrued and that there is nothing unlawful about the transmission or content of your message.

4.5.3.12 From time to time, certain disclaimers may be required for messages requiring confidentiality, legal privilege etc. Request assistance from the XDM's legal advisor.

4.5.4 It is prohibited to display or transmit:

4.5.4.1 Offensive, defamatory, discriminatory or harassing material.

4.5.4.2 Sexually explicit or other offensive images or jokes.

4.5.4.3 Unlicensed copyright material.

4.5.4.4 Non- business related video and image files.

4.5.4.5 Any message which would be deemed unlawful pursuant to the applicable law of any governing jurisdiction.

4.5.4.6 Confidential, proprietary or secret information outside without authorisation.

4.5.4.7 Advertisements.

4.5.4.8 Chain letters.

4.5.4.9 Not to send or forward e-mail notices concerning virus or harmful code warnings to other employees.

4.5.4.10 Not to send a large number of e-mail messages to a single address as it may disable the destination mailbox.

4.5.4.11 Not to "broadcast" e-mail messages unnecessarily.

4.5.4.12 Not to create or participate in pyramid schemes.

4.5.5 When using electronic mail to communicate with people on the Internet:

4.5.5.1 Do not automatically forward internal mail to an Internet site.

4.5.5.2 When sending or forwarding e-mail to the Internet, do not include the names or User IDs of any XDM employees unless required.

4.5.5.3 Do not use auto-reply functions to respond to your Internet mail. If you use auto-reply functions such as Out of Office message option for your normal XDM internal mail when you are away, be sure to select the option that excludes sending the notices to Internet Users.

4.5.5.4 Employees shall not use an electronic mail account assigned to another individual to either send or receive messages.

4.5.5.5 Employees should regularly move important information from electronic mail message files to word processing documents, databases, and other files, as e-mail messages may be erased periodically, either accidentally or as part of normal archiving and file maintenance functions.

4.5.5.6 If employees receive unwanted and unsolicited e-mail (also known as SPAM), they shall refrain from responding directly to the sender. Instead, they should contact the ICT Helpdesk.

4.5.5.7 Employees shall not employ scanned versions of hand-rendered signatures to give the impression that an electronic mail message or other electronic communications were signed by the sender.

4.5.5.8 E-mail is a vital communications tool for the XDM. Employees should therefore access their e-mail inbox at least once per day. Unopened e-mail older than one calendar month will be deleted from the server. Contact the ICT Unit (051 713 9330) should further information relating to accessing e-mail be required.

4.5.5.9 It is the responsibility of individual employees to manage their own e-mail once they have downloaded it. It is suggested that unwanted e-mails are regularly deleted (in-box, sent items and deleted items) and important e-mails are moved to appropriate folders. Important attachments should be saved in an appropriate folder within the "My Documents" folder and saved to a network server for backup. Contact the ICT Unit should further information regarding the management of e-mail be required.

4.5.5.10 The ICT Division reserves the right to delete e-mails, with prior authority from the HOD, if space becomes an issue, but Users on leave/away will be taken into consideration in this regard and the User in question will first be informed before deletion takes place.

4.5.5.11 Private e-mail correspondence should be limited to a minimum, the quantum will be regulated.

4.5.5.12 Address books should be backed up at least once a month. Contact the ICT Division should further information regarding the back up of the address book be required.

4.5.5.13 Every outgoing message should contain a disclaimer at the end e.g. "All views expressed herein are the views of the author and do not reflect the views of the XHARIEP DISTRICT MUNICIPALITY unless specifically stated otherwise. The information is intended only for the person or entity to which it is addressed and may contain

confidential and/or privileged material. Any review, retransmission, dissemination or other use of, or taking action on any action in reliance upon, this information by persons or entities other than those intended recipient/s is prohibited. If you received this message in error, please contact the sender and delete the material from your computer."
Please contact the ICT unit for further assistance if you are unsure as how to automatically add this disclaimer to the end of all your e-mail messages.

Section 05 – WEB SITE USE POLICY

5.1 INTRODUCTION

The XDM Web Site is one of the most important means of internal communication and accordingly specific policies and procedures apply regarding what can be published to the site and how this content is managed and maintained.

5.2 SUBMISSION OF CONTENT AND USE OF THE SITE

The Site is to be used for lawful purposes only. However, should the User choose to use this Site from locations other than the Republic of South Africa, they do so at their own initiative and you are responsible for compliance with applicable local laws.

Users are prohibited from posting or transmitting, by means of reviews, comments, suggestions, ideas, questions or other information through the Site, any content which is, unlawful, harmful, threatening, abusive, harassing, defamatory, vulgar, obscene, sexually explicit, profane, hateful, racially, ethnically or otherwise objectionable content of any kind, including but not limited to:

5.2.1 Any content that encourages conduct that would constitute a criminal offence or give rise to civil liability, or otherwise violate any applicable local, provincial, national, or international law; or

5.2.2 Any content that constitutes an invasion of privacy; or

5.2.3 Any content that is an infringement of any intellectual property right; or

5.2.4 Any content that contains software viruses; or

5.2.5 Any content that constitutes a political statement, commercial solicitation, or "Spam"

Although XDM does not purport to review (nor is it under any obligation to do so) any submitted content, it reserves the right to remove any content from the Site that it deems, in its sole discretion, to be an infringement of the above or harmful in anyway whatsoever. Should this policy be breached then XDM may immediately terminate and/or suspend the User's access to all or parts of the Site, without any further notice.

5.3. Each User must warrant that:

5.3.1 They own or otherwise control all rights to the content that they may submit to the Site;

5.3.2 That any use of such content will not cause injury or harm to any person or entity; and

5.3.3 They will indemnify XDM or its affiliates, directors, officers and employees, for all claims resulting from the submitted content.
By submitting reviews, comments and/or any other content (other than personal details) to XDM for posting on the Site, the User automatically grants XDM and its affiliates a non-exclusive, royalty-free, perpetual, irrevocable right and license to use, reproduce, publish, translate, sublicense, copy and distribute such content in whole or

in part worldwide, and to incorporate it in other works in any form, media, or technology now known or hereinafter developed for the full term of any copyright that may exist in such content. Subject to this license being granted, the User retains any and all rights that may exist in such content.

5.4 The following activity on or through the Site is expressly prohibited:

5.4.1 Any non-personal or commercial use of any robot, spider, other automatic device or technology, or manual process to monitor or copy portions of the Site, or the content contained therein, without the prior written authority of XDM ; and

5.4.2 The collection or use of any listings, descriptions, or price lists from the Site, for the benefit of a competing merchant that supplies products comparable to those offered on the Site; and

5.4.3 Any use or action that imposes an unreasonable or disproportionately large load of traffic on the Site, or otherwise interferes with its proper and timely functioning.

5.5 The User is responsible for maintaining the confidentiality and security of their User Name and Password for access to the Site, and accepts full liability for all activities that occur under their User Name.

5.6 Any person that delivers or attempts to deliver any damaging code to this web site or attempts to gain unauthorised access to any page on this web site shall be prosecuted and civil damages shall be claimed in the event that XDM suffers any damage or loss.

5.7 THE USE OF THIRD PARTY CONTENT .

5.7.1 XDM hosts information, pricing, opinions and other content supplied by third parties ("Third Party Content") on the Site. XDM has no editorial control over such content. XDM will, therefore, not be responsible for any incorrect pricing due to typographical errors or errors in pricing.

5.7.2 Opinions, statements, offers or any other information that may constitute Third Party Content, is that of the respective User and not of XDM, its affiliates or any of their directors, officers, employees or agents. XDM, its affiliates, or any of their directors, officers, employees, agents, do not guarantee the accuracy, completeness, and/or usefulness of any Third Party Content. All Third Party Content is provided as is.

5.7.3 It is the Users' responsibility to evaluate Third Party Content available on and through the Site. XDM and its affiliates, and their directors, officers and employees are not liable for any loss, damage or harm caused by any Users reliance on Third Party Content obtained on or through the Site. Before making any decision or placing any reliance on Third Party Content provided on or through the Site, Users should take all further reasonable steps to ensure and verify the accuracy of such content. This notice must be displayed in its entirety should one wish to publish any Third Party Content obtained from the Site

5.7.4 XDM does not review (nor is it under any obligation to do so) or control any third-party web sites that link to or from the Site. XDM is not responsible for the Content of any Third Party site linked to or from the Site.

5.8 SERVICES ADVERTISED BY MEANS OF THE SITE

5.8.1 The price and potential availability for each listing on the Site, is listed on that particular item's page. XDM cannot guarantee the availability of every or any listing on the Site

5.9 INTELLECTUAL PROPERTY RIGHTS

5.9.1 All content included on this web site, such as text, graphics, logos, buttons, icons, images, photographs, audio clips, databases and software ("the Content'), is the property of XDM or its content suppliers and protected by South African and international copyright laws. Furthermore, the compilation (meaning the collection, arrangement, and assembly) of all content on this web site is the exclusive property of XDM and is protected by South Africa and international copyright laws.

5.9.2 Except as stated herein, none of the material may be copied, reproduced, distributed, republished, downloaded, displayed, posted or transmitted in any form or by any means, including, but not limited to, electronic, mechanical, photocopying, recording, or otherwise, except as permitted by the fair use privilege under the South African copyright laws or without the prior written permission of XDM or the copyright owner.

5.9.3 Users are expressly prohibited to "mirror" any content, contained on the Site, on any other server unless with the prior written permission of XDM.

5.9.4 Users are granted a limited, revocable, and non-exclusive right to create a hyperlink to the home page of the Site so long as the link does not portray XDM, its affiliates, or their products or services in a false, misleading, derogatory, or otherwise offensive matter. Users may not use any XDM logo or other proprietary graphic or trademark as part of the link without the express permission of XDM, its affiliates or content suppliers.

5.9.5All trademarks are the exclusive property of XDM or the Trademark holder.

5.9.6 The unauthorised submission, removal, modification or distribution of copyrighted or other proprietary Content is illegal and the User could be subject to criminal prosecution as well as personal liability for damages.

5.10 LIMITED LIABILITY

5.10.1 The information, content, services, products and materials published on the Site, including without limitation, text, graphics and links are provided on an "as is" basis. XDM makes no representations or warranties of any kind, express or implied, as to the operation of the Site or the accuracy, correctness or completeness of the information, contents, materials, or products included on the Site. Without limiting the generality of the afore-going:

5.10.1.1XDM does not warrant that the Site, will be error free, or will meet any particular criteria of accuracy, completeness or reliability of information, performance or quality; and

5.10.2 Whilst XDM has taken reasonable measures to ensure the integrity of the Site and its contents, no warranty, whether express or implied, is given that any files, downloads or applications available via the Site are free of viruses, Trojans, bombs, time-locks or any other date or code which has the ability to corrupt or affect the operation of your system.

5.10.2 To the full extent permissible by applicable law, XDM disclaims all warranties, express or implied, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose. XDM will not be liable for any damages of any kind arising from the use of the XDM site, including, but not limited to direct, indirect, incidental, punitive, and consequential damages.

5.11 PRIVACY

5.11.1 XDM respects the privacy of its Users. Without limiting the aforegoing:

5.11.1.1XDM is dedicated to maintain the privacy of its online visitors and Users. On this site, XDM does not collect personally identifiable information from individuals unless they provide it to us voluntarily and knowingly.

5.11.1.2 Any information collected is used solely by XDM and its business partners who are involved in the operation of this site for internal purposes. XDM's client lists are never sold to third parties, and we will not share personally identifiable information with third parties unless the person who has submitted the information has authorised XDM to do so, or if XDM is required to by law.

5.12 GOVERNING LAW

This site is hosted, controlled and operated from the Republic of South Africa and therefore governed by South African law.

5.13 HYPERLINKS

5.13.1 No person, business or web site may link to any page on this site without the prior written permission of XDM. Such permission could be obtained from the Municipal Manager at skaza@xhariep.gov.za or telephone 051 713 9304. This clause does not apply to parties that have entered into e-trader agreements with XDM.

5.13.2 Hyperlinks provided on this site to non-XDM sites, are provided as is and XDM does not necessarily agree with, edit or sponsor the content on such web pages.

5.14 FRAMING

No person, business or web site may frame this site or any of the pages on this site in any way whatsoever.

5.15 SPIDERS AND CRAWLERS

No person, business or web site may use any technology to search and gain any information from this site without the prior written permission of XDM. Such permission could be obtained from the Municipal Manager at skaza@xhariep.gov.za or telephone 051 713 9304.

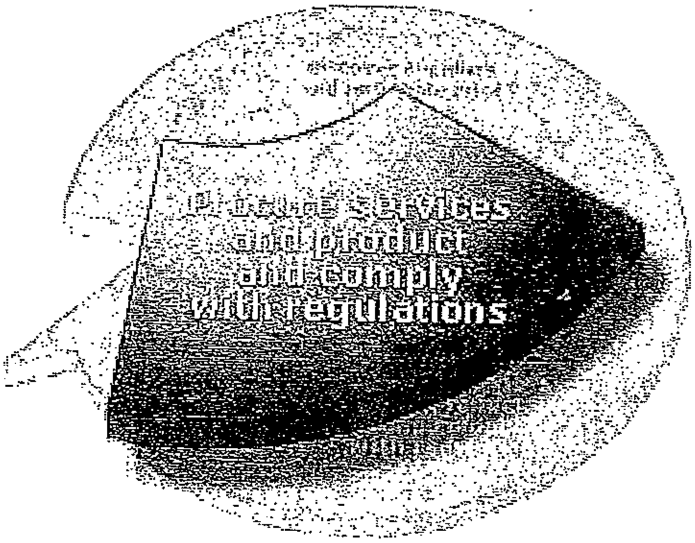
Section 06 – ICT PROCUREMENT POLICIES AND PROCEDURES

6.1 INTRODUCTION

6.1.1'Procurement' is the term we use to cover the entire process of buying goods and services from our suppliers.

6.1.2 XDM aims to provide its suppliers, both current and prospective, with up to date information on our requirements and procurement policies and procedures under which we seek to meet those needs. We also aim to develop a strong, mutually beneficial relationship with our suppliers based on openness, fairness and transparency in the conduct of our procurement process.

6.1.3 We believe our suppliers are an essential partner in making XDM a first class District Municipality and intend this information as an aid in contributing to enhance the capabilities of our suppliers in supplying our business requirements.



6.1.4 This policy guide is also intended to help XDM support the Government's procurement policy, as Municipal Managers are responsible and strictly accountable for the efficient and effective operation of their authorities, and have substantial managerial discretion in operational matters such as procurement. Accordingly, this guide generally does not set down prescriptive purchasing rules or procedures, except as set out in the Supply Chain Policy. The only exceptions are certain mandatory information and notification requirements which Cabinet has decided should apply to local government departments.

6.1.5 The procurement policy has general application to acquisition by purchase, hire, lease, rental, exchange and competitive tendering and contracting (outsourcing) arrangements. In this policy the focus is on purchasing by XDM of goods and services either directly or through a third party, and the terms "procurement" and "purchasing" are used interchangeably.

6.1.6 This policy has also endorsed certain principles namely: transparency, value for money, open and effective competition, fair dealing, accountability and due process, and non-discrimination.

6.1.7 The procurement policy approach supports XDM's sustainable industry and regional development objectives, through enhanced identification of competitive opportunities for district enterprises and their capabilities to exploit those opportunities.

6.2 OBJECTIVES OF XDM's PURCHASING POLICIES AND PROCEDURES

6.2.1 Our policies and procedures have been developed to ensure that all our purchasing activities achieve the following goals:

6.2.1.1 Procuring goods and services, which best contributed to XDM's performance.

6.2.1.2 To procure as efficiently as possible and to obtain best value for money, over whole of life, without compromising appropriate quality/standards.

6.2.1.3 To eliminate waste.

6.2.1.4 To encourage open and effective competition.

6.2.1.5 To provide for full and fair opportunity for domestic suppliers based within the District.

6.2.1.6 To improve business capabilities, including e-commerce capability.

6.2.1.7 To ensure good financial and budgetary control.

6.2.1.8 To ensure that BEE companies are given ample opportunity to tender for business with XDM.

6.2.1.9 To ensure compliance with State and Municipal Directives (MMFA).

6.2.1.10 To maintain ethical business standard and full legal compliance.

6.2.2 XDM should also note that environmental issues are an increasingly important element in procurement policy, and they should ensure that their procurement is consistent with the environmental policies and procedures of the Government.

6.3 PURCHASING POLICY STATEMENTS

6.3.1 We, at XDM, believe in:

6.3.1.1Fair Trade

6.3.1.2 Mutual Prosperity

6.3.1.3 Obeying Laws

6.3.1.3 Keeping Trust/ Confidentiality

6.3.1.4 Expanding business opportunities within the District

6.3.2 We promise potential suppliers an open and impartial opportunity to supply, based on economic factors such as quality, price, delivery time, continuity/stability of supply as well as continuity of management and technological compatibility and development capability.

6.3.3 We wish to establish good business relationships based on mutual trust and we aim to negotiate for mutually acceptable and beneficial conditions of business.

6.3.4 We look for suppliers who can best co-operate with us and help us to achieve our organisational goals and objectives.

6.3.5 In our purchasing activities as in all our areas of business, we make it a firm rule to obey the laws and respect their spirit. We also respect the confidentiality relating to products and technologies which we obtain and will not disclose such confidential information to third parties without prior agreement of the supplier concerned bearing in mind always that we are subject to the Access to Information Act.

Section 07 – COMPUTER SECURITY AND USAGE POLICY

7.1 INTRODUCTION

XDM computers and computer related resources are valuable assets that are relied upon heavily for information and decision making needs. XDM management and staff rely on the security of the computer systems to protect all systems and other valuable data on the Network. It is essential that these systems are protected from misuse and that both the computer systems and the data stored in them be accessed and maintained in a secure environment.

All ICT infrastructure must be used in a correct and responsible manner with high standards of professional conduct in accordance with XDM's code of conduct.

The policies and procedures described herein are those that the XDM intends to use in the normal operation of its computing and network systems and facilities. This document does not waive any claim that the XDM may have to ownership or control of any hardware, software, or data created on, stored on, or transmitted through the XDM's computing systems.

7.2 OBJECTIVES OF XDM's COMPUTER SECURITY AND USAGE POLICY

7.2.1 These Guidelines are issued to achieve and enforce the following:

7.2.1.1 Ensure the legal and responsible use of the XDM's computing systems and resources,

7.2.1.2 Outline responsibilities related to the accessing and usage of computer systems at the XDM,

7.2.1.3 Institute policies and procedures for the physical safeguarding of computer systems and their components, and

7.2.1.4 Provide methods for monitoring and enforcing these policies and procedures.

7.3 SCOPE

7.3.1 XDM policy regarding computer system security and usage shall:

7.3.1.1 Apply to all computer systems owned, leased or maintained by XDM. This includes: mainframe, mini and microcomputers/PCs; servers; networks (regardless of type - LAN, WAN, etc.); routers; bridges; hubs; and various peripheral equipment including but not limited to printers and modems.

7.3.1.2 Apply to all authorised Users of the XDM's computer systems.

7.4 RESPONSIBILITIES

7.4.1 The ICT Officer, will ensure that:

7.4.1.1 Appropriate and auditable internal controls, and

7.4.1.2 Appropriate and tested business continuity plan (See XDM ICT Business Continuity Plan for more detail), is in place for the computer systems at the District.

7.4.2 The ICTO or his/her designee is responsible for the design, installation, security and operation of the District's network in a manner consistent with these policies and procedures.

7.4.3 The ICTO or his/her designee will determine which department is responsible for instituting requirements for and approving all wiring; components; software and hardware purchases and installations for XDM's network.

7.4.4 The ICTO and technical advisors shall work together to promote connectivity between the XDM and other relevant networks.

7.4.5 The system and network administrator in conjunction with the network service provider are responsible for:

7.4.5.1 Developing, implementing and testing a backup plan in order to allow for the recovery of XDM's computer systems and networks in the event of a disruption.

7.4.5.2 Taking reasonable precautions to guard against the corruption of or damage to computer systems, software, and hardware or computing facilities.

7.4.5.3 Periodically evaluating the level of risk within the computer system (e.g., network, server, mainframe, etc.) and taking action, as needed.

7.4.5.4 Ensuring that all hardware and software license agreements are properly executed on all systems, networks, and servers for which they are responsible.

7.4.5.5 Ensuring that authorised User passwords are changed periodically.

7.4.5.6 Implementing technologically appropriate and reasonably current security on all workstations and microcomputers/PCs that access Private, Restricted or Confidential data.

7.4.5.7 Ensuring that problems of saturation, abuse, and malfunctioning software or hardware in the network are addressed.

7.4.5.8 Prohibiting all computer and network access in a manner that safeguards any data required to be retained for individuals with logon/operator IDs on XDM's systems when; the id has been inactive for 90 days; an authorised User has terminated employment, from XDM; or when a "courtesy account" is inactive or no longer needed.

7.4.6 XDM policies and procedures regarding computer system security and usage require that authorised Users follow password security standards including, but not limited to:

7.4.6.1 Periodically changing their computer system passwords.

7.4.6.2 Sharing or giving anyone else permission to use their logon/operator IDs or passwords is prohibited.

7.4.6.3 Storing access passwords in batch files, in automatic login scripts, in terminal function keys, in computers without access control or in other locations where another person might discover them is prohibited.

7.4.6.4 Sending access passwords through electronic mail is prohibited.

7.4.6.5 Exercise responsible, ethical behaviour when using the XDM's computing systems and resources.

7.4.6.5 Take reasonable efforts to safeguard computer systems and resources from theft; destruction; unauthorised alteration or exposure; or any form of compromise resulting from inappropriate intentional, negligent acts, or omissions.

7.4.6.5 Notify the ICT Division of any apparent or actual security violation.

7.4.7 Authorised Users will not:

7.4.7.1 Intentionally damage or misuse any of the XDM's computer system, including terminals, microcomputers/PCs, networks, printers or other associated equipment.

7.4.7.2 Intentionally write, produce, generate, copy, propagate or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software unless such action is part of authorised research or testing. Such software is often referred to as a virus, worm, Trojan Horse, or some similar name.

7.4.7.3 Use the XDM's computer systems and their applications in illegal activities.

7.4.7.4 Attempt to intercept any network communication for purposes including, but not limited to: reading message/file content; searching for passwords; rerouting packets; or packet "sniffing".

7.4.7.5 Access or copy files, regardless of media (e.g., paper, stiffy, etc.), of another User without prior consent from the file owner. Accessing the "private" files of others without permission, even if those files are unprotected, is prohibited. Altering another User's files or systems files without permission is vandalism and destruction of the XDM's property.

7.4.7.6 Use personally owned software in the XDM's microcomputers unless the software is properly licensed for such use.

7.4.7.7 Illegally distribute copyrighted software within or outside the XDM through any mechanism, electronic or otherwise.

7.4.7.8 Copy or remove software from the XDM's microcomputers in violation of the software license. This includes copying software from or to the XDM's microcomputers.

7.4.7.9 Unnecessarily or inappropriately use limited computer systems and resources including but not limited to such inappropriate uses as sending chain e-mails, spamming, mail bombing, generating unnecessary excessive print, etc.

7.4.7.10 Use the XDM's equipment for personal entertainment when other authorised Users need access to perform their work related tasks.

7.4.7.11 Print excessive copies of documents, files, data or programs.

7.4.7.12 Reconfigure any control switches or parameters, except as authorised by the appropriate IT Division.

7.4.7.13 Remove any of the XDM-owned or -administered equipment from any computer system, except as authorised by the appropriate system or network administrator.

7.4.8 XDM policies and procedures regarding computer system security and usage require that all their employees:

7.4.8.1 Are appropriately oriented and sign a computing awareness and data security compliance statement.

7.5 COMPUTER SYSTEMS AND SOFTWARE

7.5.1 The XDM's procedures regarding computer systems security and usage require that:

7.5.1.1 Only the service provider or ICT Division or their designees can modify the configuration of the XDM's computing infrastructure by adding or removing network links, computers, or peripherals (e.g., external disks, printers, modems, video systems, etc.); reconfiguring any control switches or parameters; upgrading processors, expanding memory, installing extras circuit boards, etc.

7.5.1.2 Computer system and application software will be appropriately backed up to allow for recovery if there is a disruption. Multiple generations of operating system, application and data backups should be maintained in both on-site and off-site storage facilities.

7.5.1.3 All vendor-supplied default passwords are changed before any computer or communications system is used for XDM related business.

7.5.1.4 An appropriate level of security is required on all computer systems on which Private, Restricted, Confidential or critical data is transmitted, stored or maintained.

7.5.1.5 Authorised User logon ids are inactivated if a User does not provide a correct password after three (3) consecutive attempts.

7.5.1.6 Passwords or pin numbers used to protect access to the XDM's data are not hard-coded into software developed by the XDM's staff or third parties.

7.5.1.7 The display and printing of passwords or pin numbers is masked, suppressed, or otherwise obscured such that unauthorised parties will not be able to observe or subsequently recover them.

7.5.1.8 Appropriate physical security standards are in place.

7.5.1.9 Passwords are required on all computer systems in which Private, Restricted, or critical data is stored or maintained.

7.5.1.10 Computer systems and networks have software installed and continuously enabled that will scan for computer viruses. Authorised Users downloading software from a network or installing software from a disk/ CDROM etc. shall check the software for possible virus infection before they use it.

7.5.1.11 Copyrighted software is not copied unless explicitly allowed in the software license agreement, except for one backup copy to be made and maintained by the original licensee. The XDM and its departments license many copies of microcomputer software. The XDM does not own this software. Employees are required to comply with software licenses and the Copyright Act.

7.5.1.12 Software upgrades address issues of incompatibility to previous versions, etc. of all supported software running on the affected computer system.

7.5.2 The ICT Department must approve all devices connected to the XDM's networks. Devices which do not comply, or which disrupt other network clients, may be disconnected at the discretion of the system or network administrator.

7.6 NETWORK SYSTEMS AND SOFTWARE

7.6.1 XDM policies and procedures regarding network systems and software security and usage require that:

7.6.1.1The XDM's procedures regarding network security and usage shall document network wiring, components, and software and hardware requirements.

7.6.1.2 Application and systems software available over the XDM's network must be handled in a manner that does not result in the number of copies/simultaneous Users dictated in the software license being exceeded.

7.6.1.3 All non-software proprietary information (e.g., text, images, icons, programs, etc.) retrieved from computer or network resources must be used in conformance with laws.

7.6.1.4 All inbound dial-up lines (e.g. modems) and real-time external connections (e.g., Internet) connected to the XDM's networks carrying administrative data must pass through an additional access control point (e.g., firewall) before authorised Users reach the log-in banner.

7.6.1.5 All in-bound dial-up lines to administrative and other computer systems are protected with extended User authentication systems as technically and reasonably possible.

7.6.1.6 Access security controls uniquely identify each remote access User, device and port.

7.6.1.7 Both ends of a dial-up connection are dropped when the access session is terminated.

7.6.1.8 Individuals are prohibited from connecting dial-up modems to workstations or microcomputers/PCs that are simultaneously connected to a network.

7.6.1.9 Direct network connections between any of the XDM's networks carrying administrative or other data and computers at external organisations, via the Internet or any other public network, are prohibited unless specifically approved by the appropriate manager, or their designee.

7.6.1.10 To the extent technically and reasonably possible, Private, Restricted or Confidential data transmitted over any communication network shall be transmitted in encrypted form or other appropriate and equally secure method.

7.7 WORKSTATIONS AND MICROCOMPUTER/PERSONAL COMPUTERS

Although micro computing offers improved productivity and cost-effectiveness, it requires the implementation of additional controls in those areas in which Private, Restricted, Confidential or critical data or hardware/software of the XDM may be at risk.

7.7.1 XDM policies and procedures regarding workstation and microcomputer/PC systems security and usage require that:

7.7.1.1 Workstations, personal computers, transportable computers and printers housed in unsecured areas are physically secured using appropriate security devices.

7.7.1.2 That all workstations and microcomputer/PC systems where necessary are outfitted with uninterruptible power supply (UPS) systems, electrical power filters, or surge suppressers, as appropriate.

7.7.1.3 Appropriate hardware and software security (e.g., cable lockdowns; password access control; data compression and encryption; audit log of access, updates; etc.) is placed on all microcomputers/PCs and transportable computers, which have Private, Restricted or Confidential data, stored in them (i.e., on the local drive).

7.7.1.4 There shall be a copy of all un-networked microcomputer/PC software prior to its initial usage, to the extent consistent with applicable licenses and laws. These copies (i.e., master copies) shall be stored in a safe and secure location separate from that of the microcomputer/PC (preferably off-site). These master copies shall not be used for ordinary business, but must be reserved for recovery from computer virus infections, hard disk crashes, and other computer problems.

7.7.1.5 Non-removable labels identifying the item as XDM's property shall be attached to all workstations, microcomputer/PC, transportable computers and related hardware.

7.7.1.6 Staff loaned or using XDM owned/funded transportable computers shall make every reasonable effort to secure and safeguard the physical integrity of the computer.

7.7.1.7 Authorised Users shall not program passwords, XDM assigned pin numbers (excluding telephone pin numbers) or logon /operator ids in any computer accessing the XDM's networks or Private, Restricted or Confidential data. This includes transportable computers. Additionally, microcomputers/PCs shall not be configured to allow a third party to access the XDM's network or data, without being prompted and required to enter a password.

7.7.1.8 All Private, Restricted and Confidential data on PCs not backed up centrally on a network, shall be backed-up on separate storage media after changes to the data have occurred. As noted previously, backups should be stored in an off-site location when possible.

7.7.1.9 Private, Restricted and Confidential data which have been backed-up shall not be used for data restoration purposes unless another back-up copy of the same data exists. This will prevent the only current copy of the data from being inadvertently damaged in the restoration process.

7.7.1.10 Proper disk maintenance practices are followed (e.g., clearly label stiffies; back up data, application and operating system media; store away from extreme cold/heat; protect from dust, excessive moisture or water; keep away from magnetic devices including radios, telephones, keys, wall magnets; etc.)

7.8 ACCESS AND USE

7.8.1 Access may be given to: stand-alone micro, mini or mainframe computers; or to networked computer systems. Staff access is primarily for functions associated with their work activities at the XDM. Staff members are given access to perform their job functions. It is however within the discretion of the relevant manager to permit a User limited private use.

7.8.2 The private use of any ICT resource is a privilege and not a right, and should in consequence be used in a responsible manner in accordance with the high standards of professional conduct and primarily in accordance with the XDM's code of conduct.

7.8.3 Information resulting from communication on the XDM's computer systems is the XDM's property. Authorised Users are presumed to be responsible for any activity carried out under their logon or operator ids.

7.8.4 XDM policies and procedures regarding computer system security and usage require that:

7.8.4.1 Only authorised Users have access to the XDM's computer systems.

7.8.4.2 Individuals requesting access to the XDM's computer systems will not provide false or misleading information to obtain access to the computing facilities.

7.8.4.3 Authorised Users are assigned unique logon IDs or operator IDs, and passwords to access the XDM's computers, networks and their application systems and data.

7.8.4.4 Logon IDs are only used by the person to whom they were assigned.

7.8.4.5 Logon IDs and passwords are not shared.

7.8.4.6 Authorised User passwords are changed periodically.

7.8.4.7 Individuals will not attempt to compromise authorised User passwords. This includes, but is not limited to cracking, decoding, copying password files, and "sniffing" packets for passwords or otherwise attempting to discover passwords belonging to other individuals.

7.8.4.8 Passwords are kept confidential and secure. Passwords must not be written down or stored in batch files, automatic login scripts, terminal function keys, or in computers without access control or in other locations where another person might discover them. Or subsequently recover them.

7.8.4.9 Authorised User passwords are not to be sent through electronic mail.

7.8.4.10 Computer and network access granted to an authorised User will be prohibited in a manner which safeguards any data required to be retained, for individuals with id that remain inactive for one year; when the authorised User transfers or terminates employment from the XDM; or when a "courtesy account" is inactive or no longer needed. Files of transferred or terminated employees may be reviewed and disposed of by the appropriate manager in a timely and effective manner.

7.8.4.11 Network connections are deployed to benefit the entire XDM and support its missions of public service including, research, administrative tasks and collaborative activities with other entities. These network connections are not to be used to provide commercial services not related to the XDM's missions as noted above nor shall they be used in any illegal activities.

7.8.4.12 The XDM's computing systems may not host sites for non-XHARIEP DISTRICT MUNICIPALITY organisations across any of the XDM's networks unless this activity is related to the XDM's mission of public service including, research, administrative tasks and collaborative activities with other entities.

7.8.4.13 Individuals are prohibited from remotely logging into (or otherwise using) any microcomputer/PC not designated explicitly for public logons over the XDM's networks, even if the configuration of the computer permits remote access, unless the individual has been given explicit permission from appropriate authorised personnel.

7.8.4.14 Many computers in the XDM are connected to the XDM's networks. Individuals must have an authorised logon id/operator id to access any of the XDM's computer systems including networks. The XDM's networks may also enable authorised Users to connect to computers at other related institutions. The fact that you can connect to a computer system does not automatically give individuals authority to use that computer system.

7.8.4.15 The mere lack of security on a network does not mean that a computer system is open and available for use by unauthorised Users.

7.8.4.16 Individuals must not perform or assist in the performance of any act that will interfere with the normal operation of computers, terminals, peripherals, networks, etc.

7.9 COMPUTER AND SOFTWARE USAGE

7.9.1 XHARIEP DISTRICT MUNICIPALITY policies and procedures regarding computer system security and usage require that:

7.9.1.1 The XDM's computer systems are used for purposes related to its mission of public service including, research, administrative tasks and collaborative activities with other entities.

7.9.1.2 Authorised Users use computing systems for the purposes related to the performance of duties by an employee, or other of the XDM's sanctioned activities. Use of the computing systems for commercial purposes not related to the XDM's missions is prohibited.

7.9.1.3 Abuse of the networks or of computers at other sites connected to the XDM's computers or networks by authorised Users are treated as abuse of computing resources at the XDM.

7.9.1.4 Any network traffic exiting the XDM's system is subject to the acceptable use policy/guidelines of the network through which it flows, as well as the guidelines noted herein. Possible loopholes in computer and network system security may not be used to damage computer systems, obtain extra resources, take resources from another User, or gain access to any the XDM's computer system or any computer system networked to the XDM.

7.9.1.5 Programs and files are confidential unless they have explicitly been made available to other authorised Users. The XHARIEP DISTRICT MUNICIPALITY does not routinely examine files of authorised User accounts however, to protect the integrity of the computer systems and to protect legitimate Users from the effects of unauthorised or improper use of the XDM's computing facilities, system, network or system administrators may inspect, copy, remove or otherwise alter any data, file or resource that may undermine the proper use of the computer system. Such action will be based on reasonable suspicion, authorised by the system, network or system administrator's supervisor and may be taken with or without notice to the User. Additionally, computer support personnel may access other's files when necessary for the maintenance of the computer system. When performing maintenance, every effort is made to insure the privacy and confidentiality of authorised User files.

7.9.1.6 Computer systems and networks have software installed and continuously enabled that will scan for computer viruses. Individuals downloading software from a network or installing software from a disk/CD-ROM etc. must check the software for possible virus infection before they use it.

7.9.1.7 Authorised Users must logoff the XDM's computer systems if they will not be accessing data for an extended time.

7.9.1.8 Authorised Users understand and comply with their responsibilities as noted in the responsibilities section of this document.

7.9.1.9 Authorised Users are aware that the XDM disclaims any loss or damage to software or data that results from its efforts to enforce these policies and procedures.

7.10 COMPLIANCE AND ENFORCEMENT

7.10.1 Any individual found misusing the XDM's computing systems, accessing the XDM's computing systems without approval, or otherwise violating these policies and procedures may be denied or given limited access to the XDM's computer systems and shall be subject to reprimand, suspension, or other disciplinary action in terms of XHARIEP DISTRICT MUNICIPALITY's disciplinary procedures.

7.10.2 Depending on the on the severity of the transgression, dismissal may even be appropriate. It is also possible that transgression of this policy, not only at the initiative of the employer, but also that of third parties, may lead to criminal prosecution and civil liability.

7.11 ACKNOWLEDGMENT

I have read the Computer Security and Usage Policy. I understand the contents, and I agree to comply with the said Policy.

Location:

Business Purpose:

Name:

Signature: ____________________ Date: ____________

Manager/Supervisor Signature: __________________ Date: ____________

Section 08 – INCIDENT HANDLING POLICY

8.1 INTRODUCTION

8.1.1 The aim of this policy is to:

8.1.1.1 Allow XDM to keep a record of all faults/problems and systems changes and to document such changes.

8.1.1.2 Allow the IT Division to monitor all computer faults within the departments so that any matters arising can be monitored.

8.1.1.3 Allow the ICT Department to monitor all requests to vendors.

8.1.1.4 Monitor cost to establish if it is still economically viable to repair certain equipment, or to allow management to make decisions to replace equipment that is no longer economically viable to be repaired or outdated and obsolete.

8.2 POLICY STATEMENTS

8.2.1 The following statements describe the incident handling policy:

8.2.1.1 The occurrence of all incidents and change and service requests must be logged with the ICT Division on 051 713 9330/9344. This policy covers a new service being required, a problem being experienced or further information being requested.

8.2.1.2 No action will be taken or assistance and support provided unless it is logged and a reference number provided. However, in most cases the staff member logging the call will be able to provide the required information or help immediately.

8.2.2 Depending on the nature of the problem or request, there are different procedures to follow when requesting a change, service or information or reporting a fault or a problem. However the policy is that:

8.2.2.1 The staff member must report the problem / fault to his or her manager. This can be done verbally, in writing or via e-mail.

8.2.2.2The ICT Division will then attend to the problem and issue a complaint number to enable them to reference the logged problems / faults.

In addition, no staff member may request any work directly from any ICT vendor without first following the above policy.

8.2.3 The vendors have been instructed that any requests attended to without to the proper policy and procedure having been followed will not be for the account of XHARIEP DISTRICT MUNICIPALITY. In cases where a staff member does not follow this procedure, any charge levied by the vendor, will be for the account of the relevant staff member.

8.2.4 General Guidelines

8.2.5 During an emergency situation the following guidelines and principles are advised:

8.2.5.1 Remain calm – A compromised system is a call to action but not a cause for panic.

8.2.5.2 Take good notes – Take detailed, organised and complete notes while handling any computer security incident preferably in an automated manner following a template so that no critical detail is missed especially if it may be required as evidence in the future. The documentation should be time stamped and auditable.

8.2.5.3 Notify the right people and get help – Inform those who 'need to know' about the incident. Again this should be an automated process.

8.2.5.4 Enforce a 'need to know' policy – This is one of the hardest things about handling an incident as they can be misdiagnosed early on. It is better therefore to inform those who need to be appraised of the situation so as to manage consistent communication.

8.2.5.5 Use out-of-band communications - Whenever possible, use telephones and faxes during a computer security incident. If the attackers have full access to the Help Desk's computers and they can read the mail. If the Help Desk's computers are used, this allows the intruder to know when the incident is reported and what response is received.

8.2.5.6 Contain the problem - The first time that the compromised computer is touched, it should be to disconnect it from the network, even if it is a core infrastructure resource. In order to contain the problem and regain control, all communication between the compromised host and other hosts on the network must be stopped.

8.2.5.7 Make backups - Make backups of system information as well as file-system information. Process tables, network connections, the /tmp directory and other volatile data sources should be dumped to files and then backed up with the rest of the file-system. Make multiple full backups using at least two different methods. Ensure file-system integrity with the first method and analytical portability with the second method. Any executables employed in the incident handling process should be trusted software. Once the file-system is backed up in a variety of manners, the computer can be halted.

8.2.5.8 Get rid of the problem - The problem must be completely eradicated. Determine the cause of the incident, then reload a clean operating system and improve the system's defences by installing the appropriate software. Only then can the system be reconnected to the network.

8.2.5.9 Get back in business - The goal is to make the recovered system resistant enough so that XDM has a fair chance of determining that it is under attack before it falls.

8.3 INCIDENT HANDLING PROCEDURE

8.3.1 The following phases are the constituents of XDM's incident handling procedure:

Phase 1 Identification

a). Assign a person to be responsible for the incident matching the person's skill set with the incident.

b) Determine the extent of the incident utilising diagnostic tool kits.

c) Be careful to maintain a provable chain of custody particularly when it relates to a security incident as the evidence may be required in a court of law. Examples of this could be:

- Identify every piece of evidence with a witness.
- Sign, seal and date a copy of everything.
- Place everything in a tamper-proof locked place that only a very limited number of people have access to (and be able to prove only a limited number of people have access).
- Sign, seal and date a copy of everything.

d) Coordinate with the people who provide your network services as they can proactively block incoming and outgoing traffic and can help trace security violators.

e) Notify the appropriate officials.

Phase 2 Containment

f) Deploy the On-Site XDM team to survey the situation avoiding disruption of normal routines. Task somebody to be the 'recording secretary' so that nothing is left to memory possibly using an Incident Containment Form template and Incident Survey Form that was filled in by the incident handler.

g) Keep a low profile so as to contain the problem and not raise tension at XDM unnecessarily.

h) Avoid potentially compromised code so as not to risk 'spreading' the incident's impact.

i) Back up the system.

j) Determine the risk of continuing the operation of the system. The On-Site XDM team only provides a recommendation and presents the data to justify the recommendation and the XDM ICT executive must make the actual decision itself.

k) Continue to consult with the System Owners so that they are informed and will not disrupt the team that is handling the incident.

Phase 3 Eradication

l) Determine the cause and symptoms of the incident.

m) Improve defences.

n) Perform vulnerability analysis.

o) Remove the cause of the incident.

p) Locate the most recent clean backup.

Phase 4 Recovery

q) Restore the system.

r) Validate the system.

s) Decide when to restore operations when it would have least business impact.

t) Monitor the systems.

Phase 5 Follow-up

u) Develop a follow-up report.

Section 09 – CHANGE MANAGEMENT POLICY

9.1 INTRODUCTION

The Information Resources infrastructure at XDM is expanding and continuously becoming more complex. There are more people dependent upon the network, more client machines, upgraded and expanded administrative systems, and more application programs. As the interdependency between Information Resources infrastructure grows, the need for a strong change management policy is essential.

From time to time each Information Resource element requires an outage for planned upgrades, maintenance or fine-tuning. Additionally, unplanned outages may occur that may result in upgrades, maintenance or fine-tuning.

Managing these changes is a critical part of providing a robust and valuable Information Resources infrastructure.

9.2 OBJECTIVE OF THE CHANGE MANAGEMENT POLICY

The purpose of the Change Management Policy is to manage changes in a rational and predictable manner so that staff and stakeholders can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the User community and to increase the value of Information Resources.

The XDM Change Management Policy applies to all individuals that install, operate or maintain Information Resources.

9.3 DEFINITIONS

9.3.1 Change Management: The process of controlling modifications to hardware, software, firmware, and documentation to ensure that Information Resources are protected against improper modification before, during, and after system implementation.

9.3.2 Change:

9.3.2.1 any implementation of new functionality

9.3.2.2 any interruption of service

9.3.2.3 any repair of existing functionality

9.3.2.4 any removal of existing functionality

9.3.3 Scheduled Change: Formal notification received, reviewed, and approved by the review process in advance of the change being made.

9.3.4 Unscheduled Change: Failure to present notification to the formal process in advance of the change being made. Unscheduled changes will only be acceptable in the event of a system failure or the discovery of security vulnerability.

9.3.5 Emergency Change: When an unauthorised immediate response to imminent critical system failure is needed to prevent widespread service disruption.

9.4 POLICY STATEMENTS

9.4.1 Every change to a XDM Information Resources resource such as: operating systems, computing hardware, networks, and applications is subject to the Change Management Policy and must follow the Change Management Procedures.

9.4.1.1 All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) need to be reported to or coordinated with the leader of the change management process.

9.4.1.2 A Change Management Committee, appointed by ICT Leadership, will meet regularly to review change requests and to ensure that change reviews and communications are being satisfactorily performed.

9.4.1.3 A formal written change request must be submitted for all changes, both scheduled and unscheduled.

9.4.1.4 All scheduled change requests must be submitted in accordance with change management procedures so that the Change Management Committee has time to review the request, determine and review potential failures, and make the decision to allow or delay the request.

9.4.1.5 Each scheduled change request must receive formal Change Management Committee approval before proceeding with the change.

9.4.1.6 The appointed leader of the Change Management Committee may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back-out plans, the timing of the change will negatively impact a key business process such as year end accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events.

9.4.1.7 Customer notification must be completed for each scheduled or unscheduled change following the steps contained in the Change Management Procedures.

9.4.1.8 A Change Review must be completed for each change, whether scheduled or unscheduled, and whether successful or not.

9.4.1.9 A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:

9.4.1.9.1 Date of submission and date of change

9.4.1.9.2 Owner and custodian contact information

9.4.1.9.3 Nature of the change

9.4.1.9.4 Indication of success or failure

9.4.1.10 All XDM information systems must comply with an Information Resources change management process that meets the standards outlined above.

9.5 DISCIPLINARY ACTIONS

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of XDM Information Resources access privileges, civil, and criminal prosecution.

9.6 ADDITIONAL AREAS COVERED BY XDM CHANGE MANAGEMENT POLICIES

Request Management

9.6.1 Enhancement requests and bug defect reports are captured and submitted to business and ICT management for review. Personnel responsible for Infrastructure Support roles are charged with the responsibility to capture, prioritise, and submit change requests to the appropriate change management process.

9.6.2 A business sponsor is assigned for change requests, and is notified as requests are captured. Infrastructure Support personnel categorise change requests based upon priority as enhancements, bugs, patches, updates, and any other "emergency" need. Dependent on this priority, the subsequent routing of the request is expedited. Infrastructure Support Issues and requests are managed throughout the change management life cycle.

9.6.3 Infrastructure Support personnel have the ability to manage the request management process, including: measuring process performance criteria, escalating inactive requests, prioritising "emergency" fixes, and reporting progress of requests to Users.

9.6.4 Business analysis is performed to determine likelihood of success, significance to business, resources required, and business justification.

9.6.5 A Business Analyst role analyses requests to assess risk of solution implementation and to determine minor / major impact to the business. If minor impact, the business analyst routes requests to technical analysis for further action (includes bug reports). If major impact, business analyst function performs business justification in conjunction with technical analysis, including likelihood of success, significance to the business, resources required, and system interdependencies. When complete, the business analyst prioritises based on analysis and routes to business management for decision-making.

9.6.6 Request Analysis: Technical analysis is performed to determine system dependencies, technology resources / techniques required, and project estimates.

9.6.7 For bug defect reports, a technical analyst function assesses and routes the report to appropriate development teams for immediate action. A technical analyst function identifies technical feasibility of change requests, including impacts to existing infrastructure and development, testing, and release schedules.

9.6.8 <u>Request Reporting</u>: The organisation is capable of retaining visibility on the status of requests and projects as they are analysed, prioritised, designed, developed, tested, and deployed.

9.6.9 Infrastructure Support tools are able to retain visibility and status for submitted requests through every phase of the change management process, including details about the deployment of the change. Infrastructure Support people and tools are integrated into Help Desk and Enterprise management tools, to quickly analyse and prioritise requests.

9.6.7 Deployment Management

9.6.8 The change management process follows a logical order and is controlled to ensure the logical evolution of effective enhancements to Production environments. "Major impact" projects are first built / configured as prototypes to demonstrate to management business justification and feasibility. Preliminary testing (including functionality and performance), business acceptance, and adjustments to design are used as specifications for solution development. Infrastructure changes are first built / configured / integrated in the development environment(s), followed by testing in the Test / QA environment, and are deployed to the Production environment in intermediate steps as business needs require. These may include staging, training, approvals by affected parties and management, or other activities and environments after testing, but prior to Production. Infrastructure component purchases (software, hardware, & network components) are coordinated using Requests for Proposal (RFPs) and vendor proposals to determine the best fit for the business needs based on solution requirements and specifications.

9.6.9 Procedures are in place to ensure that system changes may be immediately demoted or restored to a prior state, in the event of an unsuccessful or undesired deployment of infrastructure changes to Production environments. Business units that will be directly affected by an enhancement are given right of approval / disapproval / delay prior to a particular change's deployment into Production. This may include end-User training, documentation, and staging, as the business unit's needs require.

9.6.10 Production Deliverables are released concurrently or prior to Conversion / Roll-Out of the solution. Deliverables should include all applicable editions or updates to User and administration manuals, configuration references, topology diagrams, support procedures, and business continuity plans. Process Testing / Quality Assurance are conducted to ensure reliability and performance of all components of the organisation's technology infrastructure.

9.6.11 Emergency requests are handled in a similar manner to normal requests, with minor differences to allow for expedited development, testing, and release. Emergency / Bug changes are verified by business and technical analysis, and are then expedited through a simplified promotion and deployment process. Emergency releases must be authorised by a pre-determined manager, and logged into the appropriate system for audit purposes.

9.6.12 All emergency build / configuration / integration changes must be tested in all sufficient phases to ensure quality performance without adding additional disturbances to the current systems.

Emergency releases should be communicated to the User and administration population to alert them to the need and impacts of the emergency changes.

9.6.13 <u>The Configuration / Release management</u> function provides administration and control over the Deployment Management. A release management function has the responsibility to control the deployment of changes from one environment to the next. No other role should be allowed to "push" or "pull" changes from one environment to another, and the release management function has the authority to approve or deny change promotions and/or deployments. This function may be different personnel for each promotion stage, depending on business requirements. Release management administers and oversees Version Control and program libraries, and other systems software that automate the change deployment process.

9.6.14 All changes made for deployments to each environment are logged for solution module versions, date/time stamp, identification of User deploying the change, and execution steps for the deployment. Changes that fail in their deployment to the Production environment are analysed for root causes, and these findings are documented for organisational reference.

9.6.15 Availability of Infrastructure components is maintained within service-level agreements and business requirements. If availability of these components must be interrupted, downtime for deployment is scheduled appropriately and Users of the affected systems are notified sufficiently in advance of the change deployment to ensure business continuity.

9.6.16 The version control system controls the check-in / check-out of software and subsequent deployment throughout the deployment process. It does so by ensuring that the following concepts are possible: Either no two Users may check-out and check-in software for changes at the same time, or if simultaneous check-outs are allowed, a tool or process for reviewing and merging changes is used prior to check-in. Check-in of previously checked-out software always changes the version label in the system, such that no two versions are labelled alike. Only new software modules are allowed to be checked-in without checking them out first. The version control system is used as the source for all deployments of software to TEST/QA and PROD environments.

Section 10 – PASSWORD POLICY

10.1 INTRODUCTION

A computer access password is the primary key to computer security. The importance of password maintenance and security cannot be over emphasised. All employees and users of the XDM's computer facilities are solely responsible for the integrity and secrecy surrounding passwords allocated for their usage. The password uniquely identifies employees and users, and allows access to the XDM's information and computer services. For the users' protection, and for the protection of the XDM's resources, the password must be kept secret and not be shared with anyone else.

The ICT unit should be contacted if any further password information is required, or if there is any uncertainty surrounding the usage, applicability, and installation or issuing of passwords.

10.2 PASSWORD POLICY

10.2.1 All user-chosen passwords for computers and networks shall be difficult to guess. Do not choose:

a) Words in a dictionary

b) Proper nouns

c) Geographical locations

d) Common acronyms

e) Slang

f) Derivatives of user-IDs

g) Common character sequences such as "123456"

h) Spouse's name

i) Children's/boyfriend's/girlfriend's/pet's names

j) Car license plate

k) Your ID number/ birth date

10.2.2 Do not:

a) Construct fixed passwords by combining a set of characters that do not change, with a set of characters that predictably change.

b) Construct passwords which are identical or substantially similar to passwords previously employed.

c) Write down or otherwise record a readable password and store it near the access device to which it pertains.

10.2.3 Further policy statements:

a) Passwords shall not be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorised persons might discover or use them.

b) All vendor-supplied default passwords shall be changed before any computer or system is used.

c) All passwords shall be changed immediately if they are suspected of being disclosed, or known to have been disclosed to unauthorised parties.

d) Regardless of the circumstances, passwords must never be shared or revealed to anyone else by the authorised user.

e) Employees and users:

i. Are responsible for all activity performed with their personal user-IDs

ii. Shall not allow the user-IDs to be used by anyone else

iii. Shall not perform any activity with other users' IDs.

f) Employee and user generated passwords should in general have the following characteristics:

i. Be at least 6 characters in length

ii. Contain at least one alphabetic and one non-alphabetic character

iii. Contain a non-numeric character in the first and last position

iv. Contain no more than three identical consecutive characters in any position from the previous password

v. Contain no more than two identical consecutive characters

vi. Not contain the user-ID as part of the password

vii. Be changed at least every three months for systems that do not automatically force regular password changes.

g) "Screen savers" should be activated after 10 minutes of inactivity as a maximum, and should be password controlled.

h) Certain systems have specific password requirements over and above those shown above. These systems will prompt the user for the correct information. If in any doubt, contact the ICT unit for further information.

i) Should you forget your password contact the ICT unit for assistance. Please be aware that the ICT unit personnel are not permitted to automatically reset or reissue passwords. Replacement passwords will only be issued once certain prescribed security checks have taken place and this process may take some time to complete.

j) Refer to the ICT unit for details on Password resets. Please note though that according to the agreed Security Procedures, passwords will only be issued if the person to whom the password is being issued is identifiable.

Section 11 – COMPUTER WORKSTATION USAGE POLICY

11.1 INTRODUCTION

The XDM has a large variety of assets. Many are of great value to the XDM's success as a business. They include the physical asset and extremely valuable proprietary and confidential information. Protecting these assets is critical. Their loss, theft or misuse could adversely affect the XDM.

Every employee is responsible to help reduce the possibility and consequences of theft of all personal XDM computing resources and devices (e.g., desktops, laptops, PDAs and similar hand-held devices), related materials such as diskettes, memory keys and printed output, and the information they contain. No matter where these assets are located - .in the office, in the home, at a hotel, in a plane or car, etc. they must be protected appropriately. This section describes the actions that must be taken to protect these physical assets. Based on specific circumstances individuals may need to take additional actions to provide adequate protection. In addition, the requirements specified in the Protecting XDM Information section of this document to protect the information contained on workstations and related storage media, must be followed.

Employees are personally responsible for protecting any XDM property and information entrusted to them and for helping to protect the XDM's assets in general. In the event of the loss, destruction, or damage to an asset, for any reason, please refer to the Insurance policy and procedures.

The term Notebook is defined to include any portable computing device including but not limited to notebook computers, laptops, electronic diaries, PDAs, portable scanners etc.

11.2 POLICY STATEMENTS

11.2.1 Always use the physical (locking cable) or dock locking mechanisms if provided with your workstation.

11.2.2 If you work in an office that can be locked, and where regulations allow, lock the office.

11.2.3 Activate the password protected keyboard/screen lock.

11.2.4 Lock up all materials that contain XDM confidential information, or take them with you.

11.2.5 At the end of the workday, if your workstation is portable, secure it in a desk or filing cabinet or take it with you.

11.2.6 Keep notebooks in your possession if at all possible.

11.2.7 When travelling by air, do not put notebooks in checked baggage, and be alert to the possibility of theft when going through security checkpoints at airports.

11.2.8 When travelling by car, protect notebooks by locking them in the car boot when you begin your travel.

11.2.9 If you must leave the notebook in a hotel, lock it in the hotel safe if one is available. If a safe is not available and you have a locking cable (e.g. Kensington Cable), use that mechanism.

11.2.10 If you are travelling with XDM confidential material recorded on portable media such as paper, diskette, CD, notebook, etc., you must protect this media according to the same guidelines listed above for protecting your notebook.

11.2.11 If your workstation, or XDM confidential information, is stolen or lost, you must report the loss to the ICT unit and your manager as soon as the loss is discovered.

11.2.12 NO workstation, printer, fax machine etc. may be moved to a new location or to a new user without informing the Asset Register unit so that the asset register can be updated.

11.3 New workstations are specifically configured with standard tested settings. NONE of the settings should be changed. Workstations found to be to be operating incorrectly due to non-standard settings will incur extra maintenance fees.

Section 12 – INFORMATION PROTECTION POLICY

12.1 INTRODUCTION

The XDM has a large variety of assets, including valuable proprietary and confidential information. Protecting information is critical. XDM information is an asset of the XDM and needs to be protected wherever it exists. This section identifies basic controls that must be active on all types of computer workstations and media to protect the XDM's information. The next section discusses the additional requirements that exist when dealing with the XDM's confidential data. Note that several different controls are specified. They address different threats, and all the controls that are available on a workstation must be implemented.

The primary requirement for protecting the XDM's information is that it must be protected from all access or viewing except by people who have a business need to know the information.

12.2 POLICY STATEMENTS

a) All data created, stored or archived on any equipment housed within XDM premises or owned by the XDM and used by XDM employees and any other authorised user, is the XDM's property. The XDM reserves the right to request and inspect this data at any time without notice.

b) The unauthorised possession and/or usage of any equipment or software that could potentially be used to overwrite or alter any of the XDM's data, no matter where or how stored, will result in appropriate disciplinary action being taken.

c) A person who intentionally and without authority to do so interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective is guilty of an offence in terms of Section 86(2) of the ECT Act 25 of 2002 and may be liable to disciplinary action and/or criminal prosecution.

d) The following security controls must be activated on all computer workstations:

  i. Set a power-on password;

  ii. Set a password protected keyboard/screen lock that is automatically activated by a period of inactivity - the inactivity time interval should be no more than 10 minutes

e) Computer workstations available for shared use in any XDM location are not required to have power-on and keyboard/screen lock passwords applied. However XDM employees must not place XDM confidential information, file sharing software, user-ID files, mail files or databases on such workstations.

f) When you store XDM confidential information on computer systems (e.g. group web sites, access databases, or other shared data repositories), you must use software security controls to manage and limit access to the information.

g) Security controls must never be set to allow unrestricted access (e.g., World-readable, "public") to XDM confidential information, including calendars. To understand how to correctly set or use the security controls, advice or assistance will be provided by the ICT unit.

h) When XDM confidential information is stored on removable computer media, such as diskettes, memory keys, compact disks (CDs), etc., the information must be protected against theft and unauthorised access. Label the media confidential and keep them in a locked area or storage device when they are not in use. Never leave them exposed in unattended areas.

i) When printing XDM confidential information the information must be protected against theft and unauthorised viewing - the term "printer" includes printers, plotters, and any other device used to create hard copy output.

j) XDM confidential information may only be printed:

i. In a controlled access area, with access based on "need to know".

ii. In an attended XDM printer facility, where the output is given only to its owner.

iii. On a printer with capture/release facility that you control.

iv. On a printer that you are personally attending.

v. If none of these options are available at your location, you may use a printer located within an open area internal office space, but you must pick up your printout material within 15 minutes.

k) When participating in XDM confidential teleconferences, confirm that all participants are authorised to participate.

l) Do not store confidential XDM information on either Internet or Intranet servers.

m) Employees shall not forward information appearing on the Intranet to third parties without going through the appropriate internal channels (such as the XDM Municipal Manager or Communication Division or IT Division).

n) Employees are responsible for ensuring that they are utilising the most up-to-date anti-virus software. Employees must apply updates sent via e-mail as soon as they are received. The ICT unit should be contacted if any update message is unclear or if you are unsure as to how to apply the update.

Section 13 – INTERNAL NETWORKING POLICY

13.1 INTRODUCTION

The XDM's Intranet and internal LAN systems are for the exclusive use of authorised XDM employees and authorised users. Unlike the Internet, information on the Intranet may be disseminated only to authorised persons, and is not accessible except with specific authorisation.

13.2 POLICY STATEMENTS

a) Do not misrepresent yourself (i.e., masquerade) as someone else on the network.

b) Do not monitor network traffic (i.e., use a "sniffer" or similar device).

c) Do not add any network device that creates an external connection (e.g. a bridge, router, gateway, hub, or modem) to your workstation unless authorised to do so by the IT Division.

d) No donated or third party or non-standard equipment may be connected to any network point without the prior approval of the XDM's IT Division.

e) Do not install file sharing or peer-to-peer software unless authorised to do so.

f) If other users are allowed to access or store files on an employee's network connected workstation they must select either user-ID access control or password access control when defining the share options for the workstation disk drives and files –the ICT unit can be contacted for further information.

g) ANONYMOUS FTP, TITP, or other unauthenticated access to program or data files on individual workstations must not be allowed.

h) Before any information is posted to the XDM's Intranet, at least two approvals shall be obtained, from the department manager in charge of the relevant Intranet page and the owner of the information (or creator of the information if the owner has not yet been designated).

i) All content posted to the XDM's Intranet remains the property of the XDM.

j) Employees shall not establish Intranet servers, electronic bulletin boards, local area networks, modem connections to existing internal networks, or other multi-user systems for communicating information without the specific approval of the XDM's IT Division.

Section 14 – EXTERNAL NETWORKING POLICY

14.1 INTRODUCTION

Unlike internal LANs and the Intranet, connections to external public networks and the Internet has the potential to allow any person access to the XDM's systems. For this reason connections to the Internet and other external networks are strictly controlled.

14.2 RISKS

Connecting XDM systems and networks to non-XDM systems and networks, including the Internet, through modems or direct-line attachments, can present a serious risk to the XDM. It is possible to expose the entire XDM network and the systems and data on it, without an individual even knowing that they are doing so. Because of the potential risk, all connections between the XDM and non-XDM systems and networks are strictly controlled, and must be approved by XDM management.

14.3 POLICY STATEMENTS

a) If individuals need to connect to non-XDM systems or networks e.g. the Internet, to a business partner's system,. etc., they must use the approved XDM firewall. Users can check with the ICT unit for further information.

b) Do not dial out or otherwise connect to any non-XDM systems or networks while simultaneously connected to the XDM's internal network. To establish such a connection, first physically and logically disconnect the workstation from the XDM's internal network - contact the ICT unit for further information.

c) If users need to connect to XDM systems and networks from outside XDM premises, they must be registered to use one of the approved remote access services. Check with the ICT unit to determine how to register to use these services.

d) No donated or third party or non-standard equipment may be connected to any network point without the prior approval of the XDM's IT Division.

e) Dial line access to/from an employee's individual workstation is not allowed.

f) Employees connected via TCP/IP must not be simultaneously connected via a modem to the Internet or any other external TCP/IP network without explicit management authorisation and unless the appropriate TCP/IP commands are entered which prevents intruders from using the workstation as a pathway into the internal network. Contact the ICT unit for further information.

g) In-house production information systems, such as a server, shall not be directly connected to the Internet. Instead these systems shall connect with an application server, a database server, or some other intermediate computer that is dedicated to Internet business activity.

h) Other ways to access the Internet, such as dial-up connections with an Internet Service Provider (ISP), are prohibited from XDM owned computers, or any computer connected to any XDM network or system.

i) All web servers accessible via the Internet shall be protected by a router or firewall approved by the XDM's IT Division.

j) The establishment of a direct connection between XDM systems and computers at external organisations (tunnels or virtual private networks) via the Internet or any other public network is prohibited.

k) Employees and users shall not make arrangements for, or actually complete the installation of voice or data lines with any carrier, if they have not first obtained approval from the XDM's IT Division.

l) Information regarding access to the XDM's computer and communication systems, such as dial-up modem phone numbers, is confidential. This information shall not be posted on the Internet, listed in telephone directories, placed on business cards, or otherwise made available to third parties without the permission of the XDM's IT Division.

m) Employees and users shall not leave modems connected to personal computers in auto-answer mode so that they are able to receive in-coming dial-up calls.

Section 15 – REQUEST FOR SERVICE (RFS) POLICY

15.1 INTRODUCTION

A Request for Service (RFS) is a specific service request from ICT that is target date driven. It may also include Moves, Additions or Changes to your PC Hardware, Software and Peripherals, and quotations for the supply of equipment and/or software.

Employees must document all service requests so that changes to the ICT environment can be managed.

If the ICT unit identifies that the call is a Request for Service (RFS) then a form will be given to the requestor to complete. This form will be available electronically on the Intranet.

The form needs to be completed (with the assistance of the necessary technical people if required). This form must then be given to the IT Division who will provide a reference number.

15.2 RISKS

The risks of ordering equipment without a valid RFS and Order Number are:

a) Unplanned and/or unbudgeted expenses

b) Unplanned changes being made to the XDM IT infrastructure which may impact on the availability of services to all users

c) Delays in the ordering of items

d) Fraud

e) Suppliers supplying items in good faith and then not receiving payment, with a resultant negative image of the XDM being created.

15.3 POLICY STATEMENTS

- Employees wishing to purchase or upgrade or change or move or install any IT related equipment or software should in the first instance contact the ICT unit. The ICT unit will determine the type of call and if necessary advise the employee to log an RFS.

- NO ICT equipment or Software may be purchased, upgraded, installed without the RFS procedure being followed.

- NO donated equipment may be utilised in any way without prior approval from the XDM's IT Division.

- NO ICT equipment (including but not limited to PCs, printers, servers, FAX machines) may be moved to a new location or new user/s without following the RFS procedures.

- NO ICT equipment outside of the standard configurations will be supplied against the XDM's ICT budget.

- Unless specific permission is obtained, employees will only ever be allowed to have ONE personal computer device allocated to them e.g. only one PC not a PC and a Laptop. Should an employee believe that they have a business need for more than one device, a full justification is required, authorised by management, which should be forwarded via an RFS to the ICT unit.

- The following instructions apply to the RFS example that is included at the end of this section.

i. ALL fields on the first page MUST be completed. Incomplete forms will not be processed and will lead to unnecessary delays.

ii. RFS Number: This will be allocated by the ICT unit.

iii. Date Created: The date on which the form is completed.

iv. Employee Number: Unique employee number.

v. Department: The name of the Department in which the individual works.

vi. Requestor: Requestor's name.

vii. Physical Address: The address where Requestor works.

viii. Manager: The name of Requestor's manager.

ix. E-Mail Addr: e-mail address of the person requesting the service.

x. Phone: Requestor's telephone number.

xi. Location: Where in the building Requestor is located, e.g., floor, wing, and room number.

xii. Date Approved: This will be completed by Requestor's Manager.

xiii. Signed: Manager's signature.

xiv. RFS Title: What is the request for, e.g., Installation of a new Server.

xv. Is this a feasibility study only? As applicable. A feasibility study would, for example, be an investigation into Costs, etc.

xvi. Related RFS (if applicable): Complete if another RFS has been logged that may be linked to, or impact the RFS which is now being raised.

xvii. Description of Requirement: This must be completed in detail. Explain exactly what is needed, e.g., a Server, to be installed at the Fire Department, etc. It is important that not only the "what" is described, but also the "why".

xviii. Scope of change: In the "Description of Requirement" the actual need was explained. Here the impact of the requirement needs to be detailed in the broader sense, e.g., installing a Server may impact the LAN, etc. This is the requestor's impact analysis.

xix. Relevant date(s) and times: Please remember, that these dates may need to be changed. For example, a large request may also need to be scheduled as a Change that will need to be scheduled in terms of its impact and relation to other Changes.

xx. Software Affected: This may not always be relevant, but if so, please complete as there may be licensing implications, and therefore additional costs.

xxi. **Any other key elements:** If relevant, such as an Order Number. Please note that the more information included the better.

xxii. **Page 2:** The items on this page are self-explanatory.

XHARIEP DISTRICT MUNICIPALITY Request for Service Form

REQUESTOR INFORMATION

RFS Number:	Date created:
Employee Number:	Department:
Requestor:	Physical Address:
Manager:	E- mail Address:
Phone:	Office Number:
Date Approved:	Signature:
Contact Person:	Contact Person Contact Details:

XDM REQUIREMENT INFORMATION

RFS Title:	Is this a feasibility study only?
Related RFS (if applicable):	
Description of Requirement:	
Scope of change:	
Relevant date(s) and times:	
Software Affected:	Any other key elements (e.g., Order Number):

XDM REQUIREMENT INFORMATION
(Continued)

This section to be completed by the person requesting the service, if your RFS is PC / Laptop related

Do you currently have: (answer Yes / No to the following)

e-mail: if Yes, e-mail address:

Windows XP:	Yes	No
Internet:	Yes	No
Pastel:	Yes	No
VIP:	Yes	No
MS Office:	Yes	No
Antivirus:	Yes	No
Other (e.g., MS Project):	Yes	No

Do you currently have a network point?	Yes	No
Do you access the network via a telephone?	Yes	No

How many power sockets do you currently have?	

Please Note: All fields are mandatory: incomplete information will result in the return of this form to the originator

ICTPP16 – NOTEBOOK (LAPTOP) COMPUTERS AND OTHER HANDHELD (e.g. PDA) DEVICES POLICY

16.1 INTRODUCTION

Notebook computers and other handheld computing and electronic diary devices (for purposes of this ICTPP generically referred to as a Notebook) are increasingly being utilised by an ever more mobile workforce. Although Notebook computers are particularly useful to mobile employees, employees who are issued with Notebooks carry extra responsibilities, particularly with regard to data and hardware security.

Employees need to be particularly aware that they are responsible for the physical security of the Notebook as well as any data stored on the Notebook.

16.2 RISKS

Notebook computers by their nature and design are portable and easily damaged, lost or stolen. Apart from the major inconvenience to the employee and the loss of a capital item for the XDM, the loss and potential misuse of XDM information contained on the notebook make it vital that employees issued with notebooks are particularly vigilant.

The sections covering Passwords and Protecting XDM Information in this document are particularly relevant.

16.3 POLICY STATEMENTS

- Employees, who are mobile in terms of job requirements i.e. are expected to travel either nationally or internationally and require computing facilities whilst mobile, may qualify for a Notebook.

- The employee must apply to his Head of Department with a motivation as to why he requires a Notebook. The issuing of notebooks will be strictly controlled because of their cost and vulnerability.

- Once the HOD has approved the application, the RFS procedure should be followed.

- The type of notebook will be dictated by the individual need i.e. dependent on whether it will be utilised for general usage (e-mail, MS Word, Excel). Unless there is a specific identified and motivated need, only standard configurations, will be ordered and supplied. Authorisation of the ICT Division (via the RFS procedure) is required for notebook purchases.

- XDM will then purchase the notebook via the normal Supply Chain Management procedures and provide the employee with the device.

- The individual will be required to sign this entire ICTPP Document (Declaration), which includes, that he/she will exercise care in the safekeeping, transportation of the notebook and ensure that it is maintained and kept serviced at all times. The individual will liaise with the XDM's insurance department to determine insurance policies before removing the notebook from the XDM's premises.

- Should the notebook be lost, the employee will be held fully responsible for the loss, unless it can be determined that the employee was not at fault.

- Employees are responsible for ensuring that adequate backups of data on the notebook are taken at regular intervals (please contact the ICT unit for assistance in this regard).

- Employees are responsible for the confidentiality of the information on the notebook and need to take due care about where the notebook is used and stored.

- Whenever possible, particularly at the employee's usual place of work, the notebook should be secured by a cable type security attachment.

ICTPP17 – STANDARDS POLICY

17.1 INTRODUCTION

Standards are a vital part of being able to maintain and offer a stable and responsive ICT service. Standards reduce the overall cost of ICT by allowing the XDM to take full advantage of bulk purchase agreements.

The following set of standard products that may be utilised by employees. The usage of these products will have the following benefits for XDM:

- Reduce downtime to an absolute minimum.
- Enable support staff to be trained in specific products.
- Enable the support staff to guarantee certain response times to assist XDM employees with problems.
- Enable XDM employees to be effectively trained in the usage of these products.
- Enable XDM employees to work from numerous locations without first having to become familiar with differing products.
- Enable the ICT unit to quickly provide new or additional products.
- Enable XDM management to accurately budget future expenditure.
- Ensure compatibility between products, thus minimising interface requirements and in many cases provide automatic integration capabilities.

The standards applicable at any particular time are available from the ICT Unit.

17.2 POLICY STATEMENTS

- All procurement must follow the RFS procedure outlined in section ICTPP15.
- NO non-standard products will be ordered or installed without the specific authorisation of the ICT Unit (refer to ICTPP17).
- Employees are prohibited from installing non-standard products on any XDM owned ICT equipment (refer to ICTPP17).
- Employees are prohibited from connecting or, allowing the connection of, any non-standard equipment or products to the XDM's communication networks.
- Upon supply, each workstation is configured according to a standard set of settings, including a standard XDM screensaver. NONE of these settings may be changed without documented reference to the ICT Unit.

- Each employee will be allocated 300Mb of space on an AD (Active Directory) Server. This will be for purposes of backing up important Work/XDM information.

ICTPP18 – INSURANCE POLICY

18.1 INTRODUCTION

XDM employees are responsible for the safekeeping and correct usage of the XDM's assets. Should an asset be damaged or lost, the procedures below must be followed, whether or not an insurance claim is to be made, and irrespective as to the reasons why the asset was lost or damaged.

18.2 RISKS

The risks of not following these policies and procedures are:

- An employee may find themselves personally liable for costs associated with the loss.
- The XDM's insurance company may repudiate valid insurance claims.
- Unnecessary delays in the replacement/repair of the asset may take place.
- Fraud and theft may go undetected.

18.3 POLICY STATEMENTS

- The employee must immediately inform their manager, XDM security, and the Insurance Department the moment the loss or damage is apparent.
- In the event of loss or suspected deliberate damage, the employee must inform the SA Police, within 24 hours, and a case number must be obtained.
- The employee must log a Request for Service (refer ICTPP15) with the ICT unit requesting a quotation for the replacement or repair of the equipment.
- ICT will investigate, quote on missing items and remove all in-operable salvageable equipment to storage (to prevent further theft).
- Upon receipt of the quotation the employee should attach the quotation and any other information (e.g. case number) to the relevant completed insurance forms and forward these to the Insurance Department for claim approval.
- Upon approval the Insurance Department will transfer the approved funds into the relevant client's budget.
- Employee to submit a further RFS, with all relevant details, original quotation details, an Order number and Vote number.
- Salvaged inoperable equipment will be stored until released according to instructions either received from, or verified in writing with, the insurance company.

ICTPP19 – EMPLOYEE SEPARATION POLICY

19.1 RISKS

Should the procedure and checklist below not be followed, XDM is exposed to the following major risks:

- Fraud – through the unauthorised usage of XDM systems and assets
- Financial Loss – through the utilisation of assets and facilities that are no longer applicable.
- Information loss – through the unauthorised dissemination of confidential XDM information.

19.2 POLICY AND PROCEDURE STATEMENTS

- Manager contacts HR to initiate the normal XDM separation process.
- HR to complete Part "A" of ICT Checklist.
- ICT unit initiates actions and completes Part B.
- ICT unit returns form to initiating HR party (Fax or E-mail).
- XDM HR signs and attaches completed form to normal exit/contract termination documentation.
- XDM files documentation according to normal XDM HR procedures.

XDM Employee Separation Form – IT Procedures

Part A - to be completed by HR Department

Employee Name	
Employee Number	
Exit Date	
Phone	
Cell Number	
Manager	
Department	
Office Location	

Part B – to be completed by ICT unit

IT Assets

Equipment Type	Asset Number	Serial Number	Date Returned
Desktop			
Laptop			
Printer			
PDA			
Other - specify			

Software

Access to	User ID	Date Cancelled	Comments
E-mail			
Internet			
Financial System			
HR System			
Network (AD)			
Sign Off			
IT Division			
Depart Manager			
HR Manager			

Notes:

Location of Equipment:

Equipment to be transferred to:

ICTPP20 – SOFTWARE USAGE POLICY

20.1 INTRODUCTION

The purpose of this policy is to address software management and usage requirements for all XHARIEP DISTRICT MUNICIPALITY employees and contractors.

20.2 RISKS

The risks of utilising unlicensed and/or non-standard software products are many:

- Increased downtime due to support staff being unfamiliar with the product.
- Complete lack of support.
- Incompatibility between systems and the base Operating System.
- Virus infection.
- Incompatibility between products resulting in translation errors between systems or rework by XDM employees.
- Additional procurement costs.
- Additional installation and maintenance costs.
- Lack of adequate security.
- Severe financial penalties imposed on the XDM by suppliers of the software e.g. Microsoft.
- Severe penalties imposed on individual employees by suppliers.
- Unacceptable media exposure.
- Disruption to services due to the removal or re-installation of products.
- Increased unbudgeted and unnecessary training expenses.
- Reduction in ability and flexibility for job sharing and transitioning.
- Inability to backup or recover information.

20.3 POLICY STATEMENTS

- All software applications developed for use by the XHARIEP DISTRICT MUNICIPALITY by 3rd parties becomes the property of the XDM.
- All software applications developed for use by the XHARIEP DISTRICT MUNICIPALITY by employees becomes the property of the XDM.
- Only appropriately licensed software may be installed on the XDM's equipment.

- Only standard software may be installed on the XDM's equipment.
- Non standard software must be tested and approved by the ICT department prior to installation.
- Employees may not "self install" any software (including but not limited to standard software) without prior ICT approval (this is to ensure that correct versions of standard software are installed).
- Internal Audit and/or IT will periodically audit equipment. Any unauthorised software will be removed immediately.
- Copying and/or distributing software is not allowed;
- Downloading, installing and/or using evaluation, public domain, freeware and shareware is not allowed without prior permission from ICT.
- Any software that is installed (other than centrally controlled standard software) must be appropriately licensed. Employees are required to be able to prove licensing and/or ownership by being in possession of either original purchase order (or valid copy) and/or receipt/packing slip from original vendor and/or documented software license to use and/or original serialised software CD or diskette;
- Software (including all copies if any) purchased by the XDM must be returned to the XDM upon termination of employment or contract (refer ICTPP19 Employee Separation).

ICTPP21 – NETWORK COPIERS POLICY

21.1 INTRODUCTION

The purpose of this policy is to ensure that Network Copiers connected to the XDM's network are connected in a standard, manageable and reliable way. Additionally the responsibilities of the various parties need to be clearly understood to mitigate against unnecessary downtime and cross supplier "finger pointing" in the event of problems being experienced.

21.2 RISKS

The uncontrolled installation of Network Copier devices to the XDM's network carries with it the risk of network failures due to either faulty installation or device incompatibility.

21.3 POLICY STATEMENTS

- Network Copiers will be procured in accordance with the XDM's normal procurement regulations.
- Network Copiers may only be connected to the XDM's network once the normal RFS process has been followed.
- The responsibilities of the various parties are:
    - User of equipment –
        - Ordering of Network Copier.
        - Electrical power.
        - Completion of RFS if network connectivity is required.
        - Negotiation and agreement with the Network Copier vendor on all service, support and maintenance agreements.
        - In the event of problems being experienced with the Network Copier, the vendor of the Network Copier is to be the first direct contact.
    - XDM IT -
        - Approval of RFS.
        - Installation and testing of approved network connectivity point.
        - ICT support staff available to assist Network Copier vendor with software installation on desktop equipment, administration password and server access if required.
        - ICT support staff will **NOT** be required to solve issues relating to Network Copier's hardware or software.
        - Repair of faulty network point.
    - Network Copier Vendor-
        - Supply of hardware and software.

- Installation of Network Copier.
- Testing of Network Copier hardware and software to ensure compatibility with the XDM's environment.
- Installation of desktop Network Copier software.
- Problem rectification should problems arise on the desktop after the Network Copier software is installed.
- Problem solving relating to either Network Copier hardware or software.
- Full ongoing support and maintenance on both Network Hardware and Software.
- Initial problem determination and rectification.