



the dr&pw

Department:
Roads and Public Works
NORTHERN CAPE PROVINCE
REPUBLIC OF SOUTH AFRICA

**DEPARTMENTAL POLICY ON
INFORMATION AND COMMUNICATION
TECHNOLOGY: STANDARDS AND
GUIDELINES**

FEBRUARY 2019

Version 2

TABLE OF CONTENTS

| Contents | Page |
|---|-------------|
| 1. DEFINITIONS | 7 |
| PART ONE | 10 |
| 1. EXECUTIVE SUMMARY | 10 |
| 1.1 The Purpose of the ICT Policy, Standards and Guidelines | 10 |
| 1.2 Objectives of the ICT Policy, Standards and Guidelines..... | 10 |
| 2.Regulatory Framework..... | 11 |
| 3.Code of Ethics | 11 |
| 3.1General Imperatives..... | 11 |
| PART TWO | 12 |
| 1.IT SECURITY | 12 |
| 1.1Objective | 12 |
| 1.2 Equipment Security (Physical) | 12 |
| 1.2.1 Issuing and Returning of Equipment..... | 12 |
| 1.2.2 Removal of Equipment from the Premises and during Travelling..... | 13 |
| 1.2.3 Security of Equipment within the Department’s Buildings..... | 14 |
| 1.2.4 Server Room and Network Rooms..... | 14 |
| 1.3 Password Security..... | 15 |
| 1.3.1 General Password Construction Guidelines | 15 |
| 1.3.2 Password Protection Standards | 16 |
| 1.3.3 Use of Passwords and Pass Phrases for Remote Access Users | 17 |
| 1.4 Information Security | 17 |
| 1.4.1 Ownership and Usage..... | 17 |
| 1.4.2 Administration | 17 |
| 1.4.3 Integrity and Validations..... | 18 |
| 1.4.4 Archiving..... | 18 |
| 1.4.5 Anti-virus Protection and Updates..... | 18 |
| 2. SYSTEMS AND NETWORK | 18 |
| 2.1 Objective | 18 |
| 2.2 Security..... | 19 |
| 2.3 Hosting | 19 |

| | |
|--|----|
| 2.4 Remote Dial-Up Access and Mobile Computing | 19 |
| 2.5 Remote Printing | 20 |
| 3. RECORDS MANAGEMENT | 21 |
| 3.1 Objective | 21 |
| 4. SOFTWARE | 22 |
| 4.1 Objective | 22 |
| 4.2 Procurement..... | 22 |
| 4.3 Storage and Distribution | 22 |
| 4.4 Licensing and Installing of Software | 23 |
| 4.5 Use of Illegal and Unauthorized Software | 23 |
| 5. SLA's AND MAINTENANCE AGREEMENTS..... | 24 |
| 5.1 Objective | 24 |
| 5.2 SLA's | 24 |
| 6. BACKUP AND DISASTER RECOVERY | 25 |
| 6.1 Objective | 25 |
| 6.2 Data and Back-ups..... | 25 |
| 7. VISITS BY THE IT UNIT..... | 25 |
| 7.1 Objective | 25 |
| 7.2 IT Visits..... | 25 |
| 7.3 Visitors to the IT Section Work Area..... | 28 |
| 8. AUTHORIZATION AND ACCESS | 26 |
| 8.1 Objective | 26 |
| 8.2 User Account Management | 26 |
| 8.2.1 Account Allocation..... | 26 |
| 8.2.2 Account Holder's Obligations | 27 |
| 8.3 Operating Systems and Databases..... | 27 |
| 8.4 Business Applications | 27 |
| 9. ELECTRONIC COMMUNICATION..... | 28 |
| 9.1 Objective | 28 |
| 9.2 Building DRPW's Image | 28 |
| 9.3 Personal Use..... | 28 |
| 9.4 Addressing..... | 28 |
| 9.5 Protection of email..... | 29 |

| | |
|--|----|
| 9.6 User Accountability..... | 29 |
| 9.7 Prohibited use of email | 29 |
| 9.7.1 Contravening the Laws of the Republic of South Africa for private use..... | 29 |
| 9.7.2 Disclosing Confidential Information..... | 30 |
| 9.7.3 Abusing Bandwidth | 30 |
| 9.7.4 Spreading Malicious Code..... | 30 |
| 9.7.5 Personal Gain | 30 |
| 9.7.6 Access rights of ex-users..... | 30 |
| 9.7.7 Disciplinary Measures | 31 |
| 9.7.8 Prohibited File Attachments..... | 31 |
| 10. INTERNET USAGE..... | 31 |
| 10.1 Objective | 31 |
| 10.2 Internet / Intranet Access | 31 |
| 10.3 Prohibited use of the Internet / Intranet in DRPW | 31 |
| 10.3.1 Contravening the Laws of the Republic of South Africa | 32 |
| 10.3.2 Conducting Internet practices that could lead to litigation against the DRPW | 32 |
| 10.3.3 Disclosing Confidential Information..... | 32 |
| 10.3.4 Abusing Bandwidth | 32 |
| 10.3.5 Violating DRPW's Values | 33 |
| 10.3.6 Spreading Malicious Code (Viruses)..... | 33 |
| 10.3.7 Compromising Network Security | 33 |
| 10.3.8 Personal Gain..... | 33 |
| 11. IT PROCUREMENT | 33 |
| 11.1 Objective | 33 |
| 11.2 Procurement Requests..... | 33 |
| 11.2.1 Submission..... | 34 |
| 11.2.2 Approval and SLA's | 34 |
| 12. HARDWARE STANDARDS..... | 34 |
| 12.1 Objective | 34 |
| 12.2 Hardware Procurement | 34 |
| 12.3 Hardware Classification..... | 35 |
| 12.4 Allocation | 36 |

| | |
|--|----|
| 12.5 Maintenance..... | 36 |
| 12.6 Depreciation | 36 |
| 12.7 End User Equipment Specifications..... | 36 |
| 12.8 Peripheral Hardware Distribution..... | 36 |
| 13. ASSET MANAGEMENT | 37 |
| 13.1 Objective | 37 |
| 13.2 Acquisition of Tools..... | 37 |
| 13.3 Inventory | 37 |
| 13.4 Hardware Maintenance | 37 |
| 13.5 Hardware Retirement..... | 38 |
| 13.6 Licenses Contracts..... | 38 |
| 13.7 Asset Tracking | 38 |
| 13.8 Best Practices | 38 |
| 14. IT SUPPORT AND MAINTENANCE..... | 38 |
| 14.1 Objective | 38 |
| 14.2 Operations Manuals..... | 39 |
| 14.3 Helpdesk..... | 39 |
| 14.4 Fault Reporting Guidelines | 39 |
| 14.5 Basic Fault Finding Guidelines..... | 40 |
| 14.6 Procedure Manual..... | 40 |
| 14.7 Remote Management & Assistance..... | 41 |
| 15. IT PROJECTS..... | 41 |
| 15.1 Objective | 41 |
| 15.2 Project Planning..... | 41 |
| 15.2.1 Business Case..... | 41 |
| 15.2.2 Project Start Up..... | 41 |
| 15.2.3 Project Scope | 41 |
| 15.2.4 Project Organization and Reporting..... | 42 |
| 15.2.5 Project Schedule | 42 |
| 16. SOFTWARE AND SYSTEMS DEVELOPMENT | 42 |
| 16.1 Objective | 42 |
| 16.2 User Requirement Specification | 42 |
| 16.3 Designing of Specifications..... | 42 |

| | |
|--|----|
| 16.4 Systems Development..... | 44 |
| 16.5 Systems Manuals | 44 |
| PART THREE | 45 |
| 1. PROPOSED SOFTWARE AND HARDWARE STANDARDS..... | 45 |
| 1.1 Basic Software Standards..... | 45 |
| 1.2 Computer Hardware Standards..... | 45 |
| 1.3 Laptop Guidelines..... | 45 |
| PART FOUR | 45 |
| 1. MONITORING AND EVALUATION | 45 |
| 2. POLICY REVIEW..... | 46 |
| ANNEXURE A | 46 |
| PROCEDURE GUIDELINES FOR NETWORK CONTROLLERS | 46 |
| POLICY APPROVAL | 51 |

1. DEFINITIONS

| | |
|----------------|---|
| Acrobat Reader | Acrobat Reader forms part of the Adobe Acrobat family of application software and web services developed by Adobe Systems to view, create, manipulate, print and manage files in Portable Document Format (PDF). |
| Access Type | The authorized access to business systems may be one restricting the end-user to only enquire on the system or to update and enquire on the system. |
| BAS | Basic Accounting System |
| CD | Compact Disk. |
| CFO | Chief Financial Officer. |
| Department | Department of Roads & Public Works, Northern Cape Province (DRPW). |
| Disaster | A disaster is an event that makes the continuation of normal business functions impossible. |
| DMZ | Demilitarization Zone. |
| DPSA | Department of Public Service and Administration. |
| Email | Electronic Mail. |
| Email Spam | Email spam, also known as junk email or unsolicited bulk email (UBE), is a subset of electronic spam involving nearly identical messages sent to numerous recipients by email. Clicking on links in spam email may send users to phishing web sites or sites that are hosting malware. Spam email may also include malware as scripts or other executable file attachments. |
| Employee | An individual who has a legally binding employment contract with the DRPW. |
| End-User | An employee, contractor, consultant, service provider and/or agent, who has access to and uses the Department's systems. |
| Environment | A server or an area within a server designed for and assigned to a specified function or functions; e.g. testing, development, etc. |

8

DEPARTMENT OF ROADS AND PUBLIC WORKS
DEPARTMENTAL POLICY ON INFORMATION AND COMMUNICATION
TECHNOLOGY: STANDARDS AND GUIDELINES

| | |
|-------------------|--|
| ESET | ESET is an IT security company headquartered in Bratislava, Slovakia. |
| External End-User | Anyone who is not an employee of DRPW e.g., members of the public who may want to use DRPW systems. |
| GITO | Government Information Technology Officer. |
| GCCN | Government Common Core Network. |
| Hacker | In the computer security context, a hacker is someone who seeks and exploits weaknesses in a computer system or computer network. |
| HCM | Human Capital Management. |
| HOD | Head of Department. |
| Host | Device on the Department's network to which external devices connect. |
| ICT | Information and Communication Technology. |
| IP | Internet Protocol. |
| ISP | Internet Service Provider. |
| IT | Information Technology. |
| LAN | Local Area Network. |
| LOGIS | Logistical Information System. |
| MAC Address | A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. |
| Mb | Megabit. |
| MB | Megabyte. |
| MIOS | Minimum Interoperability Standards |
| MIS | Management Information System. |
| MISS | Minimum Information Security Standards. |
| MS | Microsoft. |
| MSDOS | Microsoft Disk Operating System. |
| Node | An electronic device on the Department's network with an IP address. |
| Novell | Novell, Inc. is an American multinational software and services company headquartered in Provo, Utah. Novell |

9

DEPARTMENT OF ROADS AND PUBLIC WORKS
DEPARTMENTAL POLICY ON INFORMATION AND COMMUNICATION
TECHNOLOGY: STANDARDS AND GUIDELINES

| | |
|------------------------------|--|
| | technology contributed to the emergence of local area networks (LANs), which displaced the dominant mainframe computing model and changed computing worldwide. |
| NWC | Network Controller. |
| PALS | Public Access Learning System. |
| PC | Personal Computer. |
| PERSAL | Personnel and Salary Information System. |
| PPPFA | Preferential Procurement Policy Framework Act, Act No. 5 of 2000. |
| RAM | Random Access Memory. |
| SDLC | System Development Life Cycle. |
| Senior End User | An employee whose position falls within the brackets of Senior Manager to Head of Department (HOD). |
| SLA | Service Level Agreement. |
| SMTP | Simple Mail Transfer Protocol. |
| SNMP | Simple Network Management Protocol. |
| Spiceworks | Spiceworks is a software development company headquartered in Austin, Texas. It was formed to provide a Facebook-like community integrated with a free ad-supported IT systems management, inventory, and help desk software application designed for network administrators working in small- to mid-sized businesses and managing up to 1,000 network devices. |
| TACACS | Terminal Access Controller Access-Control System. |
| User Account Lapse | A state in which a user account cannot be accessed without an account administrator's intervention. |
| User Account Close / Disable | A state in which a user account is no longer connected to any applications system. This state renders the account incapable of being used to access the Internet, intranet, email, office applications as well as business applications. |
| VNC | Virtual Network Computing. |
| WAN | Wide Area Network. |

| | |
|------|--|
| QNAP | QNAP Systems, Inc.,(headquartered in Taipei, Taiwan), as its brand promise "Quality Network Appliance Provider", delivers Network Attached Storage (NAS) and Network Video Recorder (NVR) solutions. |
|------|--|

PART ONE

1. EXECUTIVE SUMMARY

1.1 The Purpose of the ICT Policy, Standards and Guidelines

- The effective and efficient management of information, communication systems and knowledge has become a critical success factor in every organization. Information and communication technology (ICT) provides the resources (hardware, applications and communication systems) necessary for proper information and knowledge management.

- The ICT Policy, Standards and Guidelines are developed to ensure the following:
 - ✓ Compliance with legislation governing the use of ICT in the Department.
 - ✓ Effective and efficient management of ICT in the Department.
 - ✓ Acceptable and reasonable use of ICT.
 - ✓ Compliance with standards for IT security and inter-operability.

1.2 Objectives of the ICT Policy, Standards and Guidelines

- The overall objective of the DRPW ICT is to establish a framework for:
 - ✓ Regulating and governing the development of information and communication technology and systems.
 - ✓ Management of the information and communication technology architecture.
 - ✓ Monitoring and regulating the use of information and communication technology and systems.
 - ✓ Regulating the acquisition and management of information and technology resources.

- The specific objectives of the DRPW ICT policy are to:
 - ✓ Support the core business of the Department.
 - ✓ Integrate the use of information in the Department's business processes.

- ✓ Enable the Department to develop new or enhanced services or products.
- ✓ Provide Senior Management with timely and relevant management information.
- ✓ Facilitate and enhance communication with the Department's internal and external clients.
- ✓ Improve and enhance productivity, efficiency and cost-efficiency within the Department.
- ✓ Improve direct and indirect service delivery.
- ✓ Provide access to the Department's services.

2. REGULATORY FRAMEWORK

- The Public Service Regulations, 2001, as amended in 2002: Chapter 1, Part iii, Regulation E, and Chapter 5, Part I, Part ii, Part iii.
- The GITO Council, as approved by the DPSA: Information Technology Planning Framework, 2002.
- DPSA: Handbook on MISS, 2002: Chapter 6, Chapter 7, Chapter 8.
- DPSA: Handbook on MIOS, 2002.
- The State Information Technology Act, Act No. 88 of 1998, (the "SITA Act").
- The Preferential Procurement Policy Framework Act, Act No 5 of 2000, (the "PPPFA") and the Preferential Procurement Policy Regulations.
- The Copyright Act, Act No. 98 of 1978, as amended up to Copyright Amendment Act No. 9 of 2002.
- The departmental Supply Chain Management Policy.
- The departmental Asset Management Policy.

3. CODE OF ETHICS

3.1 General Imperatives

- **Individual accountability:**
All officials shall be responsible and accountable for adherence to this policy and to take reasonable steps to safeguard resources, assets and information.
- **Confidentiality:**
All officials shall ensure that no actions are taken which could degrade or compromise the required level of accuracy, completeness, dependability and confidentiality of resources,

information and services.

- **Integrity:**
All officials shall ensure that no actions are taken that could degrade or compromise the requirements and guidelines of this policy in a manner that may have detrimental and negative implications on the operational and service delivery environment.

- **Availability:**
All officials shall ensure that no actions are taken that could degrade or compromise the required level of responsiveness of systems, software and programs that are used to support operational or managerial requirements.

- **Controlled access:**
All officials shall be granted access to resources, information and assets for which appropriate access authorization has been established and approved. Such an official shall be granted access to those resources necessary to perform his/her assigned tasks. Controlled access will be achieved via physical and procedural means.

PART TWO

1. IT SECURITY

1.1 Objective

- The purpose of this section of the policy is to put in place guidelines to be followed by the End-Users of DRPW computer systems. It is intended to guide security conscious behavior to End-Users utilizing computers and other IT related equipment. It also covers security measures relating to access to the network and server rooms.

1.2 Equipment Security (Physical)

1.2.1 Issuing and Returning of Equipment

- Prior to issue or installation, which ever applicable, the IT Section in conjunction with the departmental Asset Management unit shall ensure the following:
 - ✓ All assets are tagged.
 - ✓ The equipment is in working order.
 - ✓ All components are listed in an asset register.
 - ✓ All components that are not in proper working order are listed in an asset register.

- In the case of a laptop, digital projector, digital camera, or any other removable equipment, the following minimum details must be recorded:
 - ✓ Serial Number.
 - ✓ Manufacturer name.
 - ✓ Issued to.
 - ✓ Issued by.
 - ✓ Date of issue.
 - ✓ Date of return.
 - ✓ Accompanying components.
 - ✓ Condition of equipment.

- The equipment is to be returned to the DRPW in the condition in which it was recorded into the register.
- All employees that are issued equipment will sign and acknowledge receipt for the equipment.
- *The End-User issued with such equipment is liable for any damage to the equipment that may occur.*
- Any damaged equipment that is identified by the End-User must be reported with immediate effect to the departmental IT Helpdesk to ensure a timely response by the IT Technical support team.

1.2.2 Removal of Equipment from the Premises and During Travelling

- Entry into or Exit from the Department's offices with equipment such as laptops, digital projectors, not excluding others not listed shall be reported to the Unit Manager and shall be monitored by the security personnel at all entrances to the Department.
- A security clearance form must be recommended by the employee's immediate supervisor and approved by the Security Manager before any IT equipment can be removed from the premises.
- The employee's security clearance form must reflect the serial number of the Laptop, digital camera, and digital projector not excluding those not listed.
- The security personnel shall check that the equipment carried out is indeed the equipment issued to the employee.
- All employees must ensure that laptops and other equipment, excluding departmental cellular phones, are placed in the trunk/boot area of the vehicle in

which they travel for security purposes.

- With regard to employees that drive a vehicle without a boot area, the equipment must be placed in a secure area of the vehicle where it is not visible to the eyes of passersby.
- Employees utilizing public transport shall arrange for secure transportation of the equipment from the Department's offices to their place of residence.
- The employee is responsible for the safekeeping of all government equipment temporarily stored at his/her residence.

1.2.3 Security of Equipment within the Department's Buildings

- Employees are to ensure that offices containing IT Equipment is locked when the employee responsible does not occupy it.
- Negligence regarding equipment security whether on or off site which ever applicable is not permissible.
- The employee will be held responsible for theft or loss of equipment due to negligence on his/her behalf.

1.2.4 Server Room and Network Rooms

- Entry into the main server room and network rooms must be highly restricted and monitored.
- Only authorized IT personnel shall have access to the server and network rooms.
- All network equipment at end-users must be physically secured in network cabinets that are well mounted and locked inside a secured network or server room.
- In the event of an outsourced technician being requested to assist with a problem in the server and network rooms, a departmental IT staff member or the Security Manager shall accompany the technician.
- All other personnel must have permission before being allowed access to such areas. An up to date access register must be kept at all times.
- Biometrics must be installed were possible, or the server room must have a security door.
- The Managers of the offsite or District must assign a reliable person to keep the keys of the server room.

**DEPARTMENTAL POLICY ON INFORMATION AND COMMUNICATION
TECHNOLOGY: STANDARDS AND GUIDELINES**

1.3 Password Security

- Passwords must be kept secured and no user accounts shall be shared. Authorized users are responsible for the security of their passwords and user accounts.
- System level passwords should be changed quarterly; user level passwords should be changed every six months.
- All servers, laptops and workstations should be secured with a password protected screensaver. Passwords must not be inserted into email messages or other forms of electronic communication. All user-level and system-level passwords must conform to the guidelines described below.

1.3.1 General Password Construction Guidelines

- Passwords are used for various purposes at DRPW. Some of the more common uses include: user level accounts, email accounts and screen saver protection. Since very few systems have support for one-time passwords, users should be aware of how to select strong passwords.
- Poor, Weak Passwords have the Following Characteristics:
 - ✓ The password contains less than eight characters.
 - ✓ The password is a word found in a dictionary (English foreign).
 - ✓ The password is a common usage word such as:
 1. Names of family, pets, friends, co-workers, fantasy characters, etc. - Computer terms and names, commands, sites, companies, hardware, software.
 2. The words "Roads, Public Works", "Kimberley" or any derivation based on your physical location.
 3. Birthdays and other personal information such as addresses and phone numbers.
 4. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 5. Any of the above spelled backwards.
 6. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).
- Strong Passwords have the Following Characteristics:
 1. Contain both upper and lower case characters (e.g., a-z, A-Z).
 2. Have digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&*()_+|=\'{}[]:~;<>?,./).

3. Are at least eight alphanumeric characters long.
 4. Is not a word in any language, slang, dialect, jargon, etc.
 5. Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered.
 - One way to do this is create a password based on a song title, affirmation, or other phrase.
 - For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

1.3.2 Password Protection Standards

- Do not use the same password for official accounts as for other non-official access (e.g., personal ISP account, etc.). Where possible, don't use the same password for various system access needs. For example, select one password for the Transversal Access systems such as BAS, PERSAL, LOGIS and a separate password for Novell GroupWise email access.
- Also, select a separate password to be used for any other accounts. Do not share official passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information.
- Here is a List of "Don'ts":
 - ✓ Don't reveal a password over the phone to ANYONE.
 - ✓ Don't reveal a password in an email message.
 - ✓ Don't talk about a password in front of others.
 - ✓ Don't hint at the format of a password (e.g., "my family name").
 - ✓ Don't reveal a password on questionnaires or security forms.
 - ✓ Don't share a password with family members.
 - ✓ Don't reveal a password to co-workers while on vacation.
 - ✓ If someone demands a password, refer him or her to this document or have them call the Security Manager.

- ✓ Do not use the "Remember Password" feature of applications (e.g., Outlook, Web Browsers Outlook Express). Again, do not write passwords down and store them anywhere in your office.
- ✓ Do not store passwords in a file on ANY computer system (including Laptops or similar devices) without encryption.
- ✓ Change passwords, at least, once every six months. The recommended change interval is every four months.
- ✓ If an account or password is suspected to have been compromised, report the incident to your IT Section and change all passwords.

1.3.3 Use of Passwords and Pass phrases for Remote Access Users

- Access to the Department's Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong pass phrase.

1.4 Information Security

1.4.1 Ownership & Usage

- Data on departmental equipment remains the property of DRPW. Thus the data must be stored on a secure network within the Department.
- All servers must be located behind a secure firewall, which will prevent hackers or unauthorized people access to the network and its data.
- All users that are granted access to the Department's systems must sign confidentiality to information form, with the Security Manager.
- All equipment is to be utilized for official purposes only.

1.4.2 Administration

- Only permanent IT Staff should have security permission to access the data directly on the database.
- Changes made to the files by the administrator must be documented as they are being made.
- It is the sole responsibility of the IT Staff to ensure that no else can directly, without use of business applications, edit the data on the database.

1.4.3 Integrity and Validations

- Integrity checks must be put in place in order to ensure completeness and accuracy of the data as it is captured into the system.
- Certain fields must be mandatory and validated against existing data to eliminate duplication.

1.4.4 Archiving

- The data must be archived on reliable media.
- The data must be copied every end of the month and retained permanently.
- Depending on the type of media it is stored on, the data might have to be recopied on newer media when the current media reaches the end of its life span.
- Inactive data should be removed from the active operational database and archived.

1.4.5 Anti- Virus Protection and Updates

- Only ESET IT Security Software (anti-virus) is to be installed on all machines. Each machine is to be configured as follows:
 - ✓ The machine must link to the correct parent server.
 - ✓ Real-time protection must be configured to perform the following actions when a virus is detected.

Action 1: Clean virus from file.

Action 2: Delete infected file.

- Virus definitions on all parent servers must update automatically.

2. SYSTEMS AND NETWORK

2.1 Objective

- This section of the policy focuses on the management of the network and that of components that constitute the network and gives guidelines for network management.

2.2. Security

- To manage the network and ensure that it operates optimally, security needs to be in place to prevent unauthorized access to the Department's network.
- Breach of security results in traffic in excess of the normal user generated traffic.
- To achieve basic network security, the following hardware configuration must be set up where applicable:
 - ✓ Telnet access to the router must be locked down.
 - ✓ SNMP access to the router must be locked down.
 - ✓ All unneeded services on the router shall be turned off.
 - ✓ Different log in levels must be enforced.
 - ✓ Generate activity logs.
 - ✓ Block all unused ports on the switches with TACACS.

2.3. Hosting

- Hosts on a network are the most targeted as they allow outside users access to the network.
- It is therefore difficult to establish whether users accessing the host are authentic or not.
- The host shall be placed in a DMZ where the outside users are unable to see the corporate network.

2.4 Remote Dial-Up Access and Mobile Computing (Wireless)

- Only Authorized personnel who require dial-up access via the GCCN network or mobile computing via approved resources and services as part of their normal duties are permitted such access.
- All dial-up or mobile users are expected and required to act responsibly and apply caution when using access codes, passwords and telephone numbers.
- Others may not use access to such facilities granted to an individual, particularly by external persons.
- Where possible, dial-up or mobile users are encouraged to work offline and utilize the dial-up access facility only when a network connection is required.
- The intention of this policy is ensure that dial-up or mobile users do not use such facilities for access to information systems and networks in a manner which may cause damage to or cause malfunction of systems, networks and information, or

may compromise its security processes, policies, procedures and standards.

- Dial-up or mobile users are to ensure that they do not tamper with networks or equipment provided which could be used to deliberately circumvent security measures of systems and networks being accessed.
- The security of dial-up or mobile equipment at alternative work-sites or at home is just as important as at Head Office or any other building of the Department. Therefore at alternative sites and at home, all reasonable precautions must be taken to protect hardware, software and information from loss, theft, damage and misuse.
- Being a dial-up or mobile user is a privilege, not a right, and as such this privilege may be revoked where the user does not abide by policies and standards of the Province or the DRPW.
- Dial-up users must terminate their connection as soon as they have finished using it or in the event of the connection being idle for more than 30 minutes.
- Approval for dial-up or mobile access must be channeled to the IT Manager for approval.
- Portable computer equipment containing confidential information or which is equipped with network connectivity must not be left unattended at any time and must be secured.
- 2.5 IP Addressing
- Each device on the network shall be assigned a unique numeric IP identifier to designate its location on the network.
- The following devices on the network require an IP Address:
 - router;
 - ✓ switches;
 - ✓ servers;
 - ✓ all workstations;
 - ✓ special purpose workstations, eg:
 - PERSAL, BAS, LOGIS, PALS;
 - ✓ network printers.

2.5 Remote Printing

- Printers must not be left unattended when confidential information is being printed or is about to be printed.

3. RECORDS MANAGEMENT

3.1 Objective

- Electronic or E-records means records generated electronically and stored by means of computer technology.
- The Department shall have back-ups and off-site storage pertaining to electronic records.
- All electronic records shall only be disposed of with clear guidelines and written authorization from the National/Provincial Archivist.
- All recorded information that is created or received by the Department in the execution of its functions (including electronic records, eg. email) are public records.
- No correspondence, whether paper-based or electronic/digital, shall leave the DRPW without an approved reference number. This specifically includes outgoing emails.
- The following phrase is to be attached prominently to ALL emails sent to other governmental bodies:
If the content of this message relates to the official business of your office, please ensure that it is filed - either in hardcopy on the paper-based file plan or electronically if your office has an Archives-approved electronic Records Management System implemented.
- Until such time as the DRPW has an Archives-approved electronic Records Management system in place ALL incoming and outgoing email messages shall be printed out and filed on the appropriate file in the Registry.
- This above directive from the Provincial Archives is to be monitored by the Records Manager, and random, but regular checks of the hard-drives of individual officials are to be made to ensure compliance with this directive.
- ALL other electronic records (including Websites and electronic Management Information Systems) are to be managed as follows:
 - ✓ The storage medium of records must conform to archival standards and backups that do not overwrite previous versions are to be made monthly. Such backups are to be stored as follows:
 - Working copies - Dedicated Servers – QNAP.
 - Security copies - Removable Drive – Fireproof Safe.

- Master copies - Removable Drive - Fireproof Safe (off-site storage – QNAP Synchronization).
- ✓ Any database/information system maintained/developed by the DRPW is to be backed up to File Servers and monthly to removable drives.
- ✓ Whenever a statistical or other report is drawn from a Management Information System, such report is to be sent to the Registry for filing on the appropriate report file.

4. SOFTWARE

4.1 Objective

- The objective of this section of the policy on Software is to give guidelines on how to procure, store and handle software. It also covers the issue of software downloads from the internet.

4.2 Procurement

- All software must be procured via the procurement policies stated in this document. Software, bought or developed, should never become the intellectual property or copyright of any member of staff or another company.
- This is to ensure that there is no loss of strategic information to competitive companies or agencies.
- It is also to ensure that no employee or contract company can, after development of a system, sell the intellectual components to a third party, a competitor or obtain personal gain to detriment the Department.

4.3 Storage and Distribution

- All software must be kept in a central repository where only two IT personnel are permitted to access it.
- A register of the software must be kept and updated when new software is procured.
- The register must reflect the name of the software, number of CD's that it comprises, number of licenses and the vendor who supplied it.

- An audit of all the software must be conducted once every quarter and the register updated accordingly.
- The register must be kept in a secure place designed by the IT Manager.
- Systems and applications software may only be distributed by the IT Section and no software may be installed or run on any departmental equipment or network without the knowledge and consent of the IT Manager.

4.4 Licensing and Installing of Software

- The unauthorized use of software could be unlawful and also a way of spreading computer viruses.
- Unauthorized software is software that may be legal but has not been authorized for use in the Department.
- Thus permission has to be obtained for the use of privately owned software on personal computers.
- All software used must be licensed.
- No software may be taken off the premises unless permission is granted to perform official duties.
- No user is permitted to download any software from the Internet.
- No user is permitted to bring software from home or any other location and install it on a departmental computer.
- The installation and configuration of a personal computer operating system are the responsibility of the IT Section.
- These officials are responsible for configuring the personal computer with approved software for applicable operating systems.
- The downloading of software from the Internet is strictly prohibited as this could create leeway for viruses to enter the network and also deteriorate the network performance.

4.5 Use of Illegal and Unauthorized Software

- Illegal software is any software which is being used unlawfully or which infringes on any copyright laws.
- It is a criminal offence to use any form of pirate software, as this is a direct infringement of the copyright law.

- The Copyright Amendment Act, 1992 (Act 125 of 1992), which amends the Copyright Law of 1978, was published in the Government Gazette No. 14129 on July 1992.
- It makes provision for far wider protection of the copyright of computer software. The Act provides for very strict penalties for the illegal copying of software and the use or possession thereof.
- Audits of PC's and all other related software will be undertaken on regular basis and without notice.
- Any illegal or unauthorized software found would be removed from the personal computers concerned and disciplinary action may be taken against those responsible.
- All staff members are to ensure that the stipulations of the Copyright Act, 1978, as amended, are adhered to.
- The illegal copying of software discs is strictly prohibited.

5. SLA's AND MAINTENANCE AGREEMENTS

5.1 Objective

- The objective of this section is to highlight the relevant ICT SLA's that the Department needs to enter into.

5.2 SLA's

- The following service level agreements are to be concluded annually with SITA:
 - ✓ SITA GCCN Services.
 - ✓ Transversal Systems Support (PERSAL, BAS, PALS).
- The Department should also enter into a SLA with the Provincial IT Department regarding the following:
 - ✓ Server Maintenance and upgrades (Novell).
 - ✓ WAN Support and administration.

6. BACK-UP AND DISASTER RECOVERY

6.1 Objective

- In this section, the steps that must be taken in order to allow for business continuity in the event of a disaster occurring at the Department, are discussed.

6.2 Data Back-ups

- Information resources must be protected from loss or damage and users are responsible for backing up information on their machines, but the IT Section will provide assistance.
- The IT Section in conjunction with departmental IT steering committee is responsible for identifying a procedure for backing up all information resources.
- All sensitive, confidential, critical and valuable information resides on the computer systems and networks must be backed up regularly.
- QNAP NetBak Replicator will be used to backup end user departmental data to the file Servers.
- The DRPW will utilize QNAP NAS Servers for central storage of end user work related files, this will be done by mapping a personal folder to each end user.

7. VISITS BY THE IT UNIT

7.1 Objective

- This section of the policy seeks to ensure that all remote sites are functional and adheres to the standards and procedures set out in this document. It also deals with the monitoring of the deterioration of all equipment.

7.2 IT Visits

- IT visits will be conducted on a regular basis to ensure that optimal functionality of all IT equipment is obtained.
- Should any irregularities of the use of IT equipment be suspected or reported an inspection visit will be conducted to investigate the matter without formal notice.
- The IT Manager will conduct Site inspections of all sites at least once a year.
- IT Technicians will visit Sites for end user support at least every second month or when there is an urgent need.

- When a routine IT visit is performed the following will take place:
 - ✓ The functionality of equipment will be tested.
 - ✓ The condition of the equipment will be evaluated.
 - ✓ All workstations will be screened for illegal and unauthorized software.
 - ✓ Hardware and software will be screened for misuse.
 - ✓ The inventory will be verified or updated if deemed necessary.
 - ✓ The Antivirus software will be checked if definitions are up to date.

7.3 Visitors to the IT Section Work Area

- Members of the public are not allowed to enter the IT Section work area. A departmental IT staff member shall at all times accompany visitors, visiting the IT Section.
- All equipment that must be brought onto the Department's premises for maintenance and/or repairs must be recorded and cleared at security before being brought onto the premises.
- Officials are not to accept any equipment from persons if the said procedure was not adhered to.

8. AUTHORIZATION AND ACCESS

8.1 Objective

- The Department should have a process of allocating user accounts in place. This is to protect centralized information and to provide ways and means by which end-users can also protect their data through the use of Passwords.

8.2 User Account Management

8.2.1 Account Allocation

- In the case when a new user account has to be created, the initial and surname of the user has to be relayed to the IT section at least one month in advance of the starting date of the user.
- The IT Manager must receive a request for the user account before an account can be created.
- The request should either be a physical one or in electronic format.

- No account shall be allocated before the approved request form is received.

8.2.2 Account Holder's Obligations

- Accounts shall be used for official business only. The use of accounts for private commercial business is not permissible.

8.3 Operating Systems and Databases

- Access to operating systems and databases shall be granted only to the IT support staff, Network Administrators, Database Administrators and Systems Software Programming staff.

8.4 Business Applications

- All users shall complete a request for access form in order to be granted access to business applications and transversal systems.
- The managers in all units shall determine which employees are granted access to business applications.
- The user has to complete an application form in order to be granted access to any business applications.
- The System Controller of that particular system will process the registration of user access.
- A database must be kept, indicating user access administration and changes.
- They shall decide upon the level and type of access each employee shall obtain.
- In these decisions the manager shall be guided by the roles and responsibilities defined for each employee.
- Development staff shall be granted access to the development environment.
- IT personnel that are not directly involved with applications software development or maintenance shall not be granted access to the development environment.
- A systems controller should be identified for each system used on the network.
- An updated list of all the system controllers must be forwarded to the IT section especially when changes are made to the existing list.
- Registration of new users onto a system must be done via the system controllers.

9. ELECTRONIC COMMUNICATION

9.1 Objective

- This section provides guidance on the usage of email as a means of communication.

9.2 Building the DRPW's image

- When using email for official communication, users should be aware of the characteristics of standard and secure email (see below) and should therefore not put the Department or themselves at risk.
- The following IT policy statement must be adhered to: *"Information and data is classified as confidential to DRPW."*

9.3 Personal Use

- Use of email facilities for personal use is prohibited.
- When offering information to mailing lists, users should ensure that the recipient is trustworthy and will not distribute their personal information to other parties.
- A good practice is to look at the privacy policy of such recipients.
- Users should not allow others to use their user-IDs and passwords.
- When accessing public email servers (eg. GMail, Webmail) or when connecting to public SMTP servers (eg. Mweb, iAfrica) from a workstation that is linked to the DRPW network, users must ensure that any attachments are scanned for viruses on the user's workstation.
- A user who automatically or manually forwards his/her internal mail to public email servers will be held responsible for security breaches resulting from this practice.

9.4 Addressing

- When a user sends email, it is the user's responsibility to ensure that the email address of the recipient is correct. Address books should be kept up to date.
- When user recognizes that an email item has been incorrectly addressed to him/her, the user should inform the sender by returning and deleting the email.
- The user is responsible for managing his/her disk space on the email server and regular maintenance (Archiving) is expected.

9.5 Protection of email

- DRPW shall install antivirus software to protect its systems against known viruses.
- The email sever will be configured to reject any email with attachments in excess of the maximum limit of 2Mb total.
- DRPW reserve the right to install software to monitor email usage.
- If such software is installed, users shall be informed of their rights and limitations thereto.
- Users should be alert to suspicious looking attachments sent by email.
- These may not be opened but deleted or referred to the IT section for further investigation.
- The user must immediately report any malfunction that may be related to a computer virus to the IT helpdesk.

9.6 User Accountability

- Users are accountable for the content of every email sent from their accounts.
- Users shall guard against unauthorised usage of their accounts by:
 - ✓ Keeping their email passwords confidential.
 - ✓ Changing their passwords on a regular basis.
 - ✓ Signing off their email accounts each time they leave their workstations.

9.7 Prohibited use of email

- The prohibited use of email includes, the following:

9.7.1 Contravening the laws of the Republic of South Africa for private purpose

- For any purpose that contravenes the laws of the Republic of South Africa - such as victimisation.
- Uses that could lead to civil or criminal litigation against DRPW, for example libelous remarks about people, products or companies.
- Electronic fraud through misrepresentation of identity, the use of an anonymous identity or someone else's identity or password for the purpose of wronging or disadvantaging that person.
- Sending of material to or about others that is clearly intended to bother, intimidate, disparage or offend.

- Sending or displaying material that does not adhere to the Northern Cape Provincial Government's code of conduct, such as pornographic material, racist remarks, and sexist remarks.
- Distributing copyright material in such a manner that the copyright is infringed.
- Intercepting, interrupting or changing electronic packages for malevolent reasons or misrepresenting the original message.

9.7.2 Disclosing of Confidential Information

- Unsecured sending of DRPW confidential information that could lead to accidental or premature disclosure.

9.7.3 Abusing Bandwidth

- Causing congestion on the network by the distribution of, for example chain letters, jokes, images and applications that add no value to the Department.
- Broadcasting unsolicited commercial email (junk email or "Spam") to mailing lists.
- Sending inappropriate messages to groups or individuals, and spreading broadcasts without the permission of DRPW Senior Management.

9.7.4 Spreading Malicious Code (Viruses)

- Any action (e.g. downloading software) that would knowingly lead to the distribution of computer viruses.

9.7.5 Personal Gain

- Using email for personal gain, outside business activities, fund raising or charitable activities not sponsored by the Northern Cape Government.

9.7.6 Access Rights of Ex-Users

- Users, whose employment with DRPW has been terminated, have no right of access to the contents of messages addressed to them - whether official or private.

9.7.7 Disciplinary Measures

- The departmental IT section as well as the Provincial IT unit (in the Office of the Premier) will monitor the email systems and inform management of any misuse of email that they are aware of.
- These contraventions by staff are subject to DRPW's disciplinary procedures.
- This could lead to sanctions ranging from censure, loss of access to the email service or dismissal if the contravention warrants it.
- Contractors and third-party users who do not observe the policy and procedures may be removed from the system, and their contracts may be cancelled if the contravention warrants it.

9.7.8 Prohibited File Attachments

- Certain file types are known to be highly susceptible to "virus piggybacking". Therefore files with the following file extensions is prohibited from being forwarded on the network and will be blocked from passing through the email gateway: (*.scr, *.cpl, *.exe, *.com, *.pif, *.rtf, *.htm, *.bmp, *.zip, *.cmd, *.html, *.txt, *.avi, *.mp3/4/5/6, *.mpg, *.mpeg, *.vbs, *.wmv).

10. INTERNET USAGE

10.1 Objective

- To formulate policy directives that will guide the Department in terms of preventing users from misusing departmental resources accessing the Internet.

10.2 Internet/Intranet Access

- Internet access is granted to end users on a need to execute a job bases.
- Internet access will only be granted to a user after a fully completed Internet access application form which is recommended by his/her Unit Head and approved by the HOD is forwarded to the IT Manager.

10.3 Prohibited use of the Internet/Intranet in DRPW

- The prohibited use of the Internet/Intranet includes:

10.3.1 Contravening the laws of the Republic of South Africa

- For any purpose which contravenes the laws of the Republic of South Africa.
- Uses that could lead to civil or criminal litigation against DRPW, for example placing libelous remarks about products or companies or persons on websites.
- Electronic fraud through misrepresentation of identity, the use of an anonymous identity or someone else's identity or password for the purpose of wronging or disadvantaging that person.
- Distributing or using copyrighted material, which has copyright in such a way that the copyright is infringed.

10.3.2 Conducting Internet practices that could lead to litigation against DRPW.

- Intercepting, interrupting or changing electronic messages for malevolent reasons or misrepresenting the original message.
- Attempting to gain, or gaining, unauthorized access to computer resources on the DRPW network or any external network (hacking).
- Attempting to bypass, or bypassing, DRPW or any other companies' security measures.

10.3.3 Disclosing Confidential Information.

- Unsecured sending of DRPW confidential information that could lead to accidental or premature disclosure.

10.3.4 Abusing Bandwidth.

- Internet/Intranet bandwidth is shared between all users with the effect that inconsiderate and unacceptable behavior will impact on all fellow-users.
- **The following statements about prohibited behavior specifically address this issue:**
 - ✓ Causing congestion on the network by, for example, watching webcams or off-loading video clips, audio files or applications that is of no value to the Department.
 - ✓ Excessively using automated downloads, search programs, query tools or polling programs (e.g. web pages that continuously update sports results) on the Internet.

10.3.5 Violating DRPW's Values.

- Visiting sites or displaying material downloaded from sites that do not adhere to the Northern Cape Provincial Government's code of conduct, e.g. pornographic sites, racist sites, etc.
- Participating in chat rooms where the subject and/or discussion do not adhere to the Northern Cape Provincial Government's code of conduct.

10.3.6 Spreading Malicious Code (Viruses)

- Any action (e.g. downloading software) that would knowingly lead to the distribution of Computer viruses.

10.3.7 Compromising Network Security.

- Establishing a dial-up connection (via a modem) to the Internet/Intranet from a workstation that is connected to the DRPW network.
- Establishing any type of connection that bypasses a properly configured and authorised firewall infrastructure that filters traffic and blocks unauthorised access.

10.3.8 Personal Gain

- Using Internet/Intranet facilities for personal, outside business activities, fund raising or charitable activities are not permitted by DRPW.

11. IT PROCUREMENT

11.1 Objective

- These guidelines inform the end-users and IT staff on how to procure IT related items.

11.2 Procurement Requests

- Procurement of any IT equipment must be done in conjunction with the departmental Supply Chain Management Policy.

11.2.1 Submission

- The personnel requiring the hardware and software items must submit an IT Requisition Form to their unit manager for approval.
- The unit manager must recommend the form if he/she is satisfied with the contents and submitted to the Unit Head for approval.
- Only the approved form will be submitted to the IT Section for the purchasing of the equipment.
- All requests must be submitted one month prior to the expected delivery/requirement date.

11.2.2 Approval and SLA,s

- Confirmation of order will be done in accordance with the departmental Supply Chain Management Procedure and practices.
- The vendor that submits a quotation that meets the minimum criteria stipulated in the specifications, coupled with costs effectiveness, will be awarded the opportunity to supply DRPW with the goods in accordance with the Supply Chain Management Procedures.
- All software must be licensed in accordance with the rules stipulated by the producer/supplier of the software.
- SLA's or Maintenance agreements requested for hardware and software must be approved by the Head of Department.

12. HARDWARE STANDARDS

12.1 Objective

- This section provides direction in terms of the allocation of IT hardware and the depreciation thereof.

12.2 Hardware Procurement

- This policy and the overall departmental Supply Chain Management Policy shall guide procurement of all hardware. Hardware devices shall either be leased or purchased outright.

12.3 Hardware Classification

- A workstation / seat is defined in this policy as follows:
 - ✓ A place where an official is able to access resources on the DRPW network and be able to perform his / her duties.
 - ✓ A seat can be fixed or mobile.
 - ✓ A seat starts from the point where network facilities are accessed (e.g. network point on the wall) up to and including production of a document in either electronic or hard copy.

- A seat comprises of and is not limited to the following equipment and/or functionalities:
 - ✓ desktop or laptop;
 - ✓ accessing resources on the network;
 - ✓ accessing emailing facilities;
 - ✓ accessing printing facilities;
 - ✓ accessing internet but not essential.

- Servers and Printers are essential though are not considered by policy as part of a seat.

- A multifunction printer is defined in this policy as a printing device that can perform the following functions:
 - ✓ print colour pages (not high volume); scan documents;
 - ✓ send and receive faxes;
 - ✓ make photocopies.

- A multifunction digital copier is defined in this policy as a printing device that can perform the following functions:
 - ✓ high volume photo copying;
 - ✓ scan documents;
 - ✓ send and receive faxes;
 - ✓ print.

12.4 Allocation

- All officials from manager level shall be allocated a laptop, the functionality of which shall conform to the standards stipulated by the procurement policy. All other officials shall be allocated a desktop with the exception of those that travel considerably, which shall be allocated a laptop. The stated exception shall only be granted upon approval via the CFO.

12.5 Maintenance

- Hardware shall be maintained in accordance with the recommended vendor specification.
- Maintenance of hardware shall remain the sole responsibility of the IT technical support team.

12.6 Depreciation

- The IT section shall ensure that the depreciation of hardware and the write-off of obsolete IT equipment is done in accordance with the departmental Asset Management Policy and Provincial Treasury Regulations.

12.7 End User Equipment Specifications

- The specifications for desktops and laptops are attached to this document as the proposed hardware and software standards.
- Each printer shared by more than five (5) people shall meet the following minimum requirements:
 - ✓ Networkable.
 - ✓ RAM = sixteen (16) MB.
 - ✓ Capable to print duplex.
 - ✓ Capable of printing a minimum of twenty two (22) black and white pages per minute or sixteen (16) pages per minute black or full colour.

12.8 Peripheral Hardware Distribution

- One black and white network laser printer shall be installed where there is more than one official in an office.
- The CFO must approve deviation from this.

- For heavy-duty printing, officials will have to make use of the nearest high volume printer or copier.

13. ASSET MANAGEMENT

13.1 Objective

- The objective of asset management, as far as ICT is concerned is to enable the DRPW to keep track of the Department's hardware and software from requisition through to retirement. Though asset management may serve to reduce the cost of hardware and software, the ultimate objective is to synchronise technology implementation with business objectives and to move IT from the tactical to the strategic level.

13.2 Acquisition of Tools

- Tools to aid in the taking of inventory and the management of assets shall be acquired. These tools must at minimum have functionality to scan bar codes imprinted on the Department's IT equipment through hand held bar code readers and asset management software.

13.3 Inventory

- A database of all IT-related assets shall be established and maintained by the departmental Asset Management Unit. The asset database will be used to control location, ownership, maintenance and utilization of assets.

13.4 Hardware Maintenance

- The following procedure is to be followed for an item submitted for repairs:
 - ✓ Faults are to be reported to the IT section.
 - ✓ The duration of the fault is to be reported.
 - ✓ The IT section is to ascertain and establish the nature of the fault.
 - ✓ A technical report has to be compiled by IT.
 - ✓ Three quotations are to be acquired for the repairs and/or maintenance of the hardware by the IT section.
 - ✓ Repairs and maintenance are to be approved by the CFO or Senior Manager.

13.5 Hardware Retirement

- All hardware should be assessed once a year to establish the value and usability thereof.
- Tag for retirement all hardware that are obsolete.
- Formulate plans to replace obsolete assets if need be.
- Cancel maintenance contracts on all obsolete assets.
- Move the assets to an asset retirement location.
- Discard all assets in accordance with the departmental Asset Management Procedure.

13.6 Licenses and Contracts

- Reports must be produced on a periodic basis to determine which contracts and licenses are up for review or renewal.
- Renewal of software licenses and contracts must be negotiated where necessary.

13.7 Asset Tracking

- Each time an asset is moved from one location to another, the new location and the date it was moved must be recorded, using the relevant forms provided by the departmental Asset Management Unit.

13.8 Best Practices

- Standardization of the desktop environment.
- Centralize hardware and software procurement - Involve all the stakeholders.
- Communicate the importance of asset management and publicize its gains.
- Senior management backing is crucial to the success of asset management.

14. IT SUPPORT AND MAINTENANCE

14.1 Objective

- This section provides guidelines to users on fault reporting procedures and basic PC troubleshooting.

14.2 Operations Manuals

- Documentation of all IT procedures and operations shall be done. These shall be updated every time there is a change to the operations procedures. The IT Manger shall supervise the documentation of operations manuals, and ascertain that the instructions are carried out to the letter. A procedure manual shall speak to this document.

14.3 Helpdesk

- All faults may be reported to the helpdesk during the following periods:
 - ✓ Period: Monday to Friday (excluding public holidays).
 - ✓ Time: 07h00 - 13h00 / 14h00 - 16h00.
- The helpdesk will be responsible for accepting, documenting, diagnosing, monitoring and resolving all IT-related faults.

14.4 Fault Reporting Guidelines

- Before a fault is reported a basic fault finding procedure must be carried out.
- Any relevant and necessary information pertaining to the fault should be readily available.
- A fault reference number will be provided for each and every fault reported to the helpdesk. This will be the only acceptable proof that a fault has in fact been recorded, should such a fault be queried at later stage. Therefore, it is advisable to request a reference number.
- IT personnel manning the helpdesk will at all times endeavour to resolve faults immediately and telephonically, within five to ten minutes.
- If a fault cannot be resolved within that time period, the call will be terminated and the fault will be referred for further action.
- In the event of a fault being referred, the user will be kept regularly informed of the progress until it is resolved.
- If IT personnel manning the helpdesk are unable to resolve a fault, depending on the nature and type of fault, it will be referred to the technicians.
- Faults outstanding for longer than two days may be referred and reported to the IT unit manager.
- Equipment sent in for repairs may take from three days to several weeks to be repaired depending on the nature and type of fault.

- An assessment of the fault will be concluded and the nature of the fault established.
- The user will be provided with a preliminary indication of the duration of the repairs / maintenance.
- Should equipment be irreparable, the user will be provided with three quotes for the replacement of the equipment.

14.5 Basic Fault-Finding Guidelines

- Check that the power switch on the computer or printer is switched on.
- Ensure that power leads are properly and firmly connected between computers and printers and wall power plugs.
- Check that the wall power plug is in fact switched on.
- Check that the monitor's power is switched on.
- Check that the monitor adjustment controls are operating correctly.
- Ensure that applications are closed properly.
- Ensure that you sign off the network correctly, especially from applications such as PERSAL.
- Ensure that you sign on to the network properly and read the instructions on the screen carefully.
- Check that the network cable between the computer and the termination box (a small box mounted on the wall near the power ducting) is firmly connected.
- Check that there is paper in the printer tray.
- Ensure that toner cartridges are replaced when indicated by the printer (normally by a warning light).
- Close all applications, before you go home and sign off the network.
- If you do not sign off from the network before going home you will have to reset or switch the computer off and on the next morning.
- When physically disconnecting computers ensure that the power has been switched off first and only then disconnect power cables or other cables.

14.6 Procedure Manual

- A procedure manual, which shall be revised as the need arises, must be drafted by the IT Manager in consultation with other relevant managers which will guide all IT technical staff on how to perform their duties.

- Failure to adhere to the procedure manual will result in disciplinary measures, which may lead to dismissal, if the extent of the damaged caused warrants it.

14.7 Remote Management & Assistance

- Assistance can be offered to end users by Remote Control using Tight VNC. The VNC application must be setup by IT staff members in such a manner that the end user must first accept the connection to the specific machine.

15. IT PROJECTS

15.1 Objective

- This section provides guidance on matters relating to the planning, initiation and management of IT projects using formal project management techniques. The Project will be administered by the IT Section. The complete Project will be monitored on Spiceworks applications.

15.2 Project Planning

15.2.1 Business Case

- Establish business objectives.
- Provide project alternatives.
- Determine costs and quantify benefits.
- Before proceeding, the responsible manager shall decide if the project is worthwhile.

15.2.2 Project Start Up

- Describe the project (Project Definition).
- Define the project management structure.
- Identify the sponsor, project manager and relevant stakeholders.
- Review the current literature relevant to the project.
- Compile a list of resources required to populate the defined structure.

15.2.3 Project Scope

- Establish the project scope and identify the project constraints.
- Analyze the risks associated with the project.

15.2.4 Project Organization and Reporting

- Select and prepare the human capital necessary for the successful completion of the Project.
- A steering committee constituting of the project sponsor, project manager, vendor representatives and key stakeholders shall be established for each project.
- This committee shall be reported to regularly and in the event of an emergent risk.

15.2.5 Project Schedule

- Create a detailed work plan with associated costs based upon an approach or methodology to be used.
- Create time frames and specify deliverables.
- Document the project approach and the project management tools that will be used.

16. SOFTWARE AND SYSTEMS DEVELOPEMENT

16.1 Objective

- This section aims to ensure that minimum security requirements shall be adhered to during the system acquisition process and that appropriate security is built into information systems.

16.2 User Requirement Specification

- The user requirements for the new systems or enhancements to existing systems shall specify the security objectives of the system as well as the security control requirements, including the need for alternative arrangements in case of systems downtime.

16.3 Designing of Specifications

- System Architecture:
 - ✓ Security services and mechanisms shall be planned, designed, developed and tested in a way that correlates with the sensitivity of the application and / or data.

- ✓ The required security mechanisms (entity authentication; modification; encryption; audit facility and recovery mechanisms) for specific applications shall be documented.

- Identification and authentication:
 - ✓ All users, data, programs, transactions and other system elements and sources shall be uniquely and specifically identified during the user requirement specification and the design of the system.
 - ✓ Identification and authentication capabilities shall be incorporated in the system design specifications to ensure verification of identities as well as individual accountability during system use.

- Authorization:
 - ✓ A mechanism shall be designed to give authorization for the access of users, programmes, terminals and transactions to system sources (eg. data).

- Controllability:
 - ✓ The system shall be designed in such a way that the various components (for example transaction modules, programmes, operating system interfaces and databases) can exercise full control over data or data capabilities.

- Integrity:
 - ✓ The integrity requirements in respect of data, programmes and the processing capability shall be specified to ensure that the system performs its allocated functions, and only those functions, correctly, consistently, within the time limit and precisely according to specifications.

- Recoverability / Availability:
 - ✓ The system design shall ensure that there is no breach of security during system failures and that the loss of data and processing ability can be traced and replaced and repaired as soon as possible.

16.4 Systems Development

- Development, testing and operational facilities shall be separated to achieve segregation of the involved and to prevent accidental change or unauthorized access to operational software and data.
- Development and operational software shall, where possible, run on different computer processors or in different domains or directories.
- Control measures and procedures for the protection of programs and data shall be built in, tested and audited to ensure that the data and programs cannot be changed without authorization, destroyed or subject to sabotage and / or espionage owing to negligence or deliberate acts.
- All systems / programs shall meet the prescribed security requirements and the programming standards.
- Master software and documentation shall be stored separately.
- The development of systems shall not be done with live data unless it is transferred to a separate test system.
- Databases containing personal data shall be depersonalized before being used for testing.
- If possible only executable code shall be held on operational systems.
- Executable code shall not be implemented on an operational system until evidence of successful testing and confirmation that the system works as intended, that it does not impact negatively on other systems and is user friendly.
- Executable code shall be stored safely and securely on fixed media.
- No unauthorized temporary amendments (patches) shall be made to production and/or operational programmes.

16.5 Systems Manuals

- The system manual must comprise of a technical, user and training section.
- Security may be integrated in the manual or a separate information system security manual may be compiled.
- The system manual shall be compiled at the start of the system development phase.
- All security aspects in respect of the system shall be identified in the collaboration with the Security Manager, documented in the system manual to ensure that prescribed security measures are adhered to.

- Limitations in respect of the use of the system interfaces shall be defined and incorporated into the system manual.
- Management and administrative control measures, that ensure the correct application of system interfaces, shall be documented.
- The system manual shall be updated after all system/programmes changes have been made.

PART THREE

1. PROPOSED SOFTWARE AND HARWARE STANDARDS

1.1 Basic Software Standards

- *Refer to DRPW – 2012 DRPW SCM Circular – IT Specifications:*
 - ✓ Basic User - Secretaries; Personal Assistants and office Administrators.
 - ✓ Advanced Users – HCM, Finance; Procurement Personnel; Executive Managers; and Senior Managers.
 - ✓ Specialist Users - Administrators; Technical Support; Technical Designers and Web Developers.

1.2 Computer Hardware Standards

- *Refer to DRPW – 2012 DRPW SCM Circular – IT Specifications:*
 - ✓ Laptop Specifications.
 - ✓ Desktop Specifications For All Users.

1.3 Laptop Guidelines

- *Refer to DRPW Utilization of Laptop Computers Policy.*

PART FOUR

1. MONITORING AND EVALUATION

- 1.1 The Directorate Monitoring and Evaluation will monitor and evaluate compliance and impact of these guidelines by all programmes and sub-programmes in the Department.

- 1.2 The Financial Inspectorate will perform investigations with regard to compliance, regulations, policies and procedures.
- 1.3 The departmental Information Technology (IT) Committee and the departmental Security and Information and Communication Technology Committee (SICTC) respectively, shall convene meetings on a monthly basis in order to assess the performance of the Department with regards to this policy.

2. POLICY REVIEW

- 2.1 This policy shall be assessed in every five (5) years from its effective date to determine its effectiveness and appropriateness. This policy may be assessed at any time as deemed necessary to reflect substantial organisational etc. changes at the Department or any change required by law.
- 2.3 Deviations from this policy must be approved by the Accounting Officer.

ANNEXURE A

- *Refer to DRPW – IT Procedures.*

PROCEDURE GUIDELINES FOR NETWORK CONTROLLERS

1. Fault Logging Procedure

- 1.1 **When a fault is reported the following procedure must be followed:**
 - The NWC shall record all faults on the Computer Management System.
 - The NWC shall attempt to assist the user telephonically (if the user is not based locally the NWC may remote to the user's workstation).
 - If the fault cannot be resolved telephonically the NWC shall provide the user with the fault reference number and advice the user as to how soon the fault can be attended.
 - If fault is resolve telephonically the fault is "logged off" on the Computer Management System and a job card is printed, signed by the NWC and passed on for filing.
 - If the fault cannot be resolved telephonically, the NWC prints a job card and visits the user requiring the technical support to establish the nature of the fault.

1.2 If the fault is resolved the following procedure is to be followed:

- The user signs the job card.
- The NWC logs off the job on the Computer Management System.
- The job card is sent for filing.

1.3 If the fault is not resolved, the following procedure is to be followed:

- The NWC issues a Temporary Removal of Item Form and lists the equipment, which has to be removed from the user 's work area.
- Both the user and the NWC sign this form before the equipment is removed.
- The NWC books the item in at the Helpdesk and the job card is attached to the item/s.

1.4 Fault Logging Procedure for equipment under guarantee

- The NWC reports the faulty equipment to the supplier and records the items together with the serial number in his / her delivery notebook.
- The NWC then delivers the equipment to the supplier or the supplier collects the equipment.
- On delivery the supplier acknowledges receipt of the equipment by signing the delivery notebook.
- On receipt from the supplier the NWC verifies the equipment received with those listed in his / her delivery notebook before acknowledging receipt of the items.
- The NWC checks the equipment and verifies if it was repaired by the supplier.
- The NWC then issues an Items Returned Form and installs the equipment at the user's workstations or the equipment is collected by the user (if collected by the user, the equipment must be stored in the storeroom and recorded in the storeroom register prior to collection).
- On collection or receipt, the user signs the job card as well as the Items Returned Form.
- The NWC "logs off" the job on the Computer Management system.
- Both the job card and the Items Returned Form are sent for filing.

1.5 Procedure for equipment that is not under guarantee

- The NWC attempts to repair the faulty equipment.

1.6 The following procedure is to be followed for replacement of hardware components:

- The NWC identifies which components must be replaced.
- The NWC acquires One (Pay for Repair Quotation) quotes for the replacement of the components.
- The NWC compiles a report for the replacement of the components and submits it to the user.
- The user compiles a submission to his / her manager for approval.
- If approved the submission is forwarded to the finance section for the issuing of an order number.
- The order is then placed with the relevant supplier and a copy of the order form is forwarded to the relevant NWC.
- When the components arrive the relevant NWC verifies whether the components supplied are correct and acknowledges receipt thereof.
- The date, serial number (if applicable) and description of the component is recorded on the existing job card and is attached to the item that has to be repaired.
- The component is tested and if working the invoice is forwarded to the finance section for processing.
- The NWC then issues an Items Returned Form and installs the equipment at the user's workstation or the equipment is collected by the user (if collected by the user, the equipment must be stored in the storeroom and recorded in the storeroom register prior to collection).
- On collection or receipt, the user signs the job card as well as the Items Returned Form.
- The NWC "logs off" the job on the Computer Management system.
- Both the job card and the Items Returned Form are sent for filing.

1.7 Procedure for receipt of newly purchased equipment

- When the new equipment is delivered, the contents must be verified against the delivery note.
- Jobs must be logged on the Computer Management System and the job cards must be printed and attached to the equipment.

- The equipment must then be recorded on the storeroom register and stored accordingly.
- The invoice for the equipment must be forwarded to the finance section for processing.

1.8 Prepping computers or laptops

- If new, the computer and accessories must be checked for comprehensiveness.
- The entire set of components of a computer must be registered against the correct user name on the Computer Management System.
- The operating system must be activated and correctly configured.
- The software must be correctly installed, configured and activated.
- The username and password must be setup on the computer.
- Additional software must be installed on the computer (e.g. PERSAL, PALS, BAS, Acrobat Reader).
- The correct Anti- virus software for the specific site must be installed.
- The correct network configuration must be setup on the computer.
- The correct network operating software must be installed and configured on the computer if required (e.g. Novell).
- Windows update utility must be run on the computer.
- Test the computer for functionality of all software and hardware.
- If the user has used another computer before, the documents, email messages and contacts must be transferred over to the new computer and verified against the original data.
- The Internet and email accounts must be setup.
- An inventory list must be printed on the Computer Management System which must be signed by the user as an acknowledgement of receipt.
- The original copy of the acknowledgement is forwarded to the Asset Management Unit for filling and updating of the asset register.
- A copy is presented to user.

1.9 Creating a New User

- When creating a new user the following information must be stated on the fault log form submitted to the Provincial IT Unit (Office of the Premier):
 - ✓ The Username (Initials and Surname).

**DEPARTMENTAL POLICY ON INFORMATION AND COMMUNICATION
TECHNOLOGY: STANDARDS AND GUIDELINES**

- ✓ The MAC Address of the computer to be used by the user.
- ✓ The IP Address of the computer to be used by the user.
- ✓ The location of the user.
- ✓ Additional services used by the user (e.g. BAS, PERSAL, PALS, Internet).

2. Peripherals (Printer cartridges, Printer, Keyboards, Flash disks etc.)

- All newly purchased peripherals must be loaded onto the Computer Management System.
- All issuing of peripherals must be done via the Computer Management System.
- On issuing a new peripheral the following must be done:
 - ✓ The faulty peripheral must first be screened for repairing before a new one is issued.
 - ✓ When a new peripheral (e.g. Keyboard) is issued the inventory data must be updated on the Computer Management System and a printout must be forwarded to the Asset Management unit for the updating of the Asset Register.
 - ✓ The user must sign an acknowledgement of receipt form on accepting the new item (this must also be forwarded to the Asset Management unit).
 - ✓ The redundant item must be handled according to the departmental Asset Management Policy.

TRANSVERSAL SYSTEMS SUPPORT

- If the system is reported offline, the NWC will check to following:
 - ✓ Is it the only user experiencing the problem?
 - ✓ How wide spread is the problem?
 - ✓ How severe is the problem?
 - ✓ If the entire system is down the NWC will inform all users affected and consult with the relevant parties concerned (SITA Networks, SITA mainframe support, departmental system controllers).
 - ✓ Should the problem be software based, a job card must be printed and the fault must be attended to (if the user is not based locally the NWC may remote to the user's workstation to attempt to resolve the problem).

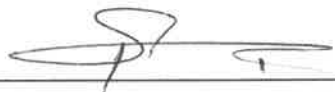
- ✓ Should the problem be one that only Specially Trained Technical Support persons may be able to resolve, the NMC will refer the fault to relevant system controller or technical support team.

POLICY APPROVAL

This policy is Approved / Not Approved

Comments:

.....
.....
.....
.....



ACCOUNTING OFFICER

05.03.19

DATE
