



**LIMPOPO**  
PROVINCIAL GOVERNMENT  
REPUBLIC OF SOUTH AFRICA

**DEPARTMENT OF  
ROADS AND TRANSPORT**

**INFORMATION TECHNOLOGY SECURITY  
POLICY**

## TABLE OF CONTENTS

## PAGES

1. Logical security policies	4
1.1 Software Security Policy	4
1.2 Antivirus Policy	5
1.3 Software development and change controls policy	6
1.4 Purchase and regulation of hardware and other equipment policy	10
1.5 Data security policy	11
1.6 Business Continuity Planning (BCP) policy	12
1.7 Backup and archival storage policy	14
2. Communications security policy	15
2.1 Networks	15
2.2 Encryption	16
2.3 Electronic mail system policy	16
2.4 Anti-cyber crime policy	17
3. Complying with legal and policy requirement	19
3.1. Being aware of legal obligations	19
4. Personal issues relating to security	20
5. Policy Review	22

## **I Preamble**

It is a long-standing view that information be shared subject to privacy and confidentiality requirements. This reflects the fact that information is a unique resource that increases than dissipates when it is used. Consistent with this principle, the Department of Roads and Transport seeks to provide appropriate access to information among its staff, clients and stakeholders. Access to information however carries with its responsibility to protect privacy, confidentiality and integrity. So to enhance this, this policy document has been accepted and by the Department of Roads and Transport and it sets forth its handling.

## **II Purpose**

To establish the basic policy for the Department that will guide the use, procedures, principles, norms and standards, rules, regulations for the protection, and presentations of all information, in any form, which is generated by, owned by , or otherwise in possession of the Department.

## **III Scope of policies**

Information Technology security policy is intended to support, protect, control the management of departmental information resources. This policy covers all information within the department including data and information.

- Kept in the database.
- Kept on computers and associated electronics gadgets, devices and systems.
- Transmitted across Local Area Network (LAN) and Wide Area Network (WAN).
- Printed and hand written on paper or notice boards.
- Sent by fax, telex, or any other form of communication.
- Kept on removable media such as CD-ROMs, hard disk, tapes, flash memories and other similar media in whatever manner.
- Kept on fixed media in whatever manner.
- Kept on fixed media such as hard disk and disk-subsystems.
- Held on film or microfiche.
- Presented on slides, overhead projectors, using visual and audio media.
- All data supporting the business and operations of the Department.

## **IV Scope**

The policy objectives are as follows:-

- To protect department's business information and any public information within its custody by safeguarding its confidentiality, integrity, authenticity and availability.
- To develop principles to protect the department's information resources from theft, abuse, misuse, distortion and any form of illegal damage.
- To enforce responsibility and accountability for information security in the department.
- To encourage employees to information an appropriate level of awareness, knowledge and skills to allow them to minimize accidents for information.
- To ensure departmental continuity with its activities during accidents towards information security.
- To voluntarily comply with minimum security information requirements as set out in the Provincial Information Policy Framework

## **V User Awareness**

Personnel members are encouraged to familiarize themselves with the departmental information security policy as well as the responsibility regarding their daily job description. Improved awareness of Information Security issues and procedures does not only reduce the risk of information accidents, but also increase the likelihood of suspicious activities being reported and preventative measures being implemented.

## **VI Handling non-compliance**

All personnel members of the department shall be personally responsible for understanding and following Information Technology Security Policy and shall be personally accountable for the consequences of any security violation resulting from their failure to observe such policy. The Department shall identify and provide appropriate information security awareness tools to support this process.

### **1. LOGICAL SECURITY POLICIES**

#### **1.1 Software Security Policy**

##### **1.1.1 Managing Passwords**

The selection of passwords, their use and management as a primary means to control access systems is to be strictly adhered to best practice guidelines. In particular, passwords shall not be shared with any other person for any reason. Users are responsible for all activities done in or from your account.

### **1.1.2 Lock Out Policy**

Software lockout mechanisms in case of failed attempted log ins shall be established and enforced.

### **1.1.3 Password Character**

Passwords should be of such a combination that it includes alphabetic, alphanumeric, numeral, upper and lower caps. Passwords formulation shall be software enforced especially to those operating critical systems.

### **1.1.4 Clear Screen Policy**

All users of workstations, PCs/ laptops are to ensure that their screens are clear/blank when not being used.

### **1.1.5 Loading Personal Screen Savers**

Employees are discouraged from loading non-approved screen savers onto the Departmental PCs, laptops and values of the Department.

### **1.1.6 Logon and logoff from your computer**

Approved login procedures must be strictly observed and users leaving their screen unattended must firstly lock access to their workstation or log off.

### **1.1.7 Security Unattended Workstations**

Equipment is always to be safeguarded appropriately - especially when left unattended.

## **1.2. Antivirus Policy**

### **1.2.1 Responsibility of IT unit with regards to Computer Viruses**

### **1.2.2 Computer Virus and Worms**

The threat posed by the infiltration of a virus is high, as is the risk to the Department's systems and data files. Formal procedures for responding to a virus incident are to be developed, tested and implemented. Virus Incident response must be regularly reviewed and tested by IT technicians.

### **1.2.3 Handling of Hoax Warnings**

Procedures to deal with hoax virus warnings are to be implemented and maintained. Hoax threats - the spreading of rumours of fictitious viruses or other malicious code \_ can waste time, as staff attempt to locate a virus which does not exist. Vigilance and good virus intelligence warnings are the key to minimising the impact of hoaxes.

### **1.2.4 Defending Against Virus Attacks**

Without exception, Anti Virus software is to be deployed across all PCs with regular virus definition updates and scanning across servers, PCs and laptop computers.

### **1.2.5 Updating Anti Virus Definition Files**

Updates of virus definition files are to be daily reduce the risk of infection from a variant for which you do not have the necessary vaccine.

### **1.2.6 Scheduled Virus Scanning**

Weekly virus scans shall be done across all data files on all PCs on the network to increase the ability to detect and cure a virus before its 'footprint' is established on the network.

### **1.2.7 Virus user Awareness**

Consistent user awareness about the risks involved in opening unsolicited e-mails and new virus infections spreading in the organisation shall be done.

## **1.3. Software Development and Change controls Policy**

### **1.3.1 Development tools and Techniques**

#### **1.3.3.1 Managing Operational Program Libraries**

Only IT technicians may access operational program libraries.

#### **1.3.3.2 Managing Program Source libraries.**

Only IT technicians may access program source libraries.

### **1.3.3.3 Control of Software Code**

Formal change control procedures must be utilised for all changes to systems. All changes to programs/systems must be properly authorised and tested before moving to the environment.

### **1.3.3.4 Controlling Program Source Libraries**

Formal change control procedures with comprehensive audit trails are to be used to control Program Source Libraries.

## **1.3.2. Software Development**

### **1.3.2.1 Software Development Process**

Software development for or by the organisation must always follow a formalised development process which itself is managed under the project in question. The integrity of the Department's operational software code must always be safeguarded using a combination of technical access controls and restricted privilege allocation and robust procedures.

### **1.3.2.2 Establishing Ownerships for Process**

All proposed system enhancement must be business driven and supported by an agreed Business Case. Ownership (and responsibility) for any such enhancements will always rest with the IT unit which will co-ordinate with the user programme.

### **1.3.2.3 Justifying New System Development**

The development of bespoke software is only to be considered, if warranted by a strong Business Case and supported both by management and adequate resources over the projected lifetime of the resultant project.

### **1.3.2.4 Managing Change Control Procedures**

Formal change control procedures must be utilised for all amendments to systems.

### **1.3.2.5 Separating Systems Development and Operations**

There shall be clear segregation of duties to all areas dealing with systems development, systems operations, or systems administration.

### **1.3.2.6 Setting up New Spreadsheets**

The classification of spreadsheets must be appropriate to the sensitivity and confidentiality of data contained therein. All financial/data models used for decision making are to be fully documented and controlled by the information owner.

### **1.3.2.7 Setting up New Databases**

Databases must be fully tested for business logic and processing, prior to operational usage. Where such databases are to contain information of a personal nature, procedures and access controls must be enforced to ensure confidentiality.

## **1.3.3. Software Specification and Selection**

### **1.3.3.1 Specifying User Requirements for Software**

All requests for new applications systems or software enhancements must be presented to Head of Department with a Business Case with the business requirements presented in a User Requirements Specification document.

### **1.3.3.2 Selecting Office Software Packages**

All office software packages must be compatible with the Department's preferred and approved computer operating system and platform.

### **1.3.3.3 Using Licensed Software**

To comply with legislation and ensure ongoing vendor support, the terms and conditions of all End User Licensing Agreements are to be strictly adhered to.

### **1.3.3.4 Implementing New Upgraded Software**

The implementation of new or upgraded software must be carefully planned and managed, ensuring that the increased Information Security risks associated with such projects are mitigated using a combination of procedural and technical control techniques.

### **1.3.3.5 Service Level Agreements**

In cases involving vendor developed software, Service Level Agreements should be put in place to ensure that adequate support by the vendor is provided for continued business operation.



## **1.3.4 Software Maintenance and Upgrade**

### **1.3.4.1 Applying 'patches' to Software**

Patches to solve software bugs may only be applied where verified as necessary by IT technicians. They must be from a reputable source and are to be thoroughly tested before use.

### **1.3.4.2 Vendor Recommended Upgrades to Software**

The decision whether to upgrade software is only to be taken after consideration of the associated risks of the upgrade and weighing these against the anticipated benefits and necessity for such change.

### **1.3.4.3 Operating System Software Upgrades**

Necessary upgrades to the Operating Systems of any of the Department's computer systems must have the associated risks identified and be carefully planned, incorporating tested fallback procedures. All such upgrades should be undertaken as formal projects.

### **1.3.4.4 Support for Operating Systems**

Operating Systems must be regularly monitored and all required 'housekeeping' routines adhered to.

### **1.3.4.5 Recording and Reporting Software Faults**

Software faults are to be formally recorded and reported to service provider responsible for software support/maintenance.

### **1.3.4.6 Disposing of Software**

The disposal of software should only take place when it is formerly agreed that the system is no longer required and that it is associated data files which may be archived will not require resolution at a future point in time.

## **1.3.5 Change Control Procedures**

### **1.3.5.1 Controlling Test Environments**

Formal change control procedures must be employed for all amendments to systems. All changes to programs must be properly authorised and tested in an test environment before moving to the live environment.

### **1.3.5.2 Using Live Data for Testing**

The use of live data for testing new systems change may only be permitted where adequate controls for the security of the data in place.

### **1.3.5.3 Capacity Planning and Testing**

New systems must be tested for capacity, peak loading and stress testing. They must demonstrate a level of performance and resilience which meets or exceeds the technical and business needs and requirements of the organisation.

### **1.3.5.4 Parallel Running**

Normal System Testing procedures will incorporate a period of parallel running prior to the new or amended system being acceptable for use in the live environment. The results of parallel running should not reveal problems or difficulties which were not previously passed during User Acceptance Testing.

### **1.3.5.5 Training in New Systems**

IT to coordinate training for users and technical staff in the functionality and operations of all new systems.

### **1.3.5.6 Documenting New and Enhanced Systems**

All new and enhanced systems must be fully supported at all times by comprehensive and up to date documentation. New systems or upgraded systems should not be introduced to the live environment unless supporting documentation is available.

## **1.4 Purchase and Regulation of Hardware and other equipment Policy**

### **1.4.1 Information Security requirements for New Hardware**

All purchases of new systems hardware or new components for existing systems must be made in accordance with Information Security and other organisation policies, as well as technical standards.

### **1.4.2 Detailed Functional Needs for New Hardware**

Except for minor purchases, hardware must be purchased through a structural evaluation process which must include the development of a Request for

Proposal (RFP) document. Information Security features and requirements must be identified within the RFP.

#### **1.4.3 Installing New Hardware**

All new hardware installations are to be planned formally and notified to all interested parties ahead of the proposed installation date. Information Security requirements for new installations are to be taken into consideration in all cases.

#### **1.4.4 Testing Systems and Equipment**

All equipment must be fully and comprehensively tested and formally accepted by users before being transferred to the live environment.

#### **1.4.5 Controlling IT Consumables**

IT consumables must be purchased in accordance with the Department's approved purchasing procedures with usage monitoring to discourage the theft and improper use.

#### **1.4.6 Issuing Laptop/Portable Computers to Personnel**

Line management must authorise the issue of portable computers. Usage is restricted to business purposes, and users must be aware of, and accept the terms and conditions of use, especially responsibility for the security of information held on such devices.

### **1.5 Data Security Policy**

#### **1.5.1 Data Integrity and Retention**

##### **1.5.1.1 Data Integrity**

There shall always be measures to ensure that safeguards are in place to protect the integrity of data files during the recovery and restoration of data files; especially where such files may replace more recent files.

##### **1.5.1.2 Giving Access to Files and Documents**

Access to information and documents is to be carefully controlled, ensuring that only authorised personnel may have access to sensitive documents.

##### **1.5.1.3 Controlling Data Distribution**

For authorised personnel, the appropriate data and information must be made available as and when required; for all other persons, access to such data and

information is prohibited with appropriate technical control required to supplement the enforcement of this policy.

#### **1.5.1.4 Restrictions of Privacy Rights**

Notwithstanding the Department respect for employees' privacy in the workplace, it reserves the right to have access to all information created and stored on the Departments system.

#### **1.5.1.5 Data Confidentiality**

All employees are required to sign a formal undertaking concerning the need to protect the confidentiality of information, both during and after contractual relations with the Department.

#### **1.5.1.7 Deleting data Created/Owned by Others**

Data is to be protected against unauthorised or accidental changes, and may only be deleted with proper authority.

#### **1.5.1.8 Protecting Documents with Passwords**

Sensitive/confidential electronic data and information should be secured, whenever possible, with access control applied to the directory on the (computer) system concerned.

#### **1.5.1.9 Archiving Documents**

The Archiving of documents must take place with due considering for legal, regulatory and business issues with liaison between technical and business staff.

#### **1.5.1.10 Information Retention**

The information created and stored by the Department's information systems must be retained for a minimum period that meets both legal and business requirements.

#### **1.5.1.11 Linking Information between Documents and Files**

Highly sensitive or critical documents must not rely upon the availability or integrity of (external) data files over which the author may have no control. Key documents and reports must be self contained and contain all the necessary information.

## **1.6 Business Continuity Planning (BCP) Policy**

### **1.6.1 Initiating the BCP Project**

IT unit is required to initiate a Business Continuity Plan.

### **1.6.2 Assessing the BCP Security Risk**

IT unit to undertake a formal risk assessment in order to determine the requirements for a Business Continuity Plan.

### **1.6.3 Developing the BCP**

Management is to develop a Business Continuity Plan which covers all essential and critical business activities.

### **1.6.4 Testing the BCP**

The Business Continuity Plan is to be periodically tested to ensure that the management and staff understand how it is to be executed.

### **1.6.5 Training and Staff Awareness on BCP**

All must be made aware of the Business Continuity Plan and their own perspective roles.

### **1.6.6 Management and Updating the BCP**

The Business Continuity Plan is to be kept up to date and re-tested periodically.

### **1.6.7 Disaster Recovery Plan**

IT unit must ensure that disaster recovery plans for their systems are developed, tested, and implemented.

### **1.6.8 Supplying Continuous Power Critical Equipment**

The computer centre area shall have its own power supply connected to main power source for the building, and a back-up UPS or a fail-safe device is necessary for preventing a disk crash if the main power fails. A battery or self-starting generator shall be available to provide power for work lights, room ventilation, as well as air conditioning.

### **1.6.9 Managing and Maintaining Backup Power Generators**

Secondary and backup power generators are to be employed where necessary to ensure the continuity of services during power outages.

## **1.7 Backup and Archival Storage Policy**

### **1.7.1 Backing up Data on Portable Computers**

Information and data stored on Laptop or portable computers must be backed up daily. It is the responsibility of the user to ensure that this takes place on regular basis.

### **1.7.2 Managing Backup and Recovery Procedures**

Backup of the Department's data files and the ability to recover such data is a top priority. The frequency of such backup operations and the procedures for recovery shall meet the needs of the business.

### **1.7.3 Restore Procedures**

Restore procedures should be tested, as partial or invalid restore can corrupt the entire systems, which may partly or extensively terminate business operations.

### **1.7.4 Archiving Information**

The storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must be carefully considered, especially where proprietary formats are involved.

### **1.7.5 Retention Periods and Disposal of Data**

The archiving of electronic data files must reflect the needs of the business and also any legal and regulatory requirements.

### **1.7.8 Managing On-Site and Off-Site Data Stores**

On-Site locations where data is stored must provide access controls and protection which reduce the risk of loss or damage to an acceptable level.

## **2. COMMUNICATIONS SECURITY POLICY**

### **2.1 Networks**

#### **2.1.1 Configuring Networks**

The network must be designed and configured to deliver high performance and reliability to meet the needs of the business whilst providing a high degree of access control and a range of privilege restrictions.

#### **2.1.2 Managing the Network**

Suitably qualified IT staff is to manage the Department's network, and preserve its integrity in collaboration with the nominated individual system owners.

#### **2.1.3 Managing Network Security**

Access to the resources available from the Department's network must be strictly controlled in accordance with the agreed Access Control List, which must be maintained and updated regularly.

#### **2.1.4 Defending Network Information from Malicious Attack**

System hardware, operating and application software, the networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorised network intrusion.

#### **2.1.5 Forming Contracts Over Networks**

Network cabling should be installed and maintained by qualified network engineers to ensure the integrity of both the cabling and the wall mounted sockets. Any unused network wall sockets should be sealed-off and their status formally.

#### **2.1.6 Dial-Up Computer Communications**

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques.

#### **2.1.7 Accessing Networks Remotely**

Remote access to the Department's network and resources will only be permitted provided that authorised users are authenticated, data is encrypted across the network, and privileges are restricted.

## **2.2 Encryption**

### **2.2.1 When To Use Encryption**

Where appropriate; sensitive or confidential information or data should always be transmitted in encrypted form. Prior to transmission, consideration must be given to the procedures to be used between the sending and recipient parties and any possible legal issues from using encryption techniques.

### **2.2.2 Encryption Key Management**

Diligent care should be taken to ensure that encrypted information while secure; is also not inaccessible, even to authorised persons, due to poor key management.

### **2.2.3 Miscellaneous Encryption Matters**

In some countries, it is illegal to use ciphers, or the type of permissible cipher may be strongly regulated. This could result in unintentionally breaking the law where encrypted data is sent to such a country.

## **2.3 Electronic Mail System Policy**

### **2.3.1 Sending Electronic Mail (E-mail)**

E-mail should only be used for business purposes, using terms which are consistent with other forms of business communication. The attachment to an e-mail is only permitted after confirming the classification of the information being sent and then having scanned and verified the file for the possibility of a virus or other malicious code.

### **2.3.2 Legal issues around e-mails**

Relying upon e-mail from legal perspective, is not advised, as simple e-mail messages are not usually not authenticated as legal and should always be authenticated.

### **2.3.3 Personal e-mail**

Personal e-mail sent from one individual to another through the Department's systems, are discouraged as they can be misconstrued as coming from the organisation and can result in Information Security issues. Where they do occur, they should be clearly marked as Private.



### **2.3.4 Receiving Electronic Mail (E-mail)**

Incoming e-mail must be treated with the utmost care due to its inherent Information Security risks. The opening of e-mail with file attachments is not permitted unless such attachments have already been scanned for possible viruses or other malicious code.

### **2.3.5 Retaining or Deleting Electronic Mail**

Data retention periods for e-mail should meet legal and business requirements and must be adhered to by all staff.

### **2.3.6 Receiving Misdirected Information by E-mail**

Unsolicited or 'spam' e-mail is to be treated with caution and not responded to.

### **2.3.7 Forwarding E-mail**

Ensuring that information you are forwarding by e-mail (especially attachments) is correctly addressed and only being sent to appropriate persons. Any security risk (virus, content) associated with the original mail to you will also apply to the forwarded e-mail.

### **2.3.8 Filtering E-mail Content**

The department will use software filters and other techniques whenever possible to restrict receive or sending or sending of inappropriate information using e-mail.

## **2.4 Anti-Cyber Crime Policy**

### **2.4.1 Defending Against Premeditated Cyber Crime Attacks**

Security on the network is to be maintained at the highest level. Those responsible for the network and external communications must receive proper training in risk assessment and how to build secure systems to minimise the threats from cyber crime.

### **2.4.2 Collecting Evidence for Cyber Crime Prosecution**

Perpetrators of cyber crime will be prosecuted by the department to the full extent of the law. Suitable procedures are to be developed to ensure the appropriate collection and protection of evidence.

### **2.4.3 Defending Against Premeditated Internal Attacks**

In order to reduce the incidence and possibility of internal attacks, access control standards and data classification standards are to be periodically reviewed whilst maintained at all time.

#### **2.4.4 Defending Against Opportunistic Cyber Crime Attacks**

It is a priority to minimise the opportunities for cyber crime attacks on the Department's systems and information through a combination of technical access controls and robust procedures.

#### **2.4.5 Defending Against Hackers**

Risks to the Department's systems and information are to be minimised by fostering staff awareness, encouraging staff vigilance, and deploying appropriate protective systems and devices.

#### **2.4.6 Establishing Remedies to IS Breaches**

A database of Information Security threats and 'remedies' should be created and maintained. The database should be studied regularly with the anecdotal evidence used to help reduce the risk and frequency of Information Security incidents in the organisation.

#### **2.4.7 Investigating the Cause and Impact of Information security Incidents**

Information Security incidents must be properly investigated by suitably trained and qualified personnel.

#### **2.4.8 Recording Information Security Breaches**

Evidence relating to a suspected Information Security breach must be formerly recorded and processed.

#### **2.4.9 Ensuring the Integrity of IS Incident Investigations**

The use of information systems must be monitored regularly with all unexpected events recorded and investigated. Such systems must be periodically audited with the combined results and history strengthening the integrity of any subsequent investigations.

#### **2.4.10 Analysing IS Incidents Resulting from System Failures**

Information Security incidents arising from system failures are to be investigated by completed technicians.

#### **2.4.11 Responding to Information Security Incidents**

The Information Security Officer must respond rapidly to all Information Security incidents, liaising and coordinated with colleagues to both gather information.

#### **2.4.12 Using Information Security Incident Check Lists**

Employees shall be supported by IT unit in any reasonable request for assistance together with practical tools, such as security incident checklists, etc, in order to respond effectively to an Information Security incident.

#### **2.4.13 Detecting Electronic Eavesdropping**

Where a risk assessment has identified an abnormal high risk from the threat of electronic eavesdropping and/or espionage activities, all employees will be alerted and reminded of the specific threats and the specific safeguards to be employed.

#### **2.4.14 Reporting Information Security Incidents**

All suspected Information Security incidents must be reported promptly to the appointed Information Security Officer.

### **3. Complying with Legal and Policy Requirements**

#### **3.1 Being Aware of Legal Obligations**

Human Resources Management is to ensure that all employees are fully aware of their legal responsibilities with respect to their use of computer based information systems and data. Such responsibilities are to be included within key staff documentation such as Terms and Conditions of Employment and the Organisation Code of Conduct.

##### **3.1.1 Complying with General Copyright Legislation**

Persons responsible for Human Resources Management are to prepare guidelines to ensure that all employees are aware of the key aspects of Copyright, Designs and Patents Act legislation (or its equivalent), in so far as these requirements impact on their duties.

##### **3.1.2 Legal Safeguards against Computer Misuse**

IT Unit to prepare guidelines to ensure that all employees are aware of the key aspects of Software Copyright and Licensing legislation, in so far as there are requirements impact on their duties e.g. (copying and distribution of software, use of unlicensed software by contractors and consultants in the Department,

resale of redundant computers with software, using software beyond evaluation period etc).

### **3.1.3 Managing Media Storage and Recording Retention**

The department will maintain a suitable archiving and record retention procedure.

### **3.1.4 Complying with Information Security Policy**

All employees are required to fully comply with the Department's Information Security policies. The monitoring of such compliance is the responsibility of compliance unit.

## **3.2 Avoiding litigation**

### **3.2.1 Safeguarding against Libel and Slander**

Employees are prohibited from writing derogatory remarks about other persons or organisations using departmental e-mail or phone systems.

### **3.2.2 Using Copyrighted Information from the Internet**

Information from the Internet or other electronic sources may not be used without authorisation from the owner of the copyright.

### **3.2.3 Sending Copyrighted Information Electronically**

Information from the Internet or other electronic sources may not be transmitted without permission from the owner of the copyright.

## **4. Personal Issues relating to security**

### **4.1 Preparing Terms and Conditions of Employment**

The Terms and Conditions of Employment of this organisation are to include requirements for compliance with Information Security.

### **4.2 Employing/Conditioning New Staff**

New employee's references must be verified, and the employees must undertake to abide by the Department's Information Security policies.

### **4.3 Contracting with External Suppliers/other Service Providers**

All external suppliers who are contracted to supply services to the department must agree to follow the Information Security Policies of the organisation. An

appropriate summary of the Information Security policies must be formally delivered to any such supplier, prior to any supply of services.

#### **4.4 Using Non Disclosure Agreements (Staff and Third Party)**

Non-disclosure agreements must be used in all situations where the confidentiality, sensitivity or value of the information being disclosed is classified as Proprietary (or above).

#### **4.5 Misuse of Department Stationery**

The Department's letter-headed notepaper, printed forms and other documents are to be handled securely to avoid misuse.

#### **4.6 Lending Keys to Secure Areas to Others**

The lending of keys, both physical and electronic, is prohibited. This requirement is also to be noted in employment contracts.

#### **4.7 Complying with Information Security Policy**

All employees must comply with the Information Security Policies of the organisation. Any Information Security incidents resulting from non-compliance will result in immediate disciplinary action.

#### **4.17 Ordering Goods and Services**

Only authorised persons may order goods on behalf of the organisation. These goods must be ordered in strict accordance with the Department's purchasing policy.

#### **4.18 Playing Games on Office Computers**

The playing of games on office PCs or laptops is prohibited.

#### **4.19 Using Office Computers for Personal Use**

Using the Department's computers for private business is prohibited.

#### **4.20 Staff Leaving Employment**

Upon notification of staff resignations, Human Resources Management must consider with the appointed Information Security Officer whether the member of staffs continued system access rights constitutes an unacceptable risk to the organisation and, if so, revoke all access rights.

**5. POLICY REVIEW**

The policy will be reviewed annually or when necessary.

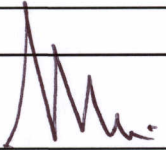
**ENDORSED**

---

---

---

---



**HEAD OF DEPARTMENT**

18/02/09

**DATE**

Note: This policy document is a blue print of the original policy that was approved by MEC Justice Piitso on 12.03.07.