

CONFIDENTIAL



LIMPOPO

PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

OFFICE OF THE PREMIER

Information and Communication Technology Policy

Version 1

Conditions for Service Use

July 2006

CONTENTS

1.	Introduction	4
2.	Purpose	4
3.	Scope of ICT policy	4
4.	Legislation and other policies.....	5
5.	Security management	5
5.1	Management accountability	5
5.2	Individual accountability	6
5.3	Disciplinary action.....	6
6.	Acceptable use	6
6.1	General use and ownership	6
6.2	Security and proprietary information	7
6.3	Internet.....	7
6.4	Intranet.....	7
6.5	Electronic mail.....	8
6.6	Unacceptable use.....	8
7.	Access control	9
7.1	Authentication authorisation.....	10
7.2	Access control security	10
7.3	Access by internal staff.....	10
7.4	Third party access.....	11
7.5	Visitors access.....	11
7.6	Physical access to server rooms.....	11
7.7	Remote access and dial in.....	12
7.8	Temporary access.....	12
7.9	Password policy	12
8.	Classification scheme	13
8.1	Classification of data and systems.....	13
8.2	Classification and responsibilities	13
9.	Information system security.....	14
9.1	Network security.....	14
9.1.1	Trusted points	15
9.1.2	Network segmentation.....	15
9.2	Servers	15
9.3	Workstations.....	16
9.4	Portable computers	16
9.5	Storage removal and disposal.....	16
9.6	Systems management.....	16
9.7	System and system development.....	17
9.8	System Implementation	17
9.8.1	Configuration management	17
9.9	Sensitive information	18
9.10	Disaster recovery and backup	18
9.11	Document security.....	19
10.	Change management policy	19
10.1	Change requests and approval	19
10.2	Change management documentation	19
11.	Risk management, audit and review.....	20
12.	Information technology acquisitions	20

13.	Inventory and assets management	20
14.	Service level agreement	20
15.	Personnel security.....	21
16.	Allocation of Equipments and Software to Users.....	21
16.1	Laptops	21
16.2	Desktops	21
16.3	Printers	22
16.4	Data Projectors	22
16.5	Software licenses	22
16.6	Memory sticks and CDs	22
16.7	Screen Filters.....	22
17.	Repair of equipment.....	23
18.	Loss of equipment.....	23
19.	Call Logging Procedure	23
20.	Registration and termination of user accounts	24
20.1	Account Registration	24
20.2	Account Deletion	24
Annex A :	Abbreviations and definitions.....	25
A.1	Abbreviations.....	25
A.2	Definitions.....	25
Annex B :	OTP information system security policy (register of changes)	27
Annex C :	Letter of promulgation.....	28
Annex D :	OTP policy comment and change proposal form	29
Annex E :	User registration form	30



1. Introduction

Information system security entails the creation of a condition to protect computer hardware, software and data against incidental and/or deliberate unauthorized changes, destruction, disposal, removal and/or disclosure. Information system security is characterized in this policy as the preservation of

confidentiality: ensuring that information and associated assets are accessible only to those authorised to have access,

integrity: safeguarding the accuracy and completeness of information and processing methods, and

availability: ensuring that authorised users have access to information and associated assets when required.

Increasingly, departments and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, viruses, computer hacking and denial of service attacks. Dependence on information systems and services implies that departments are more vulnerable to security threats. Management is hereby setting a clear policy direction and demonstrates support for, and commitment to, information system security through the issue and maintenance of this information system security policy across the department.

2. Purpose

The purpose of this information system security policy is to enable the Office of the Premier [OTP] to apply an effective and consistent level of security to all information systems that process the information of the department.

The OTP seeks to protect its information systems assets from loss and to provide a secure working environment for its employees. The objectives of the policy are to ensure, as far as reasonably possible, that

- a) the assets of the department are secured against loss by theft, fraud, malicious or accidental damage, or breach of privacy or confidence, and
- b) the department is protected from damage or liability resulting from use of its facilities for purposes contrary to the law of South Africa.

This policy applies to employees, contractors, consultants, temporaries and other workers at the OTP, including all personnel that are affiliated with third parties. This policy applies to all equipment that is owned or leased by the OTP.

3. Scope of ICT policy

The ICT policy is intended to support, protect, control and manage departmental electronic information resources. The policy covers information on:

- a) security management
- b) ICT infrastructure management;
- c) certification and accreditation;
- d) application systems acquisition;
- e) system operation;
- f) data security;
- g) system access control and password security;
- h) workstation security;
- i) communication security; and
- j) physical security.

4. Legislation and other policies

The policy is to be read in context of the legislation and standards as listed below.

- a) Minimum Information Security Standards (MISS).
- b) State Information Technology Act (Act no. 88 of 1998).
- c) SACSA/090/1(4) "Communication Security in the RSA".
- d) Protection of Information Act (Act no. 84 of 1982).
- e) Information Act (Act no. 70 of 2002).
- f) Disclosure of Information Act (Act no. 2 of 2000).
- g) Electronic Communication and Transaction Act (Act no. 25 of 2002).
- h) National Intelligent Act (Act no. 39 of 1994).
- i) Copyright Act (Act no. 98 of 1978).
- j) National Strategic Intelligence Act (Act no. 39 of 1994).
- k) National Archives of SA Act (Act no. 43 of 1996).
- l) Public Service Act (Act no. 103 of 1994).
- m) Public Finance Management Act (Act no. 1 of 1999).

5. Security management

The purpose of this subset policy is to describe the minimum security measures that will be implemented and applied to ensure that an effective and consistent level of security management is applied to all OTP systems.

Security management entails all the security aspects of information systems, including the management of security services and mechanisms, which involves the distribution of management information to these services and mechanisms, as well as the collection of information concerning the operation of these services and mechanisms. The aim is to protect systems, data and applications against unauthorised access, and to protect computer hardware, software and data from accidental or deliberate unauthorised changes, destruction, disposal, removal and/or disclosure.

5.1 Management accountability

Information system security will be coordinated and supported at top management level of the OTP. It is the responsibility of senior management to support and ensure that necessary ISS endeavours and initiatives are coordinated and enjoy the necessary privileges.

- a) IS management will be accountable for the implementation of controls that will ensure that the policies as described in this document are adhered to.
- b) An ISS committee that is responsible for all IT security related issues should be put in place. This committee will comprise representatives from management in various business units, ISS specialists and IS management of the OTP.
- c) The ISS committee will address the following security management aspects:
 - i) ISS awareness;
 - ii) Information security organisation, roles and responsibilities;
 - iii) IS risk management;
 - iv) data security;
 - v) outsourcing of IT services; and
 - vi) IS audit and review.

5.2 Individual accountability

Any person using an OTP information system is expected to follow recommended procedures, and to take all reasonable steps to safeguard the information that is handled by that system, as well as any sensitive assets that are involved. All information systems will provide a means by which individual users can be held individually accountable for their actions. The accountability principle is associated with the potential repercussion of individual/group/corporate "liability" and the onus of proving due diligence.

5.3 Disciplinary action

Should any OTP employee be found in contravention of this policy in the execution of his/her duties, he/she would be subject to disciplinary action.

Non OTP personnel found in contravention of this policy will be denied access to the OTP infrastructure.

6. Acceptable use

The purpose of this subset policy is to outline the acceptable use of computer equipment at the OTP. These rules are put in place to protect the employee and the OTP. Inappropriate use exposes the OTP to risks including virus attacks, compromise of network systems and services, and legal issues.

6.1 General use and ownership

- a) While the OTP desires to provide a reasonable level of privacy, users will be aware that the data they create on the corporate systems remains the property of the OTP. All employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of IS resources, this includes personal use of Internet, E-mail, processing and computer equipments. In the absence of such policies, employees must be guided by the OTP's acceptable use policy, and if there is any uncertainty, employees must consult their supervisor or manager.
- b) Without specific written exceptions, all programs and documentation that are generated or provided by employees, consultants or contractors, for the benefit of the OTP, remain the property of the OTP. Responsible management will ensure that all workers providing such programs or documentation sign a statement to this effect prior to the provision of these materials.
- c) The OTP has legal ownership of the contents of all files that are stored on its computer and network systems, as well as all messages that are transmitted via these systems. The OTP reserves the right to access this information without prior notice whenever a genuine business need exists.
- d) All equipment connected to the network of the OTP should run the current approved anti-virus scanning software.
- e) The OTP reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

6.2 Security and proprietary information

- a) The information classification policy and guidelines of the OTP will classify the user interface for information that is contained on Internet/Intranet-related systems as defined. Examples of confidential information include but are not limited to company private, corporate strategies, customer lists and research data.
- b) Employees will take all necessary steps to prevent unauthorised access to this information.
- c) Providing information about, or lists of OTP employees to parties outside the OTP without prior approval is prohibited.

6.3 Internet

Connection to the Internet introduces new opportunities for new risks. In response to the risks, this policy describes the policy of the OTP regarding Internet security.

- a) Access to the Internet will be granted to only those employees that have a legitimate need for such access. The ability to surf the Web and engage in other Internet activities is not a fringe benefit to which all workers are entitled. If a worker does not have sufficient Internet access, the user needs to apply for access formally through the respective manager and approved by the Manager IT support.
- b) All Internet connections will be via the approved Internet service provider of the OTP. Any other connections are prohibited.
- c) All users will authenticate themselves at an OTP internal Web proxy server before gaining access to the Internet. This authentication process will be achieved by logging on to the Internet via user name and password system.
- d) To protect the OTP from profane material and to minimise the use of bandwidth, all Internet usage will be monitored by Web content filtering software.
- e) Misrepresenting, obscuring, suppressing or replacing the identity of a user on the Internet or any OTP communication systems is forbidden.
- f) Users will not publicly disclose internal OTP information via the Internet, which could adversely affect the OTP, customer relations or public image.
- g) OTP content filtering software will prevent users from connecting to certain non-business web sites. All web sites that contain sexually explicit, profane and other potentially offensive material will be blocked out via the proxy server.
- h) At any time and without prior notice, OTP management reserves the right to examine Web browser cache files, Web browser bookmarks and other information that is stored on or passing through the computers of the OTP. Such management access assures compliance with internal policies, assists with internal investigations and assists with the management of the OTP.

6.4 Intranet

- a) All OTP network users will have access to the OTP Intranet.
- b) The OTP Intranet is intended to facilitate more efficient and more effective ways for OTP staff to communicate and conduct business. Like other OTP information systems, because it is intended for business purposes, personal use is permitted only if the approval of a department manager has first been obtained.
- c) Although the Intranet is an informal internal communications environment, the laws for copyrights, patents, trademarks and the like still apply.
- d) All information that is posted to the OTP Intranet will have a designated "owner" (responsible manager). Contact information for this owner will be clearly indicated on the page on which the information appears.

6.5 Electronic mail

- a) As a productivity enhancement tool, OTP encourages the business use of electronic communications. Electronic communications systems, and all messages that are generated on or handled by electronic communications systems, including backup copies, are considered to be the property of OTP.
- b) OTP electronic communications systems generally will be used only for business activities. Employees are reminded that the use of corporate resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.
- c) Misrepresenting, obscuring, suppressing or replacing the identity of a user on an electronic communications system is forbidden. The user name, electronic mail address, organisational affiliation and related information that are included with electronic messages or postings will reflect the actual originator of the messages or postings.
- d) OTP management will when required monitor the content of electronic communications. Content and usage of electronic communications will be monitored to support operational, maintenance, auditing, security and investigative activities.
- e) Recognising that some information is intended for specific individuals and will not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. OTP-sensitive information will not be forwarded to any party outside OTP without the prior approval of a local department manager.
- f) Users will be allocated fixed size electronic mail space on the server.
- g) Messages that are no longer needed for business purposes should be periodically cleaned by users from their personal e-mail boxes. Electronic messages that are stored in user inboxes will be backed up and deleted by the systems administration staff after a six-month grace period. This will assist to reclaim scarce storage space, and will also simplify records management and related activities.
- h) All Email messages sent from OTP mail servers will have the Disclaimer Notice:
Privileged or confidential information may be contained in e-mail messages. If you are not the intended recipient of the message, you may not copy or deliver the message to anyone. You should destroy the e-mail and notify the sender thereof. Please advise immediately if you or your employer do not consent to e-mail messages of this kind. All messages reflect the opinions of the original authors and are in no way reflective of the official business of the OTP.

6.6 Unacceptable use

Under no circumstances is an employee of the OTP, consultant or contractor authorised to engage in the following:

- a) accessing, including browsing, downloading or forwarding material that is obscene, offensive and/or of a sexual nature, in any format - whether in word or audio file;
- b) accessing, including browsing, downloading or forwarding material that is racist, discriminatory, homophobic, incites hatred or promotes violence;
- c) accessing, including browsing, downloading or forwarding material that contravenes any applicable legislative and regulatory requirements;
- d) downloading, copying and sending anything that constitutes an infringement of copyright, including images, music files and video in any format;
- e) contributing to Internet newsgroups or chat rooms without being authorised to do so;
- f) signing up to e-mail bulletin boards or news groups that require payments from the OTP, unless specific written authorisation was obtained for such a business-related cost;
- g) Making any personal comment outside the OTP from a departmental account, except where authorised to do so as part of the duties of the employee;
- h) making any defamatory or derogatory comments;
- i) Creating or forwarding chain e-mail letters, or any advertising material or any non-business-related material, except where authorised to do so as part of employee's duties;

- j) using the Internet for personal gain or profit in the time of the Department, or soliciting employees of other department for any non-departmental business enterprise;
- k) making fraudulent offers of products, items or services;
- l) Making statements about any warranties or guarantees that are offered by the OTP, unless it is as a part of the duties of the employee;
- m) Transmitting externally any OTP confidential information without the appropriate approval from line management;
- n) on receiving any unacceptable material, a user must delete such material immediately, regardless of content. Failure to delete such material will mean that the employee accepts and owns the material. The employee is advised to instruct the sender to stop sending such material and, should the sender continue to do so, IT management should be advised as soon as possible so that appropriate action can be taken;
- o) Any material that contains graphical images and multimedia files use significant Departmental IT storage and system resources, and should only be stored, scanned or incorporated in electronic messages for legitimate business purposes.
- p) Any activity that is illegal under local, state or international law while utilising IT resources that are owned by the OTP;
- q) Violating any person or company that is protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the OTP;
- r) introducing malicious programs into the OTP network or server (e.g. viruses, worms, Trojan horses, e-mail bombs etc.);
- s) effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are in the scope of regular duties. "Disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service and forged routing information for malicious purposes;
- t) executing any form of network monitoring that will intercept data that is not intended for the host of the employee, unless this activity is a part of the normal job/duty of the employee;
- u) revealing any account passwords to others or allowing use of the account of the employee by others. This includes colleagues, family and other household members when work is being done at home;
- v) using the OTP computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the local jurisdiction of the user;
- w) port scanning or security scanning is expressly prohibited unless prior notification to appropriate IS management is made; and
- x) All connection to the internet needs to be shut down at the end of the business day. Continuous sessions to the internet are prohibited, users needs to ask permission first.

7. Access control

The aim of this subset of the policy is to outline the regulatory requirements and conditions for allocation of access to systems and computer equipment at the OTP. These rules are put in place to protect the employee and the OTP. Inappropriate access to systems and information exposes the OTP to risks and compromise integrity, availability and confidentiality of systems and data that are processed.

It is the responsibility of personnel that are designated as the owners of respective IS resources to ensure that access to these resources is granted in accordance with the policy.

7.1 Authentication authorisation

- a) Any request for IS resource access will be accompanied by an authorisation letter from immediate management.
- b) Users will have a unique user name and password to identify them on the systems. All user names and passwords will conform to the naming convention of the OTP and approved password standards.
- c) Authentication to IS resources will be logged and reviewed at all system levels. The level of security that is required at that level of access will determine the strength of the authentication method that is used.
- d) Authentication scheme that is used or to be used will be reviewed based on the security requirements of resources that are being accessed. The security requirements of the resource access will dictate the appropriate authentication scheme to be used.

7.2 Access control security

- a) Physical access
Physical access to IT resources will be controlled in accordance with the physical access policy.
- b) Logical access
Logical access to network and IT resources will be granted on a need to know basis. The following are the requirements for granting access to the systems:
 - i) business motivation and approval from appropriate management; and
 - ii) approval of resource owner.
- c) Remote Access
The Office uses a software tool to allow IT technical staff to access user's machines remotely to solve user's problems. From Tool's central management console, IT staff can take control of any desktop in the OTP (with the user's permission), effectively seeing what the user sees, which simplifies troubleshooting. The user will be prompted to allow the technician to access his/her machine remotely. The user must respond to the request with a yes or a no. A no means the technician will not gain access to the user's machine whilst a yes give permission. That is, users are assisted in a short space of time because there won't be any need to go to the physical location of the machine that needs to be worked on. The tool keeps a log in the central management console with records indicating what was done, when it was done and to which machine and who did it.

7.3 Access by internal staff

- a) Only authorised personnel will be given access to the IS resources.
- b) Access to resources will be granted after an approval from appropriate management has been received.
- c) Access to data, information and system resources will be granted on a need to known basis, accompanied by a business motivation/need to access such resources.
- d) Access to IT resources will be logged and monitored on regular basis.
- e) All of the information systems privileges of the OTP will be promptly terminated immediately when an employee ceases to provide services to the OTP.
- f) The designated owner of the information asset will take responsibility for all access that is granted. The owner of the information resource will ensure that all access to the resource that is granted is appropriate and justified.
- g) The IS management of the OTP reserves the right to revoke the access privileges of any user at any time. Conduct that interferes with the normal and proper operation of the information systems of the OTP, which adversely affects the ability of others to use these information systems, or which is harmful or offensive to others, will not be permitted.

7.4 Third party access

Access to the ICT facilities of OTP offices by non-OTP third parties shall not be provided unless the appropriate measures have been implemented and a contract has been signed defining the terms of the access. Third parties shall be subjected to all the requirements of this policy.

- a) Third party organisations will be given access privileges to the IS resources after the responsible management of the OTP has determined that they have legitimate business needs. These privileges will be enabled only for the time period that is required to accomplish approved tasks.
- b) Any third party organisation that is given access to the IS resources of the OTP will have signed a non-disclosure agreement to protect the confidentiality of systems and information they access.
- c) Third party access will be monitored and reviewed on a regular basis.
- d) The IS management of the OTP reserves the right to revoke the privileges of any third party at any time. Conduct that interferes with the normal and proper operation of the information systems of the OTP, which adversely affects the ability of others to use these information systems, or which is harmful or offensive to others, will not be permitted.
- e) The OTP will allow only employees of third party organisations, which are approved in advance by the OTP to access the network connection or any OTP-owned equipment. The third party organisation will be responsible for ensuring that its authorised employee is not a security risk. On the request of the OTP, the third party organisation will provide any information that is reasonably necessary for the OTP to evaluate security issues that relate to the employee of any authorised third party.
- f) The third party organisation will notify the OTP, in writing, promptly about a change in the user base for the work that is performed over the network connection, or whenever, in the opinion of the OTP, a change in the connection and/or functional requirements of the network connection is necessary.

7.5 Visitors access

- a) No visitors will be allowed access to any of the IS resources of the OTP, unless approval from management is obtained. The hosting party/person will be responsible for ensuring that required approval is obtained before any access is granted.
- b) Visitors will not be allowed any access to the computer room, unless accompanied by the hosting personnel and monitored by personnel that are responsible for the computer room. Reasons for access will be justified and approved by management.
- c) All visitors to the OTP will be escorted from the main entrance of the building to their destination, and escorted from the building after their visit.

7.6 Physical access to server rooms

- a) Physical access to the computer room, in which servers and other IT equipments are located, will be protected by an access control system. The system will be implemented with the necessary control measures.
- b) Physical access to IS resources will be granted in accordance with a formally defined procedure. Only authorised personnel will have physical access to IT equipments. Line management will be responsible for approving and allocating access to resources.
- c) All access to secure areas will be authorised and logged. An audit trail will be securely maintained.
- d) Humidity and temperature controls will be regularly monitored. The computer room will be secured from all environmental hazards like fire, flooding, damage and theft.
- e) Movement of computer equipment in and out of the computer room will be strictly controlled.

- f) The security of mobile and portable computing equipment is the responsibility of the users. The users will ensure that they adhere to best practices in securing their portable computers.

7.7 Remote access and dial in

- a) Secure remote access will be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass phrases.
- b) At no time should any of the employees of the OTP provide his/her login or e-mail password to anyone, not even family members.
- c) The employees and contractors of the OTP with remote access privileges will ensure that OTP-owned or personal computers or workstations, which are remotely connected to the network of the OTP, are not connected to any other network at the same time.
- d) The employees and contractors of the OTP with remote access privileges to the corporate network of the OTP will not use private e-mail accounts (i.e. Hotmail, Yahoo, AOL), or other external resources to conduct official business of the OTP, thereby ensuring that official business is never confused with personal business.
- e) Routers for dedicated lines (ISDN) that are configured for access to the network of the OTP will meet minimum authentication requirements of CHAP (Challenge Handshake Protocol).
- f) Reconfiguration of the equipment of a home user for the purpose of split-tunneling or dual homing is not permitted at any time.
- g) All hosts that are connected to the internal networks of the OTP via remote access technologies will use the most up-to-date antivirus software. This includes personal computers. Third party connections will comply with requirements as stated in the *third party agreement*.
- h) Personal equipment that is used to connect to the networks of the OTP will meet the requirements of the OTP-owned equipment for remote access.
- i) Organizations or individuals that wish to implement non-standard remote access solutions to the OTP production network should obtain prior approval from remote access services and ISS.

7.8 Temporary access

- a) No temporary access to IS resources will be granted without authorisation from the responsible management that is accompanied with justification for access from the hosting person.
- b) Temporary access that is given to contractors, temporary staff and visitors will be revoked immediately when the duration of the contract or visit expires or they leave the premises.

7.9 Password policy

Passwords shall be individual and exclusive, allocated with discretion, and it shall not be disclosed without authorisation. Quality passwords with a minimum length of 8 characters shall be selected. Unauthorised disclosure shall be considered a breach of security and an infringement of Sections 3 and 4 of the Protection of Information Act or any other applicable legislation.

- a) All user-chosen passwords for computers and networks should be difficult to guess. Words in a dictionary, derivatives of user-Ids, and common character sequences such as "123456" should not be employed. Likewise, personal details such as the name of a spouse, license plate, identity number and birthday will not be used, unless accompanied by additional unrelated characters. User-chosen passwords should also not be any part of speech. For example, proper names, geographical locations, common acronyms and slang will not be employed.

- b) All user-chosen passwords will contain at least one alphabetic character and may include non-alphabetic characters. Non-alphabetic characters include numbers (0-9) and punctuation. The use of control characters and other non-printing characters is discouraged, as it will inadvertently cause network transmission problems or unintentionally invoke certain system utilities.
- c) The display and printing of passwords will be masked, suppressed or otherwise obscured, so that unauthorised parties will not be able to observe or subsequently recover it.
- d) All users will be automatically forced to change their passwords at least once every 90 days.
- e) The initial passwords that are issued by a security administrator will be valid only for the first online session of the involved user. At that time, the user will be forced to replace the password before any other work can be done.

8. Classification scheme

The purpose of this policy is to give detailed guidelines for classification of IT resources and information processed. This policy applies to all information, systems and computer equipment that are owned by the OTP.

It is the responsibilities of resource owners to ensure that resources and their responsibilities are classified accordingly.

8.1 Classification of data and systems

Systems and data will be divided into four sensitivity classifications with separate handling requirements: RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET. This standard data sensitivity classification system will be used throughout the OTP. These classifications are defined below.

- a) **RESTRICTED** is the classification that is allocated to all information that may be used by malicious/opposing/hostile elements to either harm activities or inconvenience the department or an individual.
- b) **CONFIDENTIAL** is the classification that is allocated to all information that may be used by malicious/opposing/hostile elements to harm either the objective and functions of the department or an individual.
- c) **SECRET** is the classification that is allocated to all information that may be used by malicious/opposing/hostile elements to disrupt the objective and functions of the department and an individual.
- d) **TOP SECRET** is the classification that is allocated to all information that may be used by malicious/opposing/hostile elements to neutralise the objective and functions of the institution and/or state.

8.2 Classification and responsibilities

It is the responsibility of the user to

- a) know his/her security clearance level and to understand the rights and limitations that are associated with that clearance,
- b) ensure that all the data that he/she works with is correctly classified,
- c) ensure that he/she understands the restrictions that are associated with the data that he/she works with, and
- d) ensure that all the data that he/she works with is housed and protected appropriately.

9. Information system security

This policy is intended to give necessary direction regarding the protection of the availability, integrity and confidentiality of information assets and systems of the OTP.

9.1 Network security

This policy applies to

- a) any networks to which the OTP network equipment is connected,
- b) all equipment that is connected to the networks as mentioned above,
- c) data in transit over any of the networks mentioned above,
- d) network administrators and service providers that manage the equipment,
- e) project leaders that require new equipment to be connected to the network, and
- f) all users that utilise equipment that is connected to the network.
- g) Any service provider that accesses OTP network to render service.

This includes, but is not limited to

- a) the user LAN,
- b) the server LAN,
- c) WAN connections to remote sites, and
- d) Satellite connections.

This policy will also apply to all equipment that is connected to the networks as mentioned above, and all the OTP employees that use any of this equipment. All the OTP network equipment (routers, servers, workstation, laptops etc.) will be classified according to the standard of the OTP classification scheme and placed in a network segment that is appropriate to its level of classification. Access to network segments will be controlled in an appropriate manner. Whenever data travels over a network segmentation of a lower security classification, the data will be protected in a manner that is appropriate to its classification level.

- a) All physical network segment carriers will be classified.
- b) All data that travels on the network will be classified.
- c) All users that use network equipment or request data over the network will be assigned a level of clearance according to the same system.
- d) It is the responsibility of the person that is designated as equipment owner to have all equipment under his/her control classified.
- e) Classification will be done in consultation between the owner (or an assigned representative) and the IS manager, but the final decision will lie with the security officer.

9.1.1 Trusted points

- a) The trusted point that is used to segment two networks will be appropriate for the network with the highest security level.
- b) The default behaviour of a trusted point will be to deny all traffic between the network segments that it protects.
- c) At the discretion of the OTP information security manager, the default behaviour of the trusted point will be to allow all traffic from the network with the higher security level while denying all traffic in.
- d) At the discretion of the OTP information security manager, the trusted point will be configured to allow specific data into the network with the higher security level.
- e) All trusted points will be completely under the control of the information security manager. Access to any trusted point will only be granted with the explicit permission of the information security manager, and under his/her close supervision.
- f) Whenever there is a connection that skips one security level, the strong user level control will be used. Even if strong user control is used, a connection will never skip more than one security level.

9.1.2 Network segmentation

- a) A network segment can only be classified as another security level with the approval of the OTP information security manager.
- b) Its new level of classification will be recorded in the change management document, and all divisional heads will be notified.
- c) Wherever a network segment connects to another network segment with a different security level, an approved trusted point should control the connection between the two networks. A trusted point is equipment that is capable of regulating the flow of traffic between two network segments in a manner that is appropriate to the classification of the networks.
- d) No network equipment will be connected to a network segment that is not of the same security level.
- e) The OTP Information Security Manager can choose to segment two networks of the same security level.

9.2 Servers

- a) All servers that host data and applications will be located in a physical secure environment, in which access is strictly controlled. A server access register will be kept.
- b) Logical access to servers will be allocated on a need to know basis, in accordance with the access control policy of the OTP.
- c) All servers must be loaded and protected with the latest approved antivirus software. Updates will be implemented on a regular basis for patches, signature and upgrades.
- d) Only an authorised administrator will be given administrative rights on the servers. The administrator password will be kept a secret, and only nominated personnel at the discretion of management will have access to the password.
- e) Servers will be backed up in accordance with the backup policy and procedures as outlined by the disaster recovery and backup policy, paragraph 8.10.
- f) Changes or updates to software or application systems will also be recorded in a software update register that will be kept in the server room.

9.3 Workstations

- a) All workstations will be located in a physically protected environment, in which access control measures are in place and applied consistently. It will be ensured that unattended equipment has appropriate security protection.
- b) Sensitive data will not be stored on local hard drive of workstations. All sensitive data that is processed using workstations will be saved on a secure network drive on a server.
- c) All workstations should be loaded and protected by the latest approved antivirus software.
- d) It is the responsibility of the workstation user to ensure that appropriate security measures and practices are adhered to. Protection of the data that is stored on workstations is the responsibility of the workstation user.
- e) Users will not leave their workstations unattended while accessing or processing information without appropriate protection like password-protected screen savers.
- f) Workstations that are used to access sensitive information like finance or human resource data that is classified to be highly sensitive, will be protected by means of both a password-protected screen saver and a BIOS password.
- g) Users will not share workstation passwords and user accounts with anyone.
- h) It is the responsibility of the workstation user to ensure that his/her workstation is adequately protected from logical threats as well as physical environmental threats.
- i) All users will log off from their workstations at the end of each business day.

9.4 Portable computers

- a) All portable computers (e.g. laptops, palmtops etc.) that contain classified data will be equipped with an access control and encryption capability that meets the agreed to security standard.
- b) Users need to ensure that their portable computers are loaded with the latest antivirus software by connecting it weekly to the network and updating its platforms.
- c) Users also need to ensure that all data is backed up to the home drive of the network.
- d) Any third party laptops connecting to the network must obtain approval from relevant Manager before down loading any OTP information
- e) Stolen or lost portable computers must be reported to Information Services Manager immediately.

9.5 Storage removal and disposal

If a hard disk that contains secret and top secret information needs to be removed from the OTP premises, it will be formatted before being sent for repairs, by using approved hard drive overwriting software and the files will have to be saved and kept in a safe place before the computer is released from the OTP.

If a hard disk cannot be accessed, it will be presented to OTP GITO unit to be physically destroyed. Storage media (i.e. stiffies, CDs, hard disks) will be removed from equipment before being sent out for repairs.

9.6 Systems management

- a) A mechanism will be established to ensure that the integrity of existing data can be assessed regularly. The monitoring of data integrity will be done according to a predetermined year plan.
- b) Controls to prevent the deliberate input of corrupt data or the incidental loss of correct data, and to ensure that transactions meet the requirements of accountability and audit ability, will be implemented.
- c) Processing control measures will be implemented to detect and correct errors during the processing phase and to validate the integrity of the data.

- d) Detailed error handling procedures will be established.
- e) Output control measures to verify the accuracy and integrity of processed information, as well as the correct distribution of outputs, will be implemented.
- f) A backup system, which makes the recovery of data possible, will be in place. Backup and production data will be stored in geographically separate locations. The content of backup copies will be nullified before the medium (disc or tape) is used for other purposes.
- g) A data disposal system will be established to ensure that archived data is disposed of in an orderly manner. Disposal will be performed in compliance with the National Archives of SA Act. Measures will be in place to ensure that sensitive information is not compromised in the disposal process.
- h) Only authorised in-house developers and contractors with the appropriate security clearances will do system maintenance on hardware and software. All OTP system users will ensure that computer hardware and software are handled and used according to specifications.

9.7 System and system development

The policy applies to all system developments in OTP.

- a) A senior manager of the particular business line will determine the need and alignment of the development requirement to the overall information system strategy of the OTP, as well as the business requirements of the OTP.
- b) Appropriate management at OTP will approve all system development initiatives.
- c) Security requirements of a development will be determined and the risks identified before the system is developed.
- d) All systems that are developed for the OTP will be developed in accordance with the approved departmental model SDLC. Security requirements of the system will be established.
- e) Prior to live implementation of a system, an individual, independent of the development team, will review the security of the system. No system will be put on production without testing and sign-off by the head of the development team, in consultation with the system owner who will ensure that all aspects of the SDLC were followed.
- f) System documentation will be complete and handed to the system owner before a system can be put in the production environment.

9.8 System Implementation

All computer hardware and software will be implemented in terms of an implementation plan compiled by the IS unit in collaboration with SITA. The implementation plan will also address the activities related to the coordination and implementation of the security measures and specify acceptance criteria to be met before the system is put into operation.

9.8.1 Configuration management

In order to prevent fraud, sabotage, espionage, subversion and actions that endanger security, effective configuration management will be applied to systems that are in operation. Configuration items of an OTP system will be uniquely identified and controlled in order to determine and control the influence of a change to a configuration item on the system and system interfaces.

- a) Configuration management must ensure that any additions, omissions or changes that are made to the system are authorised and do not compromise the set security measures.
- b) Computer hardware and software will be implemented in accordance with an implementation plan. The implementation plan will address the activities that are related to the coordination and implementation of the security measures, and will specify acceptance criteria to be met before the system is put into operation.

- c) Complete, updated manuals/documentation will be available to operators, programmers, system analysts, users and auditors, as applicable. Backup copies will be made of all electronic documentation and stored in a geographically separate location in a safe.
- d) The use of system utility programs (e.g. monitoring/sniffing tools/debugging tools) that might be capable of overriding system and application controls will be restricted and tightly controlled.

9.9 Sensitive information

- a) Sensitive information will not be stored on unsecured media like local drives of workstations, OTP disks and the e-mail system.
- b) If needed, encryption technologies will be used to encrypt sensitive data that is stored on the network, e-mail and any electronic media.

9.10 Disaster recovery and backup

A disaster is any event/occurrence that will render the normal operation of computer systems unusable that could result in the loss of data or irretrievable corrupted data, corrupt systems, damage to hardware etc. Events that could lead to a disaster occurring are the following:

- Power cuts/dips, lack of UPS or backup power generators, faulty air conditioner
- Fire, Water, Natural disaster
- Virus attacks, no access control mechanisms, theft

To protect the IT environment of the OTP, it is important to ensure that regular backups of the critical information stored on the network servers as well as the information on selected workstations are carried out. In case of a disaster, critical information should be recovered through backups with minimal loss of time. Therefore, the purpose of the document is to give the framework on which the backup policy and procedures as well as recovery methods and procedures will be based.

The OTP will have a documented disaster recovery plan, approved and endorsed by senior management of the OTP. The disaster recovery plan will be communicated to all parties that are responsible for the management and operations of the IT infrastructure. The recovery plan will at least be classified CONFIDENTIAL.

Data backup procedure will be established and adhered to for all the information systems and operations. Data backup devices will be kept in a safe off site environment in a separate building, which can be accessed with ease by authorised personnel when needed.

The backup schedule should be made such that it ensures that, on any given day, the data is current as of:

- The previous day (Yesterday)
- Each Friday of the current month
- The last Friday of each month, for up to three years
- The last Friday (or any other chosen Friday) of each year the process has been in place

The backup schedule should be as follows:

- Daily incremental backups should be done every evening after hours
- Weekly full backups should be done every Friday evening after hours
- The monthly full backup, is the one done on the last Friday of the months

The tapes should be recycled in the following manner:

- Daily incremental backup tapes should be retained to a minimum of up to seven days
- Weekly full backups tapes should be retained to a minimum of two five weeks
- The monthly full backups should be retained for a minimum up to 36 weeks
- Yearly backups should be retained for five years

Disaster recovery plans will be tested, evaluated and continually updated.

9.11 Document security

- a) All documents, manual files and printouts will be classified in accordance with the information security classification scheme of the OTP. It is the responsibility of the person accessing or using the documentation to understand the sensitivity of the material that is contained in the documentation.
- b) Access to highly classified documents will be strongly controlled. Authorisation from the appropriate owner will be obtained. It is the responsibility of the owner to ensure that all access requirements to the documentation are satisfied as outlined by the classification requirements and security status of the recipient.
- c) Documents and sensitive data files will be kept in a safe environment. A backup procedure for all manual files and documents that are critical to the business of the OTP will be put in place to ensure the availability of information in the manual file system.
- d) Sensitive documents will not be printed on network printers that are accessible to everyone.
- e) Requests for access to highly classified documents will be scrutinized and logged if granted. All sensitive documents that are accessed will be accompanied by a business motivation and authorisation.
- f) Systems and network documentation will be classified as SECRET. Access to this documentation will be strictly controlled. Only people that are authorised to view, change or modify the system configurations will be allowed access to the documentation.
- g) Systems and network documentation will be kept and locked away in a safe place.

10. Change management policy

This policy applies to the following changes to IT resources:

- a) changes to network topology, new network equipment installation, upgrade to the network, network protocols, configuration;
- b) application and system configuration changes; and
- c) database changes.

10.1 Change requests and approval

- a) A formal change management process will be established, including approval of change requests.
- b) All changes must be made in accordance with an approved change management process of the OTP.
- c) All approved changes will be monitored to ensure that it is implemented according to specification.
- d) The effects of changes will be analysed before changes are approved and implemented.
- e) It is the responsibility of Information Service Management to ensure that all approved changes to critical IT resources are at a minimal level of risk to the IT infrastructure.

10.2 Change management documentation

- a) Documentation that reflects all significant changes to production, computer and communication systems at the OTP will be prepared within a week from the time that a change took place.
- b) This documentation will reflect the proposed change, management approval, and the way in which the change was performed.
- c) Documentation will be classified as CONFIDENTIAL. Only authorised personnel will have access to the documentation.



11. Risk management, audit and review

- a) The head of the department will conduct a comprehensive risk analysis to determine the risk of the unauthorised disclosure or loss or disruption of information that requires protection against unauthorised disclosure or loss or disruption.
- b) The OTP reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
- c) Users, system owners and identified participants will cooperate with the audit team to accomplish the desired goal.
- d) The audit findings and recommendations will be prioritised, and responsibility for implementation will be assigned.
- e) Audit logs will be kept for all systems and applications. System administrators will review these logs on regular basis. All suspicious activities that are identified will be reported and investigated.
- f) All systems administrators must review these logs on a regular basis. All suspicious activity must be reported.

12. Information technology acquisitions

- a) Procurement of hardware and software will be done in accordance with the approved procedure of the OTP information technology procurement.
- b) All ICT purchases will be reviewed and approved by the Information Technology Committee or DGITO.
- c) The security requirements of newly acquired software/hardware will be established in consultation with the OTP IS unit.
- d) The IS unit will advise on and approve all ICT and related procurements by providing control and direction with regard to ICT purchases in the OTP.

13. Inventory and assets management

- a) An inventory of all ICT resources will be kept by means of an inventory register by the Asset Management unit. Items in the inventory register will be uniquely identified by means of an asset number/tag number.
- b) The Asset register will be updated when new hardware/software is procured. It is the responsibility of the assets management component to ensure that all newly procured items are included in the inventory register.
- c) Equipment and software that are no longer used will be written off from the asset register by the asset management unit.

14. Service level agreement

The OTP have entered into an agreement with SITA and other service providers for all the IT services at the OTP. The aspects below will be addressed.

- a) What arrangements are in place to ensure that all parties involved in the service level agreement are aware of their security responsibilities?
- b) How the integrity and confidentiality of the ICT assets of the OTP are to be maintained and tested.
- c) What logical and physical controls will be in place to restrict the business information of the OTP to authorised users?
- d) The scope of services to be delivered.
- e) The duration of the service level agreement.
- f) Failure to meet the requirements of the agreement by any of the parties that are involved.
- g) Right to independent audit of the services that are delivered.

15. Personnel security

- a) The employees of the OTP that access information systems, and the data that is processed by the systems will meet the necessary security requirements as determined by the sensitivity of the information that is accessed. The OTP will provide the security requirements with any access.
- b) Access to the systems and data will be immediately terminated as soon as evidence to non-compliance with the security requirements is gathered.
- c) All employees of the OTP will have approved job descriptions with IS security roles and responsibilities included.
- d) All employees will sign a secrecy declaration and non-disclosure form not to disclose or reveal any sensitive information that they are privileged to access as a result of their job assignment to any unauthorised personnel.
- e) Staff disclosing information to the media and press will do so with permission granted at an appropriate level of management in the OTP.

16. Allocation of Equipments and Software to Users

The procedure for acquiring equipment such as PCs, laptops, printers, etc. is as follows:

- a) A User need to complete ICT requisition form to request for the equipment/software/services he/she needs with the motivation why the equipment is needed. The request must be endorsed by their Senior Manager of the requesting staff member and must be forwarded to DGITO.
- b) The DGITO presents to the ITC that to and approve/disapprove the applications. The DGITO will approve requests on the standard equipment list as delegated by the ITC.
- c) The equipments/software/services are procured.
- d) The equipment/software is delivered to Asset Management who receives and allocates a tag number.
- e) A list of user/s who requested the equipment/s is compiled by the DGITO and the equipment/s is delivered to the user/s by Asset Management, each user must sign for the equipment he/she received.
- f) Each User log calls for IT staff configure the equipments to access infrastructure of the Office.

16.1 Laptops

Laptops are normally allocated to Senior General Managers, General Managers, Senior Managers, the Director-General and the Premier of the department. However, notebooks are allocated to some staff members on request who by their nature of work are required to do Computer related office work outside the department premises. The GITO office will keep a loan notebook, to be loaned to officers without laptops who are required to do presentations/work outside the department premises. The notebook will be loaned and returned after use. Requests for such a loan will be made with GITO office at least two days before the notebook will be required.

16.2 Desktops

Desktops are allocated to all the other staff members who occupy an office and are required use a computer in their work.

16.3 Printers

Senior Management will be provided with a mono laser printer which will be shared with the Personal Assistant in their offices. All other staff will be connected to network mono laser printer next to their offices. All business units will be provided with at least one mono laser printer.

Colour laser printers will be provided to Senior General Managers, the DG and some General Managers. All other managers will be connected to colour laser printers that will be located in the workstation/Photostat rooms. Managers are required to control the usage of colour printing by their subordinates in order to save costs on the replacement of colour toners. Printing on all network printers will be monitored with monitoring tools to determine the usage of printing by each Business Unit.

16.4 Data Projectors

The data projectors are centralised in Asset Management and will loaned whenever needed. This was necessitated by the fact that data projectors are not used by business units on a daily basis. Some units keep these equipments and use them once in a year which becomes inefficient in the utilization of these devices. The department ends up buying many of these equipments that accumulated dust in the cabinets. There are currently five data projectors that will be made available on request and returned after use. One will be kept in the GITO office to accommodate immediate needs but the rest will be kept in Asset Management. Requests for data projectors should be made with the PA in GITO at least two days before and she/he will liaise with asset Management if more are needed.

16.5 Software licenses

The GITO will manage and control all software that is running in the department's network. Original copies of software will be kept in the GITO Office. The number of these licences will be kept and managed by the unit. Users who need software to be loaded on their machines must request permission from the unit. No unauthorised software will be allowed on the equipments of the department. If such software is discovered it will be uninstalled from the users machine. Users are therefore requested to notify the GITO unit of any software that is running on their machines that is not licensed to the department. A software licence register will be kept by the IT office and licences are renewed upon expiry if they are still being used.

16.6 Memory sticks and CDs

Memory sticks will be allocated to staff that have to carry information in transit, and are therefore not regarded as backup storage medium. Each user will be allocated with one memory stick. Memory sticks will be allocated to the DG, Senior General Managers, General Managers and Senior Managers and managers. They are also allocated to users in Service Delivery Unit and Communications as well as those users with laptops that don't have stiffy drives. Memory sticks will also be allocated to users on request endorsed by their managers. CDs are allocated to staff members as per need.

16.7 Screen Filters

All desktop users need to have screen filters. Users without screen filters should request to be provided.

17. Repair of equipment

Equipments break or malfunction at times while being used. Such equipments must be reported to the GITO stating the symptoms of the malfunctioning or breakage. The GITO will engage service providers to fix the problem. The affected user will be loaned with equipment that is still in working order if one exists. Users are requested to be patient whilst the equipment is taken for repairs. Some repairs take up to a month or two to get fixed since spare parts might have to be ordered overseas.

If the equipment is a computer the GITO will try to retrieve the data if possible and store it securely. If successfully retrieved, the data will be cleaned from the machine before it goes for repairs. If the machine cannot be started, and data cannot be retrieved, the machine will be sent out for repairs as is, although there is no guarantee that the data will be retrieved after repairs. The equipments will be returned to the users after they have been repaired. The technical staff will reinstall the software and the data of the user to the machine.

18. Loss of equipment

An employee who loses an IT equipment belonging to Office will follow this procedure:

- a) Report the loss to the police station and obtain a case number.
- b) Provide the case number to Security and Risk management in the Office
- c) Security and Risk to investigate the matter and produce a report that must be sent to the DTC. The report will indicate whether the loss is a result of negligence by the staff member.
- d) The decision of the DTC will be binding based on the findings from security and risk management.
- e) If the findings indicate negligence by the employee, then the employee must replace the equipment, the relevant SBU manager must ensure that the employee complies. If the employee fails to comply, then an amount equivalent to the value of the equipment will be deducted from the employee's salary.

19. Call Logging Procedure

Users are expected to log a call whenever the equipments they use, are not working or malfunctioning.

- a) The user identifies the problem and prepares the following: equipment type, model, serial number, equipment tag number, the user's name, office number and location.
- b) The user calls the call desk, number 0800115575 and a call is opened on the ARS system. The user will be provided with a reference number, which he/she must keep safe.
- c) The technician will attend to the user to solve the problem.
- d) If the problem is solved, then the call is closed otherwise it must remain open until the problem is solved.
- e) If the problem is not attended to the user must inform the DGITO, the next business day and must provide the reference number of the call logged.
- f) If the equipment is broken the equipment will be sent for repairs

20. Registration and termination of user accounts

20.1 Account Registration

- a) The user completes a User Registration form obtainable from Human Resources.
- b) The completed and signed form is forwarded to the DGITO.
- c) The user accounts are created to access the LAN, email and relevant applications.

20.2 Account Deletion

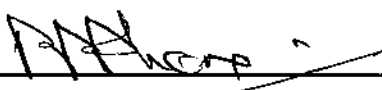
- a) When a user leaves the services of the Office, HR must inform the DGITO using the User Registration form indicating the termination date.
- b) The user's machine is backed-up and the data is erased.
- c) The user accounts are terminated.
- d) The user's mail account is removed from the address book.

20.3 Lifespan of Computer & Disposal

The lifespan of a computer (both a desktop and laptop) is three years according to international standards. The computer equipments that are more three years will be identified for disposal and collected and stored in one location. The equipments will be cleaned of the data they had. After being cleaned, the equipments will be disposed. The disposal method will be determined by Asset management. The disposed equipments will be written off the asset register.

21. Approval

The Information and Communication Technology Policy comes into operation on a date to be determined by the Accounting Officer



7 **DIRECTOR GENERAL**



EFFECTIVE DATE



Annex A : Abbreviations and definitions

A.1 Abbreviations

OTP	Office of the Premier
DTC	Departmental Tender Committee
IS	Information Systems
IT	Information Technology
ICT	Information and Communication Technology
ITC	Information Technology Committee
SITA	State Information Technology Agency
ITC	Information Technology Committee
MISS	Minimum Information Security Standard
ISS	Information System Security
SDLC	Systems Development Life Cycle

A.2 Definitions

Accreditation	An official acknowledgement that an appropriate implementation of security has been applied to a particular system, connection and/or product.
Accrediting authority	An appointed body in SITA to accredit products, domains and/or inter-domain connections.
Audit	Actions that are taken to detect and investigate events that might represent a threat to security. To conduct the independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedure, and to recommend any indicated changes in controls, policy or procedures.
Certification	Involves a survey of the security that has been applied to an information system, connection and/or product and the confirmation that there is compliance with the security policy and standards.
Certifying body	An appointed body in SITA to certify products, information system domains, and/or inter-domain connections.
Communication security	Transmission of data from the point of origin to the destination without changing the sequence or content of the data, ensuring the confidentiality, integrity, availability and authenticity of the data.
Configuration control	The management of changes made to hardware, software, firmware and documentation of a system throughout the development and operational life cycle of the system.
Discretionary access control	An access control mechanism that restricts access to objects that are based on the identity of subjects and/or the groups to which it belongs. The controls are discretionary in the sense that it allows users that have been assigned certain access privileges to exercise their discretion in granting other users the same access to system resources, in particular to information.
Domain	Refers to those aspects of an information system that are relevant only to its ability to support its authorised users in achieving a uniform business objective. All its components are protected according to controls that are specified in a single security plan, and the domain is managed on a day-to-day basis by a single management authority (system manager).
Enterprise security management	The centralised security control and administration of multiple platforms, including distributed as well as mainframe systems, in order to provide for uniform application of security policies.
Information systems	Applications and systems to support the business while utilising information technology as an enabler or tool.
Information system security	To preserve the availability, integrity and confidentiality of information systems and information according to affordable security practices.

CONFIDENTIAL

Information technology	All aspects of technology that are used to manage and support the efficient gathering, processing, storing and dissemination of information as a strategic resource.
Inter-domain connection	A connection (including a manual connection) between two separate domains for the purpose of the sharing or exchange of information or other resources.
Key personnel	System personnel whose activities are critical for the effective functioning of the system.
Key posts	High-risk posts that are filled by persons whose activities will not be interrupted due to the sensitive nature and continuity thereof.
Local area network	A high-speed communication infrastructure that enables users to share resources such as hardware, software, data or Wide Area Network (WAN) communication in a cost-effective manner.
Local area network security	LAN security entails the protection of the confidentiality, integrity and availability of all information that is provided or obtained by a LAN, as well as that of the LAN resources.
Logical access control	Access control mechanisms that are implemented and enforced by network operating systems, operating systems, application software and communication processes (e.g. authentication, resource access, audit etc.).
Mandatory access control	An access control mechanism that partitions system resources according to the sensitivity of the information that is contained in the objects (as represented by a label), and the formal authorisation (e.g. security clearance) of subjects to access information of such sensitivity on a need-to-know basis. Predetermined access rules are implemented in the trusted system hardware and software so that access to a particular partition is not left to the discretion of other users.
Monitoring	Performance measurement to ensure the confidentiality, availability and integrity of operational systems and information.
Non-SITA third party	Any organisation/institution/department other than SITA, a national department, provincial administration or organisational component listed in schedules 1 and 2 of the Public Service Act, 1994.
Office	Office of the Premier
PABX security	The protection of the confidentiality, integrity and availability of all information that is provided or obtained by a PABX, as well as that of the PABX resources.
Participating department	Any department making use of the services that are provided by SITA.



Annex B : OTP information system security policy (register of changes)

OTP information system security policy register of changes on servers

[illegible]

171

Annex C : Letter of promulgation

This policy regarding information system security in **OTP** is effective upon receipt.

This document is the property of **OTP** and will only be issued to participating **OTP** departments and such members who require it in the performance of their official duties. Any person who finds this document will deliver it to the nearest **OTP** department or SAPS office, together with details of the circumstances under which it was found.

The information contained in this document will not be communicated directly or indirectly to the press or any unauthorised person.

Proposed changes and amendments will be sent to the **Director General, Office of the Premier, P/Bag x9483, Polokwane, 0700**, via normal service channels.

1 
Director General

Date... 27/7/2006



Annex D : OTP policy comment and change proposal form

Detail of proposer	Title: Name: Address: Department: Phone:
Change request details	Policy reference: Action Modify/replace/delete/add (Circle one)
Suggested change	(Detail proposed change)
Reasons	(Detail reasons to support proposed change)
	Date: _____ Signature: _____

Annex E : User Registration Form

Whenever an official is employed by or resigns from the OTP and is/was assigned to perform functions which allowed access to the OTP computer applications he/she must complete this form and a copy must be sent to the GITO. This form is obtained from Human Resources.

Surname and initials	
ID Number	
Persal number/Internal control number	
Date of employment	
Date of resignation	
Region and division	
Workstation name and address	
User-code assigned to official	

Applications or Screen names to which official must have access:

Application	Grant Access	Deny Access

Official Signature: **Date**

Supervisor Signature: **Date**

HR Signature: **Date**

DGITO signature: **Date**