Northern Cape Provincial Government

Information Security Policy

Information Technology Operations

DOCUMENT CONTROL

Document details	
Province	Northern Cape
Document	Information Security Policy Information Technology Operations
Document Name	NCPG IS Policy
Document Number:	Version 1.3
Document Status:	Approved
Author(s):	PISM and PGITO Members

Revision information		
Revision Number	**Revision Date**	**Change Reference**
1.0	18 November 2010	Initial Document
1.1	26 January 2012	Approved Document
1.2	5 August 2014	Reviewed and Approved
1.3	30 September 2015	Reviewed

Contents

GLOSSARY

Access Control	Refers to, exerting control over, whom can interact with a electronic and or digital resource.
DGITO	Departmental Government Information Technology Officer
PGITO	Provincial Government Information Technology Officer
DISO	Departmental Information Security Officer
GITO	Government Information Technology Officer
PISM	Provincial Information Security Manager
ID Management	Describes the management of individual identities, their authentication, authorization,roles, and privileges/permissions within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime, and repetitive tasks.
IS	Information Systems
Mobile Computing	It is a form of human–computer interaction by which a computer is expected to be transported during normal usage. Mobile computing has three aspects: • Mobile Communication - addresses communication issues in ad-hoc, and, infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. • Mobile Hardware - mobile devices and or relevant device components. • Mobile Software - the characteristics and requirements of mobile applications.
NCPG	Northern Cape Provincial Government
OECD	Organisation for Economic Co-operation and Development
Remote Access	This refers to communication with a data processing facility from a remote location or facility through a data link
Segregation of Duties	The concept of having more than one person required to complete a task. In business the separation by sharing of more than one individual in one single task shall prevent from fraud and error reduction.
SITA	State Information Technology Agency
BACS	Biometric Access Control System
BAS	Basic Accounting System
Enrolment Officer	A person designated to enroll a user on to BACS
LOGIS	Logistical Information System
PERSAL	Personnel and Salary Administration System
NCPT	Northern Cape Provincial Treasury
System Controller	For purposes of this policy includes the BAS, PERSAL and LOGIS System Controller
User	For purposes of this policy includes users of BAS, PERSAL and LOGIS

INTRODUCTION

OBJECTIVES

1. The broad objective of this policy is to provide the NCPG with an information system and information communications security policy and standards in order to apply an effective and consistent level of security to all information systems that process public service information.

2. Particular objectives are to:

    a. apply cost-effective protection to classified information which is processed by public service information and related technology assets;

    b. protect sensitive information that is processed by public service information systems or technology;

    c. be able to demonstrate accountability by a structured method of information system and information technology security implementation and verification across public service;

    d. develop an information system and information technology security culture that reflects a consistent approach, based on an understanding of the security issues and a cost-effective way of dealing with them.

GUIDING PRINCIPLES

This policy is based on the OECD' Guidelines for the Security of Information Systems and Networks (2002)[1] and the South African National Standard on Information technology -- Security techniques -- Code of practice for information security management (17799:2005)[2]. The following fundamental security principles are applicable throughout the policy:

1. **Awareness**

    Departments should be aware of the need for security of information systems and networks and what they can do to enhance security.

2. **Responsibility**

    All departments are responsible for the security of information systems and networks.

3. **Response**

    Departments should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

4. **Ethics**

    Participants should respect the legitimate interests of others.

5. **Democracy**

    The security of information systems and networks should be compatible with essential values of a democratic society.

6. **Risk assessment**

    Departments should conduct risk assessments.

7. **Security design and implementation**

    Departments should incorporate security as an essential element of information systems and networks.

[1] OECD Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org

[2] SANS 17799:2005 Information technology -- Security techniques -- Code of practice for information security management, June 2005. www.sabs.co.za

8. Security management

Departments should adopt a comprehensive approach to security management.

9. Reassessment

Departments should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

LEGISLATIVE MANDATE

Public Service Act and Regulations

In terms of the Public Service Act[3], 1994, the Minister for the Public Service and Administration ("MPSA") is responsible for –

(a) any policy which relates to information management and information technology in the public service; and

(b) the provision of a framework of norms and standards with a view to giving effect to any such policy (section 3(1)(f)).

The Public Service Regulations, 2001[4], contain the following provisions that relate to information technology security ("IT security"):

(a) The Minister shall, in consultation with the Minister of Intelligence, issue Minimum Information Security Standards (herein referred to as the MISS) for the public service in the form of a handbook called the Handbook on Minimum Information Security Standards.

(b) Any person working with Public Service information resources shall comply with the MISS.

(c) A head of department may request exemption from a provision of the MISS. The request shall be submitted to the Minister. The Minister shall, in consultation with the Minister of Intelligence, grant the request for exemption if the exemption is considered necessary for the effective functioning of the relevant department or a part thereof.

(d) A head of department shall ensure the maintenance of information security vigilance at all times in the department.

(e) When a non-compliance with the MISS comes to the knowledge of an employee of a department, she or he shall report it immediately to the head of department or an employee designated for this purpose by that head.

(f) Every time a change and/ or modification is made to a Public Service Information system, the system shall be certified for compliance to the MISS.

(g) A head of department shall regularly, on the basis of the threat posed by the incident, submit to the Director-General: National Intelligence Agency, the Auditor-General and such other authorities as the head considers appropriate-

(i) an incident report of every non-compliance with the MISS;

(ii) a plan on how incidents of non-compliance will be corrected and how to prevent similar incidents in future; and

(iii) an exemption report of all exemptions granted under (c) of this part and all deviations from the MISS because of such exemptions.

[3] PUBLIC SERVICE ACT, 1994i, Proclamation 103 published in GG 15791 of 3 June 1994, Copyright Juta & Company Limited, www.dpsa.gov.za

[4] PUBLIC SERVICE REGULATIONS, Chapter 5 Part II, 2001, Government Notice No. R. 1 of 5 January 2001, www.dpsa.gov.za

State Information Technology Agency Act

According to the State Information Technology Agency Act 88 of 1998 ("SITA Act")[5], the **objective of the State Information Technology Agency** ("SITA") is to provide **information technology, information systems and related services** in a **maintained information systems security environment** to, or on behalf of, **participating departments and organs of state** and in regard to these services, act as an agent of the South African Government (section 6). The following terms are defined in that Act as follows:

> *"information systems"* means applications and systems to support the business whilst utilising information technology as an enabler or tool;
>
> *"information systems security"* means to preserve the availability, integrity and confidentiality of information systems and information according to affordable security practices;
>
> *"information technology"* means all aspects of technology which are used to manage and support the efficient gathering, processing, storing and dissemination of information as a strategic resource; and
>
> *"participating department"* means any department making use of services provided by the Agency, i.e. SITA (section 1).

SITA must in the execution of its functions —

(a) maintain a comprehensive information systems security environment according to approved policy and standards; and

(b) adhere to the policies on information management and information technology and a framework of norms and standards to give effect to such policies, as well as regulations made in this regard by the MPSA in terms of the Public Service Act and the State Information Technology Agency Act (section 7(2) and (3)).

The **Minister** may make Regulations regarding the security requirements of the different departments and organs of state (section 23(c)).

National Strategic Intelligence Act

In terms of the National Strategic Intelligence Act 39 of 1994[6], **the National Intelligence Agency must fulfil the national counter-intelligence responsibilities**, and for this purpose must conduct and co-ordinate counter-intelligence.

According to that Act the term **"counter-intelligence"** means **measures and activities** conducted, instituted or taken to impede and to neutralise the effectiveness of foreign or hostile intelligence operations to protect classified information to conduct security screening investigations and to counter subversion, treason, sabotage and terrorism aimed at or against personnel, strategic installations or resources of the Republic (section 2(1)(b)).

The functions of the **National Intelligence Co-ordinating Committee** ("Nicoc") includes amongst other, to co-ordinate the intelligence supplied by the members of the National Intelligence Structures to Nicoc and interpret such intelligence for use by the State and the Cabinet for the purposes of,

(a) the detection and identification of any threat or potential threat to the national security of the Republic;

(b) the protection and promotion of the national interests of the Republic; and

(c) making recommendations to the Cabinet on intelligence priorities (section 4(2)(b) and (f)).

The **Minister** may, after consultation with the Joint Standing Committee on Intelligence, subject to subsection (2), **make regulations regarding the protection of information** and intelligence (section 6(1)(a)).

[5] STATE INFORMATION TECHNOLOGY ACT, Act No 88 of 1998, www.dpsa.gov.za
[6] National Strategic Intelligence Act 39 of 1994, www.info.gov.za

Minimum Information Security Standards

On 4 December 1996 Cabinet approved the Minimum Information Security Standards ("MISS") document as national information security policy. This policy incorporates the provisions, principles and policy standards contained in the MISS.

Electronic Communications and Transactions Act

The Electronic Communications and Transactions Act of 2002[7] deals with the protection of critical databases. It defines the following accordingly:

(a) "critical data" is defined as "data that are of critical importance to the national security of the Republic, and/or the economic and social wellbeing of its citizens"; and

(b) "critical database" is defined as "organised collections of critical data in an electronic or digital form from where it may be accessed, reproduced or retracted data".

The **Minister of Communications** may, by notice in the Gazette,

(a) declare certain classes of information which is of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens to be critical data; and

(b) establish procedures to be followed in the identification of critical databases (section 53(a),(b)).

The **Minister** may prescribe minimum standards or prohibitions in respect of,

(a) the general management of critical databases;

(b) access to, transfer and control of critical databases;

(c) infrastructural or procedural rules and requirements for securing the integrity and authenticity of critical data;

(d) procedures and technological methods to be used in the storage or archiving of critical databases;

(e) disaster recovery plans in the event of loss of critical databases or parts thereof; and

(f) any other matter required for the adequate protection, management and control of critical databases (section 55(1)).

The Director-General may, from time to time, cause audits to be performed at a critical database administrator to evaluate compliance with the provisions of this Chapter. The audit may be performed either by cyber inspectors or an independent auditor (section 57(1)(2)).

[7] ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT, Act No. 25 of 2002, www.gov.za

1. Access Control of Information Systems – Information Technology Operations

Purpose	To ensure that adequate access control measures are in place to protect information and IT resources from loss, possible data corruption, unauthorised use/ viewing and denial of service.
Scope	This policy applies to all government and department networks and systems.
Target audience	The persons responsible for complying with and implementing sections of this policy, relevant to their responsibilities, are the Government Information Technology Officer (GITO), System/Data Owners (S/DO), SITA, IT Outsourcers, Service Providers and IT staff.
Summary of policy	The policy aims to ascertain that adequate access control measures are in place to ensure that information and IT resources are protected from loss, unauthorised use or viewing and denial of service. This policy focuses on password & user ID management, access rights & privilege control and segregation of duties. In addition it addresses remote, emergency and administrator access requirements
Details of the policy	The requirements for complying with this policy are set out in the following sections: 1.1 Password and User ID Management 1.2 Biometric Access Control System 1.3 Access rights and privilege control 1.4 Remote Access 1.5 Administrator Access 1.6 Third Party Access 1.7 Segregation of Duties 1.8 Mobile computing and teleworking

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
1.1 Password and User ID Management					
	1. Business requirements for access control to all applications must be defined and documented and approved by the Director General. System owners must provide the GITO with a clear statement of the business requirements for system access, so that the GITO can oversee access to IS services and data. Data owners and service providers will also be given the statements of business requirements.1 2.	DG, GITO, DGITO, S/DOs	Updated annually or when changed	Access Control Procedures	No
	3. IT users' access to functions and information must be restricted according to individual user roles and based on a "need to know and need to do basis" as specified by information system owners.	GITO, DGITO, S/DOs, IT staff	Based on role changes	Access Control Procedures	Yes

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
	4. Responsibility for extending appropriate levels of authorisation to users will be maintained in a manner consistent with the organisation's security policy.	GITO, DGITO, S/DOs, IT staff	Based on role changes	Access Control Procedures	
	5. Access will only be granted to users and / or third parties after the required authorisation processes have been completed.	DG, GITO, DGITO, SITA, IT Outsourcer	Ongoing	Access Control Procedures	
	6. IT users of the system must be identified using a unique User ID and authenticated with a password to ensure repudiation.. Shared User IDs may be issued to a group of users or for a specific job subject to management approval as long as the risks of doing so has been considered by Information owners and compensating controls set in place.	DGITO, IT staff, SITA, IT outsourcer, GITO	Ongoing	Access Control Procedures	No
	7. IT personnel are responsible for all activities performed with their personal user IDs as well as special logon IDs. As such, user IDs and other logon IDs may not be utilised by anyone other than the individuals to whom they have been issued and users are forbidden from performing any activity with IDs belonging to other users. Gross negligence or wilful disclosure of this information can result in disciplinary action, including termination.	DGITO, IT staff, SITA, IT Outsourcer	Ongoing		Yes
	8. Inactive user sessions should be terminated by system enforced controls. Special consideration should be given to terminal based sessions in high risk locations.	DGITO, IT staff, SITA, IT Outsourcer, HR	Revised annually or upon joining and resignation of users		Yes
	9. Procedures addressing user access must cover initial registration of new users, disabling inactive user accounts as well as de-registration of a user once access is no longer required.	GITO, DGITO, SITA, IT Outsourcer	Review annually		Yes
	10. A procedure for issuing new or changed passwords must be in place.	GITO, DGITO, SITA, IT Outsourcer	Ongoing		Yes
	11. In order to prevent unauthorised access to the Department's computer system, a formalised password standard must be in place regarding password length and composition (alphanumeric), frequency of change and re-use of passwords.	DGITO, IT staff, SITA, IT Outsourcer	Ongoing	Access Control Procedures	Yes
	12. Users' access rights must be enforced by automated access control mechanisms to ensure individual accountability.	DGITO, IT staff, SITA, IT Outsourcer	Ongoing	Access Control Procedures	Yes
	13. All network services (e.g. Netware / Persal / BAS / Groupwise) must be authenticated. This must include all logons requiring a unique user-id and password to ensure that only authorised users gain access to the network services (with the exception of documented instances as described in point 3).	DGITO, IT staff, System owner, SITA, IT Outsourcer	Ongoing		Yes
	14. Passwords must be changed immediately if there is indication of system or password compromise.	DGITO, IT staff, System	Ongoing		Yes

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
		owner, SITA, IT Outsourcer			
1.2 Biometric Access Control System					
	1. The Biometric Access Control System (BACS) used by the Northern Cape Provincial Treasury, an electronic signature system protecting the integrity of the data and to enhance security and access control to the BAS, PERSAL and LOGIS systems. User profiles are regarded as electronic signatures which are regulated by the Electronic Communication and Transaction Act 2005 (Act 36 of 2005) which, BACS complies to.	NCPT	Ongoing	Biometric Access Control System Support Procedure Manual	Yes
	2. Where there is no System Controller at the department due to the fact that the role has been centralized at Provincial Treasury, the procedure manual applies to Sub-System Controllers and Representatives in the departments.	NCPT, System Controllers, Sub-system Controllers, IT Staff, DGITO	Ongoing	Biometric Access Control System Support Procedure Manual	Yes
	3. This BACS procedure manual applies to all provincial departments and will is effective from the date of approval of the procedure manual by the Head of Department of Provincial Treasury.	NCPT, System Controllers, Sub-system Controllers, IT Staff, DGITO	Ongoing	Biometric Access Control System Support Procedure Manual	Yes
	4. All users must be enrolled on to BACS by an enrolment officer designated by Provincial Treasury.	NCPT, System Controllers, Sub-system Controllers, IT Staff, DGITO	Ongoing	Biometric Access Control System Support Procedure Manual	Yes
	5. Access to BAS, PERSAL and LOGIS will be regulated by BACS and will not be possible without a smartcard and biometric fingerprint scanner.	NCPT, System Controllers, Sub-system Controllers, IT Staff, DGITO	Ongoing	Biometric Access Control System Support Procedure Manual	Yes
	6. Controllers of the systems are accountable for implementing, maintaining and communicating procedures to ensure the continuous control over BACS in the departments.	NCPT, System Controllers, Sub-system Controllers, IT Staff, DGITO	Ongoing	Biometric Access Control System Support Procedure Manual	Yes

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
1.3 Access Rights and Privilege Control					
	1. Systems requiring protection against unauthorised access must have the allocation of privileges controlled through a formal authorisation process and a record of all privileges allocated must be maintained.	System Owners, DGITO, IT staff, SITA, IT Outsourcer	Updated annually or when changed	Access Control Procedures	No
	2. A formal test and review of users' access rights must be conducted periodically by the GITO and the System/Data owners. IT staff must generate relevant reports to facilitate this process.	GITO, DGITO, S/DOs, SITA, IT Outsourcer	Every 6 months		No
	3. Privileged access rights, which allow users to override system controls, must be reviewed regularly by the GITO and system owners. It is recommended that these reviews occur more frequently (every three months) than other access rights.	GITO, DGITO, S/DOs	Quarterly		No
	4. All commands issued by computer system operators are required to be traceable to specific individuals via the use of comprehensive logs and unique user ids.	DGITO, IT staff, SITA, IT Outsourcer	Ongoing		Yes
1.4 Remote Access – External to Gov VPN controlled by SITA					
1.5 Administrator Access					
	1. Administrator and root level system accounts must be strictly controlled.	DGITO, PISM, IT staff, SITA, IT Outsourcer, GITO	Ongoing	User access control	No
	2. Such privileged accounts (i.e. administrator) may only be granted by a clear chain of authority and delegation and kept to an absolute minimum.	DGITO, PISM, IT staff, SITA, IT Outsourcer, GITO	When required	User access control	No
	3. All tasks performed by computer administrators are required to be traceable to specific individuals via the use of comprehensive logs and unique user IDs. These logs must be reviewed on a regular basis by IT Operations and escalated to the GITO.	DGITO, PISM, IT staff, SITA, IT Outsourcer, GITO	Monthly	User access control	Yes
1.6 Third Party Access					
	1. Any connection to the Department backbone network must be supported by the GITO / Accounting Officer and authorised by SITA.	DGITO, PISM, IT staff, SITA, IT Outsourcer, GITO	Establishment of new connections	Third Party Access Procedure	No
	2. The Department computers or networks may only be connected to third party computers or networks after the GITO has determined that the combined system will be in compliance with the Department's security requirements.	DGITO, PISM, IT staff, SITA, IT Outsourcer, GITO	Initial connection and reviewed yearly	Third Party Access Procedure	No
	3. Third party users must be restricted to the minimum services and	System owners	Ongoing	Third Party	Yes

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
	functions necessary for the business process, as determined by the system owner.			Access Procedure	
	4. As a condition of gaining access to the Department's computer network, every third party must ensure that the computer's anti-virus software is up to date.	Infrastructure team DGITO,	Annually	Third Party Access Procedure	No
	5. A register of authorised third party access users, as well as the access levels provided, must be reviewed regularly (at least quarterly for ongoing contracts and ad hoc when access is set up) by the GITO to confirm that there is still a valid business requirement.	GITO, DGITO	Every six months	Third Party Access Procedure	No
	6. All third party logon accounts must be revoked when the arrangement terminates.	GITO, DGITO, SITA, PISM, IT Outsourcer	As soon as termination occurs	Contracts	Yes
1.7 Segregation of Duties					
	1. The Department's systems and technical support staff must support a clear separation of functions (such as system administrators vs. regular users) to prevent unauthorised access and functions being performed.	System owners, GITO, PISM, DGITO	Updated annually and when changed	User access control	Yes
	2. The System Owners must determine and establish the IT user roles and responsibilities in their business unit to ensure that IT Operations can adequately enforce segregation of duties.	SOs, IT Operations	Ongoing	User access control	No
1.8 Mobile Computing and Tele-working					
	1. 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.	Line management, DGITO, User	Upon issue of portable computers		Yes
	2. Persons who are issued with portable computers and who intend to travel for business purposes must be made aware of the information security issues relating to portable computing facilities and implement the appropriate safeguards to minimise the risks.	System owner, Data owner, GITO, DGITO, User	Ongoing	Security Awareness Training	Yes
	3. Laptop computers are to be issued to, and used only by, authorised employees and only for the purpose for which they are issued. The information stored on the laptop is to be suitably protected at all times.	System owner, Data owner, GITO, DGITO, User	Ongoing	Security Awareness Training	Yes
	4. Off-site computer usage, whether at home or at other locations, may only be used with the authorisation of line management. Usage is restricted to business purposes, and users must be aware of and accept the terms and conditions of use, which must include the adoption of adequate and appropriate information security measures.	System/Data owners, Line Management DGITO, User	Ongoing		Yes

2. Physical and Environmental Security Management – Information Technology Operations

Purpose	To ensure that critical or sensitive business information processing facilities are housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. The protection provided must be commensurate with the identified risks.
Scope	This policy applies to all IT Staff and Third Parties who have physical access to the Department's information processing facilities and computer
Target audience	The persons responsible for complying with and implementing sections of this policy, relevant to their responsibilities, are the Government Information Technology Officer (GITO), Provincial Information Security Manager (PISM) SITA, System Owners (SO), IT Outsourcers and Service Providers.
Summary of policy	This policy aims to prevent services being disrupted by loss or damage to computer equipment, communications equipment, power or facilities. Additionally, it aims to ensure that physical access is restricted to authorised individuals and that IT facilities processing critical or sensitive information are protected. This policy focuses on secure areas, equipment security, visitors, clear desk policy and disposal.
Details of the policy	The requirements for complying with this policy are set out in the following sections: 2.1 Secure areas 2.2 Equipment Security

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
2.1 Secure Areas					
	1. Buildings and rooms housing major concentrations of IT equipment, operational IT equipment, local cabling, non-critical hardware and storerooms for IT equipment are classified as secure areas	GITO, DGITO, PISM	Ongoing	Secure Area Categorisation Procedure No	No
	2. Criteria must be established for the categorisation of computer rooms within the Department, so as to address the risks associated with the different categories. [Eg, Training Rooms, Storage, Server Rooms, Network Rooms, other]	GITO, DGITO, PISM	Ongoing	Secure Area Categorisation Procedure No	No
	3. Based on the category of the secure area, the Department must ensure that the physical and environmental controls implemented to protect the information processing facilities are consistent with the equipment they contain. The following controls must be considered for secure areas where applicable: • Secure areas must be adequately protected by access systems and exit points (e.g. windows) are also appropriately secured; • Secure areas must have UPS protection and generator backup, where it is necessary and practical to do so;	GITO, DGITO, PISM, IT Outsourcer, SITA	Ongoing	Secure Area Categorisation Procedure No	No

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
	• Secure areas must have a fire detection system that automatically informs an appropriate person who reacts according to a defined process, it must comply with all relevant health and safety legislation and have good access to appropriately signed fire exits; • Secure areas must have an air conditioning system that operates 24 hours a day 7 days a week. It must be designed to keep the room within the IT manufacturers' recommended specifications for temperature and humidity throughout the year; • Temperature, humidity, power and cleanliness must be monitored so that potential problems with air conditioning equipment and power supplies can be anticipated; • Water detection equipment must be installed for secure areas in locations liable to flooding; • Emergency lights that can be activated in the event of a power failure must be in place; • Staff utilising secure areas may not eat or drink in the facilities and must keep the room clean and free of unnecessary contamination; • A periodic program of specialist cleaning must be in place. The frequency of cleaning must be appropriate to the environment and include under floor and above ceiling cleaning where there is a raised floor and false ceiling. The activities of the cleaners must be monitored by an appropriate Department appointed employee for the duration that the cleaners are busy in secure areas.				
	4. A procedure to authorise, review and revoke physical access to data centres and computer rooms must be in place.	GITO, DGITO, PISM, SITA, IT Outsourcer	Ongoing	Access Granting SOP for Server Rooms	No
2.2 Equipment Security					
	1. The Department premises for information equipment must be constructed so that they offer adequate protection against environmental threats and hazards such as fire, water damage and vandalism.	GITO, DGITO, PISM, SITA, IT Outsourcer	Ongoing	Equipment Maintenance Procedure, Secure Area Categorisation Procedure	No
	2. Based on the category of the server room, the equipment must	GITO, DGITO,	Ongoing	Equipment	No

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
	be protected from power failures and electrical anomalies by a suitable electrical supply.	PISM, DGITO, SITA, IT Outsourcer		Maintenance Procedure, Secure Area Categorisation Procedure	
	3. procedure addressing the maintenance and removal of Department equipment, property and software must be established including staff identification, logging of work done, offsite maintenance controls and supervision to ensure that no modifications are performed on any equipment other than that which is to be maintained.	GITO, DGITO, PISM, SITA, IT Outsourcer	Ongoing	Equipment Maintenance Procedure, Secure Area Categorisation Procedure	No
	4. Confidentiality agreements must be in place to ensure the security and confidentiality of information stored on equipment that is subject to third party and off site repair.	GITO, DGITO, PISM, SITA, IT Outsourcer	Ongoing	Equipment Maintenance Procedure, Secure Area Categorisation Procedure	No
	5. A procedure for the authorisation and utilisation of equipment used outside the Department's premises must be in place. To minimise the risk of theft, destruction, and/or misuse, personnel must exercise good judgment and safeguard their portable, laptop, notebook, personal digital assistants (PDA) and other transportable computers and sensitive information contained therein.	GITO, DGITO, PISM, SITA, IT Outsourcer	Ongoing	Equipment Maintenance Procedure, Secure Area Categorisation Procedure	No
	6. Each laptop computer must be marked for identification and inventory control. Inventory records of laptop computers must be kept current.	GITO, DGITO, PISM, SITA, IT Outsourcer	Ongoing	Equipment Maintenance Procedure, Secure Area Categorisation Procedure	No
	7. The loss or theft of any computer hardware and/or software must be reported in writing to the Security Manager and the respective Line Manager, as well as SAPS for a case number. The theft or loss must be recorded.	Security Manager, Line Manager, DGITO, SAPS	Ongoing	Equipment Maintenance Procedure, Secure Area Categorisation Procedure	No
	8. If computer equipment is transported by vehicle, it should be stored in the secured boot. At any other time it should be part of hand luggage.	User	Ongoing		No

3. Management of Information Security Function and Information Assets – Information Technology Operations

Purpose	To establish an Information Security Function with appropriate roles within the Department and maintain appropriate protection of information assets.
Scope	This policy applies to all Department IT users, Third Parties and outsourcers who have access to the Department information and/ or are utilising applications and computer installations.
Target audience	The persons responsible for complying with and implementing sections of this policy, relevant to their responsibilities, are the Government Information Technology Officer (GITO), Provincial Information Security Manager (PISM), SITA, IT Outsourcers and Service Providers
Summary of policy	The policy aims to ensure that a management framework is established to initiate and control the implementation of information security within the Department. Additionally it aims to ensure that information assets have a nominated owner and that they are accounted for. Finally, it addresses information and software ownership and responsibilities for data protection, software copyright compliance and similar considerations.
Details of the policy	The requirements for complying with this policy are set out in the following sections: 3.1 Secure Infrastructure 3.2 Accountability for assets 3.3 Software copyright 3.4 Legal and Regulatory compliance 3.5 System Audit considerations

	Policy Statements	**Responsible Person**	**Frequency**	**Related Procedures**	**Technology Dependent**
3.1 Secure Infrastructure					
	1. A centralised Information Security Function (ISF) communicated through a management forum must be established to ensure a clear direction for security initiatives and visible management support. The ISF should consist of a group of individuals in Provincial Departments who are responsible for Information Security and Information Technology and who can assist Accounting Offices and employees in carrying out their responsibilities for the protection of integrity, availability, and confidentiality of client and business information assets.	GITO, DGITO, Department Risk Manager & Security Manager & Records Manager	Ongoing	Not Applicable	No
	• Responsibilities of this function include: • Ensuring proper protection of the Department's information; • Approving, implementing and maintaining the information security policy; • Develop, implement and maintain information security standards, procedures and guidelines;	GITO, DGITO, Department Risk Manager & Security Manager & Records Manager	Ongoing	Not Applicable	No

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
	• Carry out awareness and control campaigns; • Provide professional information security education, training, and awareness programs and services to all users of the Department information assets; Assign security roles and responsibilities; • Co-ordinate the implementation of security across the organisation; • Act as a liaison Function on information security matters among all the Department business units and are the focal point for all information security activities throughout the Department; • Support and advise the line functions in the implementation of information security policies and standards for both information data and the systems that handle it; • Assist management in performing security risk analyses, preparation of action plans and security evaluation of in-house developed and vendor products and solutions; • Certify the validity of all information security risk analyses; and • Investigate information security breaches and perform other activities necessary to assure a secure information-handling environment.				
	2. Security roles and responsibilities of the Information Security Function, which can be performed in-house or outsourced, must be defined. Specific roles that need to be defined include: ***Provincial Information Security Manager (PISM)****:* The PISM is responsible for establishing and operating the IS security function. ***Departmental Information Technology Steering Committee***: The Information Security Steering Committee is responsible for overseeing the Information Security Function and its activities and to provide clear direction and visible management support for security initiatives.	GITO, DGITO, SITA, Government & Department Risk Manager, PISM	Ongoing	Not Applicable	No

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
	3. All security personnel should be made aware of their responsibilities and reporting lines.	GITO, DGITO, PISM, Government & Department Risk Manager, SO/DO	Ongoing	Not Applicable	No
	4. The Internal auditor unit must periodically review the adequacy of information system controls, as well as compliance with such controls.	Auditor General, Internal Audit, Other insurance providers (NIA)	Ongoing	Review based on all procedures	No
	5. The Human Resources department is responsible for facilitation and coordination of periodic annual declarations of personnel understanding of policies and their security responsibilities, assisting in information security education, and carrying out disciplinary actions.	Human Resources, GITO, DGITO, PISM	Ongoing	Disciplinary procedure, Access procedure for user Life Cycle	No
	6. The respective System Owners and/or outsourcing partners oversee access to restricted areas such as the computer rooms. They may also be called in during investigations of information security violations.	System Owners, SITA, IT Outsourcers	Ongoing	Disciplinary procedure, Access granting procedure for server rooms.	No
	7. It must be ensured that outsourcing of information services to a third party service provider does not introduce any degradation of information security	System Owners, SITA, IT Outsourcers	Ongoing	Disciplinary procedure, Access granting procedure for server rooms.	No

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
3.2 Accountability for Assets					
	1. All major information assets must be accounted for and have a nominated owner to whom the responsibility for the maintenance of appropriate controls should be assigned.	GITO, DGITO, System/DATA owners, Asset Manager	Ongoing	Management of Information Assets Procedure	No
	2. A detailed information systems (IS) inventory containing descriptions of all critical IS inventory must be maintained. Documentation must include: -Ownership; Identification (including location and labelling); -Description; and Configuration	GITO, DGITO, System/DATA owners, Asset Manager	Ongoing	Management of Information Assets Procedure	No

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
	3. A formal process should be in place to maintain the accuracy of the asset inventory. The inventory of IS equipment should be verified against the asset inventory on an annual basis by the business unit manager or an appointed delegate	GITO, DGITO, System/DATA owners, Asset Manager	Ongoing	Management of Information Assets Procedure	No
	4. All IS equipment must be individually marked. The mark should be prominently displayed on the equipment and the method of marking should not be removable without trace. The mark should contain a unique reference number and clearly indicate that the equipment is the property of the Department.	GITO, DGITO, System/DATA owners, SITA, IT outsources, Asset Manager	Ongoing	Management of Information Assets Procedure	No
3.3 Software Copyright					
	1. Bi-Annual scan check, must be performed by the Asset Management unit of the Department in collaboration with IT and Audited against Asset Register.	IT staff, GITO, DGITO, Asset Manager	Ongoing	Authorised Software procedure	No

4. Information Classification – Information Technology Operations

Purpose	To ensure the protection of sensitive Department data, information, knowledge and intellectual capital against improper disclosure. This is intended to be achieved by classifying the data, information, knowledge, and intellectual capital and developing mechanisms to protect it
Scope	This policy applies to all Department data, information, knowledge and intellectual capital.
Target audience	The persons responsible for complying with and implementing sections of this policy, relevant to their responsibilities, are the Government Information Technology Officer (GITO), Provincial Information Security Manager (PISM), System Owners (SO), Data Owners (DO), SITA, IT Outsourcers and Service Providers, Provincial Archivist, Registry Manager.
Summary of policy	This policy aims to ensure that adequate controls are in place to classify and protect sensitive Department data, information, knowledge and intellectual capital.
Details of the policy	The requirements for complying with this policy are set out in the following sections: 4.1Classification System 4.2 Information Classification Training

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
4.1 Classification System					
	1. All Department data, information, knowledge and intellectual capital must be classified according to an information security classification system, and the confidentiality, integrity and availability thereof protected accordingly.	Records Manager System Owners, Data owners	Ongoing		No
	2. All data, information, knowledge and intellectual capital shall be classified and labelled as one of the following security classes: *Highly confidential* - information is of such a nature that unauthorised disclosure, modification or destruction would cause significant damage to the Department, or seriously impact any aspect of operations. *Confidential* - information is of such a nature that unauthorised disclosure, use, destruction or modification would be against the best interests of the Department, its customers or any other individual. *Public* - information that is designated for release to the general public, or which requires no protection against disclosure.	Records Manager System Owners, Data owners, Users	Ongoing		No
	3. When the confidentiality classification of an information asset is unknown or unspecified, the information asset should be treated as 'Restricted.' If the unspecified information clearly contains customer, client or any personal information, the asset should be treated as 'Highly Confidential.' The asset should be properly classified as soon as possible.	Records Manger, Provincial Archivist	Ongoing		No
	4. The information classifications should allow for changes, and should be reviewed periodically.	Records Manger, Provincial Archivist	As Required		No
	5. Responsibility for changing the classification of an information asset lies with the asset owner or with individuals who have custodial responsibility for that information asset.	Records Manger, Provincial Archivist	Ongoing		No
	6. The minimum security control requirements, for each classification level, must be identified and implemented.	Records Manger, Provincial Archivist	Ongoing		No

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
4.2 Information Classification Training					
	1. Managers of all levels and system owners will receive information classification training on the assessment process in order to classify the information assets that they own and/or supervise and review the information classification process in the areas they are in charge.	Records Manger, Provincial Archivist	Annually		No
	2. The Human Resource Department will participate in trainings, not only to properly classify information assets in their area, but also on how to handle information asset violations by employees including: How to keep record of employee violations How to handle situations and different violations according to its severity.	Human Resource Department	Annually		No
	3. Users will receive training on how to handle information assets according to its classification. The training should include access and storage of electronic and printed information.	Records Manger, Provincial Archivist, Security Manager	Annually		No

5. Infrastructure and Protection – Information Technology Operations

Purpose	To ensure that the Information Technology infrastructure is managed from an information security perspective.
Scope	This policy applies to all information, critical applications, computer installations and networks.
Target audience	The persons responsible for implementing this policy are the Information Systems Infrastructure Manager Officer (GITO), Provincial Information Security Manager (PISM), Operations Mangers, Network Managers, Application Managers, Information Technology Managers, Internal Audit, IT Outsourcers and Service Providers.
Summary of policy	The policy aims to ensure that the network is protected and managed to preserve the availability, confidentiality and integrity thereof. Additionally it aims to protect the network from malicious software and code to ensure the integrity, availability and confidentiality of information and IT equipment. This policy also provides management with an accurate and coherent assessment of the security condition of The Department through the use of monitoring controls. Finally to reduce the disruption caused by disasters and security failures (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of business processes, preventative and recovery controls.

Details of the policy	The requirements for complying with this policy are set out in the following sections: 5.1 Protecting the Network 5.2 Managing the Network 5.3 Firewall Management 5.4 Malicious Software Management (Malware) 5.5 Patch Management 5.6 Monitoring and Logging Management 5.7 Business Continuity Management 5.8 Capacity Management 5.9 Backups 5.10 Information Security on Removable Media 5.11 Un-authorised Hardware Installation 5.12 Usage of Personal Electronic Devices

	Policy Statements	**Responsible Person**	**Frequency**	**Related Procedures**	**Technology Dependent**
5.1 Protecting the Network					
	1. The internal network addresses, configurations and related system design information for the Department's networked computer systems must be restricted so that both systems and users outside the internal network cannot access this information without explicit approval from the GITO or delegated official.	GITO, DGITO, Lan/Wan Staff, SITA	Ongoing		Yes
	2. *Authorisation for Network Services*: Changes to network services provided on the Department network that could affect information security must be approved by the System Owner prior to their implementation and use.	GITO, DGITO	Prior to Implementation		No
	3. *Register of Connections:* A register must be maintained which covers all categories of connectivity into or from the Department network, including: Internet remote access, RAS, extranet, private extranet, Internet admin and maintenance, admin RAS, Internet service usage, dial-out services, VPN, WAN/GAN, Intranet, and LAN to LAN.	Lan / Wan Staff, DGITO	Ongoing		Yes
	4.				
	5. *Protection of Security Systems:* Security systems operating within and across public and Department networks must be protected against internal and external intruders. The systems are to be installed in a physically secured and access-restricted area.	SITA, IT Outsourcer, GITO, DGITO, PISM, IT Staff	Ongoing		No

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
	6. *Auditing of Traffic:* Traffic between public and Department networks must be logged as appropriate.	SITA, IT Outsourcer, GITO, DGITO, PISM, IT Staff	Weekly / Monthly		Yes
	7. *Wireless networks:* Wireless networks are to be treated as untrusted networks and the necessary controls implemented to ensure security of the trusted network is maintained.	GITO, DGITO, IT Staff	Ongoing		Yes
5.2 Managing Network Connections					
	1. Only trusted entities are allowed full access to the Department network. All entry points to the Department network must be reviewed and approved ..	GITO, DGITO, SITA IT Staff	Quarterly		No
	2. *Network configuration*: The layout of wiring and all network devices will be documented.	DGITO, IT Staff	Reviewed Annually or upon Change		No
5.3 Firewall Management and Intrusion Detection System (IDS) – SITA MANAGED					
5.4 Malicious Software Management (Malware)					
	1. The early detection of virus infections on data media and networks must be assured by the implementation of Department approved and up-to-date anti-virus and integrity- checking software on all possible devices	GITO, DGITO, Antivirus Specialist (SITA, IT Outsourcer)	Ongoing	Procedure for Anti-virus updates	Yes
	2. Anti-virus software must be installed on all personal computers and servers that are connected to the Department network.	GITO, DGITO, Antivirus Specialist (SITA, IT Outsourcer)	Ongoing	Procedure for Anti-virus updates	Yes
	3. There must be an automatic, daily, update of the virus definitions for all servers and personal computers.	GITO, DGITO, Antivirus Specialist (SITA, IT Outsourcer)	Daily	Procedure for Anti-virus updates	Yes
	4. When a remote user connects to the network the anti-virus definitions on their computer must be updated automatically.	GITO, DGITO, Antivirus Specialist (SITA, IT Outsourcer), User	Ongoing	Procedure for Anti-virus updates	Yes
	5. Data downloaded from e-mail systems or public networks are	GITO, DGITO,	Continuously	Procedure for Anti-virus	Yes

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
	required to be checked for viruses before use.	Antivirus Specialist (SITA, IT Outsourcer), User		updates	
	6. End users must be prevented from disabling or changing the configuration of the anti-virus software installed on their personal computers.	GITO, Antivirus Specialist (SITA, IT Outsourcer)	Ongoing	Procedure for Anti-virus updates	Yes
5.5 Patch Management					
	All security-related operating system and production software patches must be kept current and properly implemented.	GITO, DGITO, SITA, IT Outsourcer, IT Staff	Daily	Patch management Procedure	Yes
5.6 Usage of Personal Electronic Devices					
	1. It is the policy of the Department that Personal Electronic Devices containing or accessing the information resources at the Department must be approved prior to connecting to the information systems at the Department. This pertains to all devices connecting to the network at the Department, regardless of ownership.	GITO, DGITO, PISM	As Required		Yes
	2. Personal Electronic devices are easily lost or stolen, presenting a high risk for unauthorised access and access to the network at the Department. These risks must be mitigated to acceptable levels. Portable computing devices and portable electronic storage media that contain confidential, personal, or sensitive Department information must use encryption or equally strong measures to protect the data while it is being stored.	GITO, DGITO, PISM	As Required		Yes
	3. All information stored on Personal Electronic devices should be password protected using a strong password that is in line with the guidelines stipulated in section 1.1 (Password and User ID Management) of the Department information security policy, where this is technically feasible.	GITO, DGITO, PISM	As Required		Yes
	4. Disposal of personal electronic devices should be performed in a manner such that the data is not recoverable. Where users are uncertain about how to securely dispose of removable media, IT staff should be contacted for assistance.	GITO, DGITO, PISM	As Required		Yes
	5. Personal Electronic devices should always have the latest	GITO, DGITO,	As Required		Yes

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
	Symantec Antivirus definitions, latest Windows or platforms updates. IT Staff should be contacted for assistance.	PISM			

6. Security Incident Management – Information Technology Operations

Purpose	To minimise the damage from security incidents and malfunctions by actioning and resolving reported issues and to monitor and learn from such incidents.
Scope	This policy applies to all IT Staff and Third Parties who make use of the Department's information systems, critical applications and computer installations.
Target audience	The persons responsible for complying with and implementing sections of this policy, relevant to their responsibilities, are the Government Information Technology Officer (GITO), System Owners (SO), Data Owners (DO), SITA, IT Outsourcers, Service Providers and IT staff.
Summary of policy	This policy aims to minimise the risks associated with information security incidents to ensure timely detection, reporting and response to actual or suspected incidents
Details of the policy	The requirements for complying with this policy are set out in the following sections: 6.1 Reporting security incidents and malfunctions 6.2 Responding to security incidents and malfunctions 6.3 Learning from incidents 6.4 Disciplinary process

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
6.1 Reporting security incidents and malfunctions					
	1. The GITO / Responsible Delegated Official is responsible for maintaining an incident register which will include details such as logging date, review, escalation etc. where all security incidents are recorded.	GITO / Responsible Delegated Official	Ongoing	Incident Management procedure	Yes
	2. All Department employees, IT staff, third parties, contractors and temporary staff must be made aware of the security incident reporting procedure and that they are required to report any security incidents and malfunctions as soon as possible. – Security Incident Procedure (SOP)	GITO, DGITO, Line Managers, Users	Ongoing	Incident Management procedure	No

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
6.2 Responding to security incidents					
	1. The first priority in responding to any security incident in the Department is to stop the security breach itself and prevent its recurrence. Where the severity of the incident and its likelihood of recurrence justify it, the Department management can and must take any steps necessary on a temporary basis, such as removing systems from operation, revoking system accesses or removing involved personnel from the Department facilities.	Security Manager, GITO, DGITO, SO, DO, SITA, IT Outsourcer	Ongoing	Incident Management procedure	No
	2. To address security incidents and malfunctions, a formal incident response procedure must be established setting out the action to be taken in the event on an incident. The procedures must consider: • The evaluation of reported security incidents and weaknesses; • Determining actions to address the security incidents and weaknesses; and • Monitoring progress on the actions.	Security Manager, GITO, DGITO, System Owners, Data Owners	Ongoing	Incident Management procedure	No
	3. Response procedures to address security incidents must be documented indicating what actions and escalation needs to be taken in the event of incidents within categories such as: • Access control; • Network Security; • Critical Asset Rooms; • Equipment Security; • Communications Security; • Computer Virus; • Systems availability; and • Software Security.	Security Manager, GITO, DGITO, SO, DO, SITA, IT Outsourcer	Ongoing	Incident Management procedure	No
	4. The GITO must ensure that all open incidents and actions against open security incidents and weaknesses are reviewed and monitored.	Security Manager, GITO DGITO,	Weekly	Incident Management procedure	No
	5. Security incidents and malfunctions need to be resolved and closed by IT staff and / or management in a timely manner consistent with documented response procedures	Security Manager .DGITO, IT Staff, SO, DO	Ongoing	Incident Management procedure	No

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
6.3 Disciplinary process – Dealth with in Departmental Disciplinary Procedure					

7. Internet and E-mail security – Information Technology Operations

Purpose	To ensure the confidentiality and integrity of e-mail messages is protected in transit, the risk of e-mail misuse is minimised and that e-mail services are available when required, making it an effective communication tool. In addition, to ensure appropriate use of the Internet and minimise the threat posed by the Internet to The Department's networks.
Scope	This policy applies to all IT Staff and Third Parties who make use of the Department's electronic mail system and/or have access to the Internet.
Target audience	The persons responsible for complying with and implementing sections of this policy, relevant to their responsibilities, are the Government Information Technology Officer (GITO), SITA, System Owners (SO), Data Owners (DO), IT Outsourcers and Service Providers.
Summary of policy	This policy aims to ensure that adequate controls are in place to manage the use of Internet and e-mail services and to ensure that risks involved with utilising these services are managed. This policy focuses on Internet, Intranet and e-mail usage.
Details of the policy	The requirements for complying with this policy are set out in the following sections: 7.1 Internet 7.2 E-mail

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
7.1 Internet – DPSA / SITA					
	1.				
	2. Workstations with the capability of connecting to the Internet should have the following additional controls implemented: • Desktop firewalls; • applying Software updates; •	SITA, IT Outsourcer, Line Management, DGITO, IT Staff	Ongoing	Software Update Procedure, System Configuration Procedure	Yes

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
7.2 E-mail					
	1. Mail servers must be configured to prevent the messaging system being overloaded by limiting the size of messages or user mailboxes.	SITA, IT Staff	Ongoing	System Configuration Procedure	Yes
	2. E-mail systems must be monitored by the GITO to determine if future availability and up time will meet the requirements.	GITO, DGITO, SITA, Outsourcer, PISM	Monthly	E-mail monitoring procedure	Yes
	3. E-mail must be scanned for the following conditions and where they occur, the message must be blocked and quarantined: • attachments that could hide malicious code (e.g. exe files, zip files, MPEG etc.);	SITA, IT Staff, GITO	Continuous	E-mail monitoring procedure	Yes
	4. A generic disclaimer, approved by the legal department, must be attached to all e- mails.	IT Staff, GITO, DGITO	Ongoing		Yes
	5. The GITO must make users of the Department's e-mail systems aware of the consequences of their actions when using e-mail, that the use of e-mail may be monitored and that the content of the e-mail messages may be legally and contractually binding. – AUP	GITO DGITO	Initial training, Yearly update awareness, Ongoing reminders	Security Awareness Training	No

8. Managing Information Security related to Outsourcing and Third Parties – Information Technology Operations

Purpose	To ensure that the outsourcing of Information Technology and third party access is governed by formal arrangements addressing the risks, security controls and procedures between the parties.
Scope	This policy applies to all information, critical applications, computer installations, networks and systems under development that is outsourced or to which third parties has access.

Target audience	The persons responsible for complying with and implementing sections of this policy, relevant to their responsibilities, are the Government Information Technology Officer (GITO), Provincial Information Security Manager (PISM), SITA, System Owners(SO), Data Owners (DO), IT Outsourcers, Service Providers, all the Department IT users, IT Third Parties, Contractors and Temporary Staff.
Summary of policy	This policy aims to ensure that there are controls in place to manage outsourcing of Information Technology services and to ensure that risks involved with third parties working for the Department are managed.
Details of the policy	The requirements for complying with this policy are as follows: • Outsourcing management • Third party management

	Policy Statements	**Responsible Person**	**Frequency**	**Related Procedures**	**Technology Dependent**
8.1 Outsourcing Management					
	1. Controls must be in place to provide reasonable assurance that outsourcing arrangements have the appropriate security controls.	GITO, DGITO, PISM, Government & Department Risk Manager	Ongoing	Outsource and Third Party Contractual Procedure	No
	2. As part of the contract procedure, a risk assessment should be carried out under the guidance of the PISM in order to determine the security implications and security control requirements.	PISM, Risk Manager	For every outsourcing agreement	Risk Assessment Procedure	No
	3. Security should not suffer for any reason (e.g. cost reduction, better cost visibility, access to expertise, focus on mainline business issues, etc.) by the outsourcing of information services.	GITO DGITO,	Ongoing	Monitoring Procedure	Yes
	4. All Department security policies, standards, procedures and specifications have to be adhered to by outsourcing sites and/or by external individuals.	GITO, DGITO, SITA, IT Outsourcer	Ongoing	Monitoring Procedure	No
	5. Arrangements should include protection of sensitive data by utilising appropriate access controls and encryption techniques.	SITA, IT Outsourcer	Ongoing	User Access Control	Yes
	6. Contractual agreements must address as a minimum: • What arrangement will be in place to ensure that all parties involved in the outsourcing including subcontractors, are aware of their security responsibilities; • How availability of services are to be maintained in the event of a disaster;	GITO, DGITO, Contractual Department, PISM	Ongoing	Outsource and third party Contractual Procedure	No

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
	• Nature, timing and frequency of security incidents to be reported to; • How legal requirements are to be met; • Service level agreements on availability of service; • What physical and logical controls will be used to restrict and limit the access to the Department's sensitive business information to authorised users; • What levels of physical security are to be provided for outsourced equipment; • Confidentiality agreement; • Measures to ensure appropriate involvement in IT changes by outsourcing parties; • A list of all external individuals authorised to access IT assets must be available to on request; and • Subject to the results of the risk assessment performed, may elect to reserve the right to audit the outsourcer, but at a minimum must request regular "proof" of security compliance from the outsourcer.				
	7. Depending upon the nature of the outsource contract all information security standards for third party access must be mandated, as applicable to outsource contracts.	GITO, DGITO, SITA, IT Outsourcer	Ongoing	Outsource and third party Contractual Procedure	No
	8. At the end of the contract, the third party must return or destroy all Department technical connectivity information at the external site and all third party access rights to the Department's IT assets must be removed.	GITO, DGITO, SITA, IT Outsourcer	Termination of Contracts	Third party Contractual Procedure	Yes
8.2 Third Party Management					
	1. External IT consultants, computer security response teams, contractors or temporary staff who require access to the Department network are specifically prohibited from doing so unless it has been approved by the GITO.	GITO, DGITO,	Ongoing	Third Party Access Procedure	Yes
	2. Access to the Department's information processing facilities by third parties must be controlled.	GITO, DGITO, SITA, IT Outsourcer	Ongoing	Third Party Access Procedure	Yes
	3. Third party access to Department information assets will only be authorised in cases where there is a clearly defined business need. The access facility provided should limit the third party to the agreed method of access, the agreed access rights and the agreed level of functionality.	GITO, DGITO, SITA, IT Outsourcer	Ongoing	Third Party Access Procedure	Yes
	4. It must be ensured that external and Third Party connections to the Department's network, obtain prior approval of the	GITO, DGITO, System Owner /	Ongoing	Third Party Access Procedure	Yes

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
	system owner(s), the information process owner (if different from system owner) and the GITO, and that they are adequately protected against any forms of malicious code such as viruses.	Information Process Owner			
	5. Unless specified otherwise by the contract, the third party must comply with all Department information security policies. Information assets that have been entrusted to a third party should only be used by that third party for the purposes agreed on within the contractual agreement. Department information must not be disclosed to any non-department party for any purpose other than the one that has been expressly authorised by the Department.	GITO, DGITO, SITA, IT Outsourcer	Ongoing	Outsource and Third Party Contractual Procedure	No
	6. The confidentiality and integrity of sensitive information must be protected over connections with third parties. A formal risk analysis must be conducted for each third party connection and appropriate controls must be implemented to reduce risks to an acceptable level. The level of protection required will be determined by the assessed risks and the classification given to the connection.	GITO, DGITO, SITA, IT Outsourcer	Ongoing	Risk Management Procedure	Yes
	7. Third party access to Department information assets and in particular, access to customer data must be in accordance with legal and regulatory requirements for trade and business secrecy and data protection.	GITO, DGITO, SITA, IT Outsourcer	Ongoing	Third Party Access Procedure	Yes
	8. All third party employees should agree in writing to maintain strict secrecy concerning Department information. The third party should ensure that all its employees and agents who have access to Department information are aware of and carry out their security responsibilities with respect to that information.	GITO, DGITO, SITA, IT Outsourcer	Ongoing	Outsource and Third Party Contractual Procedure	No
	9. Default access by third parties to Department information assets are required to be set to “no access” (i.e., all access rights should be explicitly granted). When granted, third party access to Department information assets should be for the minimum necessary period of time. The granting of access rights should follow the principle of “Least Privilege” and be based upon a valid “Need-to-Know.	GITO, DGITO, SITA, IT Outsourcer	Ongoing	Third Party Access Procedure	Yes
	10. When third party access needs to be granted with system-level privileges (e.g., root or super user level access), such accesses are to be established for a limited duration, and preferably de-activated when not required. The access usage may be subject to supervision and should be fully logged.	SITA, IT Outsourcer	Ongoing	Monitoring Procedure; Third Party Access Procedure	Yes
	11. A regular review of all previously approved third party access	GITO	Every three months	Third Part Access	Yes

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
	must be conducted by the GITO. Any changes to the conditions upon which the third party access was previously granted must be reviewed by GITO.	DGITO,		Procedure	
	12. Third party access must be governed by formal agreements, which must include: • The definition of security administration, management, control activities and service level commitments to/from the third party; • The separation of Department data from other companies' data, if on an external system; • The restrictions on copying information and securing assets; • The requirement to prohibit access to Department data and systems without explicit authorisation from the Department and to maintain a list of individuals who have access to such data or system; • Requirements of the third party to comply with any necessary security standards and procedures e.g. logical and physical access rights; • The right of the Department to monitor (and revoke) administrator rights; • Facilities to rapidly disable any individual user ID; • The responsibilities of both parties and procedures for reporting and handling security incidents; • The right of the Department to audit contractual responsibilities; • The right of the Department to perform on-site inspections of the data centre of external companies; • The implications on business continuity plans; • The right of the Department to perform on-site inspections of the data centre of external companies; • The implications on business continuity plans; • The measures to ensure the return and/or destruction of information and other information assets at the end of the contract; • The approval of the Department if the external company wants to further outsource activities regarding services executed for the Department; • Actions to be taken upon termination of the outsourcing contract; • Detail specification of the outsourced service; • Well-defined level of service quality; and • Confidentiality clauses, to ensure the third party	GITO, DGITO, Risk Manager, SITA, IT Outsourcer	Ongoing	Outsource and Third Party Contractual Procedure	Yes

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
	connection do not make unauthorised use of the Department's information.				

9. Information Security Training – Information Technology Operations

Purpose	To ensure that all Department employees have the appropriate competencies and receive the required training to maintain appropriate protection of information assets.
Scope	This policy applies to all Department IT users, Third Parties and outsourcers who have access to Department information and/ or are utilising applications and computer installations.
Target audience	The persons responsible for complying with and implementing sections of this policy, relevant to their responsibilities, are the Government Information Technology Officer (GITO), Provincial Information Security Manager (PISM), SITA, System Owners (SO), Data Owners (DO), IT Outsourcers and Service Providers.
Summary of policy	The policy aims to ensure that an Information security training framework is established to initiate and control the implementation of information security within the Department.
Details of the policy	The requirements for complying with this policy are set out in the following sections: 9.1 Information Security Training

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
9.1 Information Security Training					
	1. All The Department technical and IT Operations staff must receive training on Information security threats and safeguards, and the extent of the training should reflect staff member's individual responsibility for configuring and maintaining Information security safeguards. Where IT staff change jobs, Information security needs must be re-assessed and new training provided as a priority.	GITO, DGITO, PISM	As required		No

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
	2. All new staff are to receive mandatory Information security training as part of induction. The induction training should include training on the contents of the Department's information security policies.	Human Resource department, GITO, DGITO, PISM	Upon new user join	Security Awareness training	No
	3. An appropriate summary of the Information security policies must be formally delivered to, and accepted by, all temporary staff and contractors, prior to their starting any work for the Department.	GITO, DGITO, PISM, Business Owners	Before contractor work commences		No
	4. The Information security functions and Department management should provide training to all users of new systems to ensure that their use of the system does not compromise Information security.	GITO, DGITO, PISM, System Owners	Before system is released into production	Procedure for Training of New Systems	Yes
	Policy Statements	**Responsible Person**	**Frequency**	**Related Procedures**	**Technology Dependent**

10. Prohibited and Proprietary Software – Information Technology Operations

Purpose	To ensure that The Department owned and personal software does not introduce risks to The Department's information system environment and that proprietary The Department software is protected.
Scope	This policy applies to all The Department application and computer system software, as well as personal software and shareware.
Target audience	The persons responsible for complying with and implementing sections of this policy, relevant to their responsibilities, are the Government Information Technology Officer (GITO), Provincial Information Security Manager (PISM), System Owners (SO), Data Owners (DO), SITA, Outsourcers, Service Providers, all Department IT users, IT Third Parties, Contractors and Temporary Staff
Summary of policy	This policy aims to ensure that prohibited software is not introduced to the information system environment of the Department and additionally that the copyright of Department owned software is maintained.
Details of the policy	The requirements for complying with this policy are set out in the following sections: 10.1 Prohibited Software 10.2 The Department Owned Software

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
10.1 Prohibited Software					
	1. The following software is prohibited from being installed on any Department information system: • *Bootlegged Software*: Illegal "pirated" or "bootlegged" copies of software or data are not permitted on Department systems. • *Powerful System Tools*: Programs that are designed to investigate and/or exploit the Department's information security environment (including password crackers, scanners, network sniffing devices, network packet sniffing devices and other "hacking" tools) are prohibited, except when expressly authorised by an appropriate member of the Information Security Function. • *Shareware/Freeware*: All software available from the Internet, where no licensing requirements are given, are not to be downloaded to Department equipment, except when expressly authorised by an appropriate member of the Information Security Function. • *Personal/Non-department Software*: Only upon approval from the Information Manager may personal software be installed on Department equipment. The Department therefore reserves the right to access and/or remove such software when there is neither reasonable justification nor approval for such installations.	PISM, SITA, IT Outsourcer	Ongoing	Software Scan Procedure, Monitoring Procedure, System Configuration Procedure	Yes
	2. Inappropriate Content: Images and/or text involving racial, nudity or sexual themes are not appropriate for the workplace and reduce the availability of Department resources. These items may never be stored in or displayed on Department equipment.	SITA, IT Outsourcer	Ongoing	Software Scan Procedure, Monitoring Procedure, System Configuration Procedure	Yes
	3. If, at any stage a user believes that a particular software product, whether freeware, shareware or proprietary software, would assist in the furtherance of the Department's business then a written motivation must be sent to the GITO for approval.	GITO DGITO,	Ongoing	Software Scan Procedure	No

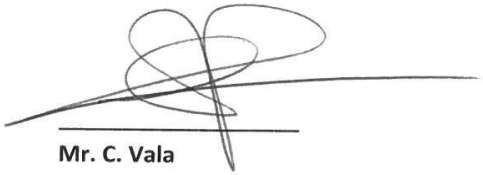
	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
10.2 Department Owned Software					
	1. Software developed by the Department or third parties on behalf of the Department are proprietary to the Department and third parties. In order to protect its proprietary interests and to ensure compliance with the terms of applicable licences, all Department IT users, IT Third Parties, Contractors and Temporary Staff are expressly prohibited from: • Copying Department software for use on any computer other than the Department supplied Personal Computer without the written permission of the GITO having the authority to grant such permission; • Copying or granting access to Department software for distribution to independent contractors, clients or any third party; •	System Owner, GITO, DGITO, SITA, IT Outsourcer	Ongoing	Software Scan Procedure, Third Party Access Procedure, System Development Procedure, System Configuration Procedure	Yes

11. Information Security Wireless – Information Technology Operations

Purpose	The purpose of this policy is to ensure that wireless environments are controlled and based on business requirements.
Scope	This policy applies to all Department IT users, Third Parties and outsourcers who have access to Department information and are utilising wireless data communications devices.
Target audience	The persons responsible for complying with and implementing sections of this policy, relevant to their responsibilities, are the Government Information Technology Officer (GITO), Provincial Information Security Manager (PISM), SITA, System Owners (SO), IT Outsourcers and Service Providers.
Summary of policy	This policy prohibits access to Department networks via unsecured wireless communication mechanisms.
Details of the policy	The requirements for complying with this policy are set out in the following sections: 11.1 Information Security Wireless Communications

	Policy Statements	Responsible Person	Frequency	Related Procedures	Technology Dependent
11.1 Information Security Wireless Communications					
	1. All wireless Access Points / Base Stations connected to the Department's network must be registered and approved by GITO. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in corporate laptop or desktop computers must be registered with GITO.	GITO, DGITO, System Owners, SITA	As Required		Yes
	2. All access points (APs) must be logically secured to prevent unauthorised access to the AP configuration environment. These AP devices must be configured to only allow pre-defined authorised administrators to make configuration changes. AP's must also be physically secured to protect the AP against physical manipulation.	GITO, DGITO, System Owners, SITA	As Required		Yes
	3. All wireless LAN access must use Department-approved vendor products and security configurations.	GITO, DGITO, System Owners, SITA	As Required		Yes
	4. All computers with wireless LAN devices must utilise a Department-approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point to point hardware encryption of at least 56 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address.	GITO, DGITO, System Owners, SITA	As Required		Yes
	5. The SSID shall be configured so that it does not contain any identifying information about the Department, such as the Department, division title, employee name, or product identifier.	GITO, DGITO, IM	As Required		Yes
	Policy Statements	**Responsible Person**	**Frequency**	**Related Procedures**	**Technology**

APPROVAL



Mr. C. Vala
Information Technology
Office of the Premier, Northern Cape, Kimberley

30/09/2015
Date