LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
COOPERATIVE GOVERNANCE,
HUMAN SETTLEMENTS & TRADITIONAL AFFAIRS

INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY POLICY

Revised Date: 26 September 2011
Version: Final

Version Control

Version	Date	Author(s)	Details
Draft 1.0	17/01/2011	Leon Nieuwoudt	Draft Information Security Policy
Draft 2.0	11/02/2011	Leon Nieuwoudt	Amendment based on comments from Policy and Research division
Final draft	9/03/2011	Leon Nieuwoudt	Amendment based on comments from Policy and Research division
Final	28/03/2011	Leon Nieuwoudt	Changing of final draft to Final after circulation period to staff members
Final	26/09/2011	Leon Nieuwoudt	Update of departmental name change

Contents

1. Preamble

Increasingly, departments and their information and communication 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 and communication systems and services means departments are more vulnerable to security threats. Management shall set a clear policy direction and demonstrate support for, and commitment to, information and communication system security through the issue and maintenance of this information and communication system security policy and standards across all COGHSTA offices. This document shall be read in concurrence with the Minimum Information Security Standards (MISS).

2. Terms and definitions

Accountability: ensuring that the actions of an entity/individual may be traced uniquely to that entity/individual, who may then be held responsible for that action

Authentication: establishing the validity of a claimed entity/verification of the identity of an individual or application

Availability: being accessible and useable upon demand by an authorised entity

Confidentiality: the principle that information is not made available or disclosed to unauthorised individuals, entities or processes

identification and authentication: functions to establish and verify the validity of the claimed identity of a user

information and communication systems: applications and systems to support the business, utilising information technology as an enabler or tool

information technology: any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of vocal, pictorial, textual and numerical data or information

integrity: the inherent quality of protection that maintains the accuracy of entities of an information and communication system and ensures that the entities are not altered or destroyed in an unauthorised manner

monitoring: performance measurement to ensure the confidentiality, availability and integrity of operational systems and information

password: confidential authentication information composed of a string of characters

remote access: the access of remote users to corporate IT services by means of telephone lines or 3G data card through a gateway/computing that is performed at a location that is distant from a central site, over a network connection

GITO: Government Information Technology Office(r)

VPN: Virtual Private Network

RAS DIAL-BACK: Method of using a telephone line to dial into the network

Espionage: Obtaining electronic data while not being authorised for personal gain

Cryptographic devices: Devices to encrypt and decrypt electronic data

COGHSTA: Department of Co-Operative Governance, Human Settlements and Traditional Affairs

3. Purpose

The purpose of this policy is to provide the COGHSTA with an information and communication system security policy in order to apply an effective and consistent level of security to all information and communication systems that process COGHSTA information.

4. Objectives of this Policy

The objectives of this policy are to:

a) apply cost-effective protection to security classified information which is processed by COGHSTA information and communication systems;

b) apply a reasonable level of protection to unclassified information so that COGHSTA offices can exercise control over that information, particularly in relation to public release;

c) be able to demonstrate accountability by a structured method of information and communication system security implementation and verification across COGHSTA offices; and

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

5. References and Related Legislations and Regulations

The following publications govern the execution of the Information Security Policy and were taken into consideration during the drafting of the guidelines and policy:
State Information Technology Act (Act no 88 of 1998).
Protection of Information Act (Act no 84 of 1982).
Minimum Information Security Standards (MISS), Second Edition March 1998
Departmental Internet Usage Policy,
Departmental Email Policy,
Departmental Password Policy,
Departmental Security Policy,
Departmental ICT Equipment Usage Policy.

6. Scope of the policy

This policy is applicable to all employees of the COGHSTA, including learners and interns as well all other stakeholders who make use of the COGHSTA ICT network.

7. Information System Security

7.1 Individual accountability

a) All personnel who use/access/perform any function on or manages any part of the Departmental Information Technology Systems are responsible and accountable for following appropriate recommended procedures and for taking all possible steps to safeguard the information handled by that system and any sensitive assets involved. All Information Technology Systems shall provide means by which individual users can be uniquely identified and held individual accountable for their actions, in respect of which the system shall provide for appropriate records.

b) All users of the Departmental Information Technology systems are responsible, within the span of their control, to ensure that no actions are taken which could degrade or compromise the confidentiality, the level of accuracy, completeness, dependability and responsiveness levels of the programmes, services and information handled by the system.

c) Users of the systems shall report any observed or suspected action/security weaknesses in, or threat to, systems or services to GITO.

d) GITO is the overall custodian of this policy.

7.2 Controlled access

a) An employee of the COGHSTA shall be granted access to only the classified level of information and assets for which appropriate access authorisation(s) and the need to know have been approved.

b) A person shall be granted access to only those Information Technology system resources necessary to perform the assigned functions and only when such access will not lead to a breach of this or any other security principles.

c) Appropriate segregation of duties, specifically allocated and defined in writing, shall apply.

d) Controlled access will be achieved via physical and procedural means. Unique identification of the user to the system must be provided. An access authorisation structure shall determine access and privileges, grant such access and privileges and record, control and monitor these.

7.3 Categorisation of information and information classification system

The comprehensive information classification system as developed by the Security Manager in terms of the Departmental Security Policy shall apply to the categorisation and classification of information. Refer to the Departmental Security Policy section 6.2.2.3.1 – page 9 of 19.

7.4 Levels of protection

a) The protection applied to information technical systems shall be commensurate with the sensitivity levels of the information and assets involved and shall take into consideration the identified threats to and vulnerabilities of the information system.

b) Risks or threats that Information Technology systems are exposed to shall be identified, analysed, evaluated and quantified in terms of the probability of them occurring and the potential impact of such an event of the COGHSTA and its activities. A documented security plan should exist to manage risk situations, which should be revised on a regular basis.

7.5 Disaster Recovery Plan

An approved disaster recovery plan and procedures should exist to minimize the impact of any type of disaster on the Information Technology Systems. It should be classified as Top Secret and handled on a need-to-know basis.

7.6 Security education

Officials who have access to systems should be subjected to a programme of effective and appropriate security education to foster their security awareness on risks and the approved Information Technology system principles.

7.7 System access control and password security

a) Access to computer systems shall be controlled by means of an approved computer access control system which identifies the authorised user and verifies his/her identity.
b) The access control system shall update an audit trail of all authorised and unauthorised efforts to gain access to the computer systems. Unauthorised access attempts shall be considered a breach of security.
c) Passwords shall be individual and exclusive, and shall not be disclosed without authorisation in forced exceptional cases, and without documenting the incident. Unauthorised disclosure of passwords shall be considered a breach of security.

7.8 Desktop and laptop security

a) Desktops shall be located in a physically protected environment where access control measures have been instituted and are applied consistently. Unattended equipment shall have appropriate security protection.
b) All portable computers are governed by the Departmental ICT Equipment Usage Policy.
c) Access to computers on which classified data is processed, shall be controlled and limited by means of approved access control software.

7.9 Physical security

Areas where computer-related equipment are accommodated, or office areas where classified information is dealt with, shall be protected in such a way that unauthorised access is prevented. Access control systems and procedures should regulate, record and monitor movement in these areas.

7.10 Utilisation of private computers

When private computers are used, written approval shall be obtained from GITO to use a private computer for official purpose. A computer register shall be established containing full personal particulars of the person, as well as details of the computer. Classified information bearing a sensitivity of Confidential or higher shall not be stored on a private computer.

7.11 ICT Hardware and Software

The procurement and usage of hardware and software shall be done in accordance with the Department ICT Equipment Usage policy.

8. ICT Communication Security

To ensure a safe environment in which information of a classified nature could be communicated, electronically or verbally.

8.1 Security of data transmissions

Communication pertaining to classified information should be encrypted in accordance with the COGHSTA approved cryptographic devices.

8.2 Modems/dial-up communications

No modems shall be connected to communication networks without the authorisation from GITO. Authorisation shall only be given on receipt of a detailed motivation approved by the particular employee's Senior Manager, requesting such facilities and a security plan detailing the manner in which the use of the modem and classified information transmitted through this modem will be regulated and controlled.

8.3 Electronic mail

The use of electronic mail and internet is governed by the Department Electronic mail and Internet usage policy.

8.4 Other mobile devices

Other mobile devices like I-Pads and mobile smart phones shall be allowed to connect to the Department's email facility for sending and receiving of emails. These mobile devices shall be correctly configured to access the Departmental email facilities as per the device operational manual. Users shall familiarise themselves with the operation of these devices and the security risks involved.

9. ICT Security System Controls

9.1 Security and computer viruses

In order to secure the network it is necessary that:

a) If any desktop or laptop or server poses a risk to the network, other hosts or service delivery, the host shall be disconnected from the network until the risk has been resolved.

b) Access to any desktop or laptop or server shall not be prevented by any logical or physical means. Default access granted by the network may not be removed.

c) All desktops, laptops and servers shall use the latest security patch levels, as approved by GITO.

d) The computer name of all desktops, laptops and servers shall contain the exact username of the owner, unless authorised by GITO.

e) GITO shall maintain virus-scanning software to protect the departmental network against any virus attacks.

9.2 Firewall and perimeter security

The department's secure network is protected from the internet and non-secure networks with firewalls and Intrusion prevention systems.

a) External network connections to the internal network may only be used for the purpose(s) it was authorised and intended for. All services being accessed from external or non-secure networks shall use secure protocols.

b) Wireless devices and VPN access are not allowed on the department's network, unless provided by GITO.

c) RAS dial-back shall be activated and only to a pre-defined and authorised telephone number.

d) GITO has to approve all exceptions to abovementioned connection requirements.

e) VPN network extensions are only permitted making use of secure tokens, managed and supplied by GITO.

10. Security breaches

10.1 Responsibility for reporting breaches of security

a) All employees have the responsibility to report any incident of security breach to GITO.

b) Breaches of security shall at all times be dealt with using the highest degree of confidentiality in order to protect the official(s) concerned and prevent him/her from unnecessary injustice.

11. Consequences of non-compliance

Non-compliance of this policy may lead to disciplinary actions, legal liability as well as dismissal.

12. Implementation

This policy comes into effect from the date of approval.

13. Policy review

This policy shall be reviewed annually.

COMPILED BY

---------- ----------

SENIOR MANAGER: Acting

INFORMATION TECHNOLOGY

28/09/2011

DATE

ACKNOWLEDGED BY:

ICT security policy revised to reflect Auditor-General's recommendations and the departmental name change

28-09-2011

GENERAL MANAGER: **DATE**

GOVERNMENT INFORMATION TECHNOLOGY OFFICE

ACKNOWLEDGED BY:

Noted and Supported for approval.

26/10/2011

SENIOR GENERAL MANAGER: **DATE**

SHARED SERVICES

ADOPTED /~~NOT ADOPTED~~:

02/11/11

HEAD OF DEPARTMENT **DATE**

APPROVED/~~NOT APPROVED~~

Approved

HONOURABLE MEC

04/11/2011

DATE