




# education

Department of Education  
**REPUBLIC OF SOUTH AFRICA**

## **INFORMATION TECHNOLOGY POLICY (ITP)**

**MARCH 2008**

Document No:	<b>ITP0002</b>
Revision:	<b>2.0</b>
Author:	Mr. A Raubenheimer and Mr. H Barnard
Approved:	
Effective Date:	<i>16 May 2008</i>

## TABLE OF CONTENTS

<b>1. Aim. ....</b>	<b>3</b>
<b>2. Legislative framework.....</b>	<b>3</b>
<b>3. Definition of terms.....</b>	<b>3</b>
<b>4. Scope and application.....</b>	<b>6</b>
<b>5. Classification of information access levels.....</b>	<b>6</b>
<b>6. Access to the IT infrastructure.....</b>	<b>6</b>
6.1 Data access controls and user account management.....	6
6.2 Use and ownership of information.....	7
6.3 Remote access and dial-in services.....	8
6.4 Information security classification and responsibilities.....	9
6.5 Network security.....	9
6.6 Trusted points.....	10
6.7 Network segmentation.....	11
6.8 File server security.....	11
6.9 Security of workstations.....	12
6.10 Security of portable computers.....	13
6.11 Storage, removal and disposal of computers.....	13
6.12 Information storage space.....	14
<b>7. Access to application system and system development .....</b>	<b>14</b>
<b>8. Personnel security.....</b>	<b>21</b>
<b>9. Access to the Internet.....</b>	<b>22</b>
<b>10. E-mail policy.....</b>	<b>24</b>
<b>11. File transfer protocol services.....</b>	<b>26</b>
<b>12. Misconduct.....</b>	<b>27</b>
<b>13. Risk management, audit and review.....</b>	<b>28</b>
<b>14. Disclaimer against liability.....</b>	<b>29</b>

## 1. Aim

- 1.1 To provide for measures that should be applied in the Authorization of Information Technology systems and to provide for security measures required to access the information systems of the Department.

## 2. Legislative and policy framework

- 2.1 This policy derives its authority from prescripts contained in the following Acts and policies:
- (a) Minimum Information Security Standards (MISS).
  - (b) State Information Technology Agency Act (Act no. 88 of 1998).
  - (c) SACSA/090/1(4) "Communication Security in the RSA".
  - (d) Protection of Information Act (Act No. 84 of 1982).
  - (e) Promotion of Access to Information Act (Act No. 2 of 2000).
  - (f) Electronic Communications and Transaction Act (Act No. 25 of 2002).
  - (g) Copyright Act (Act no. 98 of 1978).
  - (h) National Strategic Intelligence Act (Act No. 39 of 1994).
  - (i) National Archives of South Africa Act (Act No. 43 of 1996).
  - (j) Public Service Act (Proclamation No. 103 of 1994).
  - (k) State and SITA procurement regulations and policies
- 2.2 The policy addresses end-user information technology by defining guidelines for the optimum Authorization of IT systems.

## 3. Definition of terms

<b>Accreditation</b>	An official acknowledgment that a particular service or product could be applied in government systems.
<b>Accrediting authority</b>	A jurist or organ of state appointed by Cabinet to accredit services or products.
<b>Audit</b>	Actions that are taken to detect and investigate events that might deviate from specified procedures or policies.
<b>BIOS</b>	Basic Input Output System – Software that has been hardwired on the computer hardware that directs operations of the machine and security settings required for the machine to operate optimally.
<b>Certification</b>	Confirmation that there is compliance with the security policy and standards.

<b>Certifying body</b>	A body appointed to certify products, information system domains, and or inter-domain connections.
<b>Configuration control</b>	The management of changes made to hardware, software, firmware and documentation of a system throughout the development and operational life cycle of the system.
<b>Disclaimer on e-mails</b>	This e-mail is intended only for the addressee named above. As this email may contain confidential or privileged information, if you are not the named addressee or the person responsible for delivering the message to the named addressee, please contact the Department of Education.
<b>Discretionary access control</b>	An access control mechanism that allows users that have been assigned certain access privileges to exercise their discretion in granting other users the same access to system resources, in particular to information.
<b>Enterprise security management</b>	The security control and administration of multiple platforms, including distributed as well as mainframe systems, in order to provide for uniform application of security policies.
<b>Information systems (IS)</b>	Applications and systems to support the business with information technology as an enabler or tool.
<b>Information systems security (ISS)</b>	To preserve the availability, integrity and confidentiality of information systems and information according to affordable security practices.
<b>Information technology (IT)</b>	All aspects of technology that are used to manage and support the efficient gathering, processing, storing and dissemination of information as a strategic resource.
<b>Inter-domain connection</b>	A connection (including a manual connection) between two separate computer domains for the purpose of the sharing or exchange of information or other resources.

<b>Local area network (LAN)</b>	A high-speed communication infrastructure that enables users to share resources such as hardware, software, data or Wide Area Network (WAN) communication in a cost-effective manner.
<b>Local area network security</b>	The protection of the confidentiality, integrity and availability of all information that is provided or obtained by a LAN, as well as that of the LAN resources.
<b>Logical access control</b>	Access control mechanisms that are implemented and enforced by network operating systems, operating systems, application software and communication processes (e.g. authentication, resource access, audit etc.).
<b>Mandatory access control</b>	An access control mechanism that partitions system resources according to the sensitivity of the information that is contained in the objects, and the formal authorization (e.g. security clearance) of subjects to access information of such sensitivity on a need to know basis.
<b>MISS</b>	Minimum Information Security Standard – Minimum standards required to operate and configure security of systems and technology in government
<b>Monitoring</b>	Measures to ensure the confidentiality, availability and integrity of operational systems and information.
<b>System Development Life Cycle (SDLC)</b>	A methodology used to develop, test, document and commission software application systems
<b>Transversal Systems</b>	Applications and systems to support government staff and/or other sectorial functions with information technology as an enabler or tool (E.g. PERSAL, BAS and LOGIS).

<b>Trusted point</b>	A device that is capable of regulating the flow of traffic between two network segments in a manner that is appropriate to the classification of the networks
----------------------	---

#### 4. Scope and application

- 4.1 A person or any system component must be granted access to only that information and those assets for which appropriate access authorizations have been approved. Access must be limited to only those information system resources necessary to perform the assigned tasks.

#### 5 Classification of information and access levels

- 5.1 Systems and data are classified into four sensitivity areas with separate handling requirements. This standard data sensitivity classification must be used throughout the DoE. The classifications are defined below.
- 5.2 **RESTRICTED** is the classification that is allocated to all information that may be used by malicious or opposing or hostile elements to **inconvenience** the Department or an individual.
- 5.3 **CONFIDENTIAL** is the classification that is allocated to all information that may be used by malicious or opposing or hostile elements to **harm** either the objective or functions of the Department or an individual.
- 5.4 **SECRET** is the classification that is allocated to all information that may be used by malicious or opposing or hostile elements to **disrupt** the objective and functions of the department and an individual.
- 5.5 **TOP SECRET** is the classification that is allocated to all information that may be used by malicious or opposing or hostile elements to **attack or dismantle** the objective and functions of the institution and or state.

#### 6. Access to the IT Infrastructure

##### 6.1 Data access controls and user account management

- 6.1.1 User names and passwords for access to the LAN must conform to the following naming convention and password standards:
- (a) A user name must start with a surname followed by the initials of the employee. The format is ***surname.initial***

- (b) Password information will be valid for 30 days, after which users will be required to change their passwords.
  - (c) Passwords must contain a combination of alphabetic and numeric characters. Numeric characters should not be located at the beginning or the end of the password.
  - (d) A password must be longer than six characters.
  - (e) Passwords can only be repeated after 10 unique passwords have been assigned.
  - (f) A user will be locked out of the infrastructure after submitting three incorrect passwords. A lock-out can only be reset by IT support staff after a call has been logged.
  - (g) No user is allowed to share login information with other users.
  - (h) The use of control characters and other non-printing characters is discouraged, as it may inadvertently cause network transmission problems or unintentionally invoke certain system utilities.
  - (i) The display and printing of passwords must be masked, suppressed or otherwise obscured, so that other parties must not be able to observe or subsequently recover it.
- 6.1.2 Critical services will be open during office hours. Users need to apply for permission from the GITO to access critical services after office hours.
- 6.1.3 Any person using a DoE information system is expected to follow the required access and security procedures of the system. The formally appointed administrator/controller of the relevant system is responsible to manage the authorization of users, the level of tasks/access granted and the security requirements prescribed. Users must take all reasonable steps to safeguard the information that is handled by that system, as well as any sensitive assets that are involved. The administrator/controller of the systems must provide means by which user accounts can be regularly monitored and disabled if it is inactive for 30 or more days and/or resignation/transfer of the user. Controls should also be in place by which individual users can be held individually accountable for their actions.
- 6.1.4 The formally appointed System Controller of transversal systems (e.g. BAS, LOGIS and PERSAL) is responsible to manage the authorization of users, the level of tasks/access granted and the security requirements prescribed by the owner of the system. Controls must be put in place by the System Controller to manage and monitor the user accounts and to disable inactive accounts of 30 days and older and/or resignation/transfer of users

## **6.2 Use and ownership of Information**

- 6.2.1 While the DoE provides a reasonable level of privacy, all data created on the corporate systems remains the property of the DoE. Employees are expected to exercise good judgment regarding the reasonableness of using the infrastructure for personal use.
- 6.2.2 Without specific written exceptions, all programs and documentation that are generated or provided by employees, consultants or contractors, for the benefit of the DoE, remain the property of the DoE.
- 6.2.3 The DoE has legal ownership of the contents of all files that are stored on its computer and network systems, as well as all messages that are transmitted via these systems. The Director-General reserves the right to access this information without prior notice whenever a business need exists.
- 6.2.4 All equipment connected to the network of the DoE must run the approved anti-virus scanning software.
- 6.2.5 The DoE reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
- 6.2.6 The designated owner of the information asset must control access to systems. The owner of the information resource must ensure that all access to the resource that is granted is appropriate, justified and in accordance with the approved minimum standards set for information systems security.
- 6.2.7 It is an offence for any person to access, amend or delete other people's information without their permission or the permission of the Director-General.

## **6.3 Remote access and dial-in services**

- 6.3.1 Only wireless broadband remote access through a secure APN (SITA) will be considered by the Director-General where such a need arises. On approval of the Director-General the GITO Office will configure the SIM cards according to need and authorization and implement mechanisms to control this function.
- 6.3.2 The DoE staff with remote access privileges must ensure that the computers which are remotely connected to the DoE LAN are not connected to any other network at the same time. Login credentials should not be revealed to any other person.



- 6.3.3 Reconfiguration of the equipment of a home user for the purpose of split-tunneling or dual homing is not allowed.
- 6.3.4 All hosts that are connected to the DoE LAN via remote access technology must use the most up-to-date anti-virus software (refer to 5.2.4 and 6.9.3). This includes personal computers. Third party connections must comply with requirements as stated in the *third party agreement*.
- 6.3.5 Personal equipment that is used to connect to the DoE LAN should meet the requirements of the DoE-owned equipment for remote access.

#### **6.4 Information Security Classification and responsibilities**

- 6.4.1 It is the responsibility of the user to –
  - (a) Know his or her security clearance level and to understand the rights and limitations that are associated with that clearance,
  - (b) Ensure that all the data that he or she works with is correctly classified,
  - (c) Ensure that he or she understands the restrictions that are associated with the data that he or she works with, and
  - (d) Ensure that all the data that he or she works with is housed and protected appropriately.
- 6.4.2 Programme Managers will classify the security level of the information of people working under them.

#### **6.5 Network security**

- 6.5.1 This policy applies to –
  - (a) any network to which the DoE network equipment is connected,
  - (b) all equipment that is connected to the network as mentioned above,
  - (c) data in transit over any of the network mentioned above,
  - (d) network administrators that manage the equipment,
  - (e) project leaders that require new equipment to be connected to the network, and
  - (f) all users that utilise equipment that is connected to the network.
- 6.5.2 This includes, but is not limited to -
  - (a) the user LAN/VPN,
  - (b) the server LAN/VPN,

(c) WAN/VPN connections to remote sites and satellite connections.

6.5.3 DoE network equipment (routers, servers, workstations, laptops, etc.) must be classified and placed in a network segment that is appropriate to its level of classification. Access to network segments must be controlled in an appropriate manner. Whenever data travels over a network segmentation of a lower security classification, the data must be protected in a manner that is appropriate to its own classification level.

- (a) All physical network segment carriers must be classified.
- (b) All data that travels on the network must be classified.
- (c) All users that use network equipment or request data over the network must be assigned a level of clearance according to the same system.
- (d) It is the responsibility of the person that is designated as equipment user to have all equipment under his or her control classified.
- (e) Classification must be done in consultation between the owner (or an assigned representative) and the GITO.

6.5.4 Staff members must be given login credentials to execute their functions. It is an offence to access the network infrastructure using other login credentials not specifically allocated to a staff member.

6.5.5 All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as deemed relevant to their job function. The following topics should be covered in the security awareness program:

- (a) The importance of security to both the organisation and the individual,
- (b) Security needs and objectives for the information technology systems in terms of confidentiality, integrity and availability;
- (c) Implication of security incidents to the Department;
- (d) The objectives behind, and an explanation of, the corporate information security policy, operating policies, and the risk management strategy, thus cultivating an understanding of risks and safeguards;
- (e) Reason for restricted access to certain areas (authorised personnel, door locks, tags/badges, entrance log) and to information (logical access control, read/update rights), and why these restrictions are necessary;

- (f) The need to report actual and attempted breaches of security;
- (g) Procedures related to security compliance checking.

## **6.6 Trusted points**

- 6.6.1 A trusted point is equipment that is capable of regulating the flow of traffic between two network segments in a manner that is appropriate to the classification of the networks. The highest security level must be assigned to a trusted point that is used to segment two networks.
- 6.6.2 The default behavior of a trusted point must be to deny all traffic between the network segments that it protects.
- 6.6.3 At the discretion of the DoE GITO, the default behavior of the trusted point could allow all out-bound traffic from the network with the higher security level while denying all in-bound traffic.
- 6.6.4 At the discretion of the GITO, the trusted point could be configured to allow specific data into the network with the higher security level.
- 6.6.5 All trusted points must be completely under the control of the GITO. Access to any trusted point must only be granted with the explicit permission of the GITO, and under his or her close supervision.
- 6.6.6 Whenever there is a connection that skips one security level, strong user level controls must be used. Even if strong user controls are used, a connection must never skip more than one security level.

## **6.7 Network segmentation**

- 6.7.1 A network segment can only be classified at another security level with the approval of the DoE GITO.
- 6.7.2 Its new level of classification must be recorded in the change management document, and all divisional heads must be notified.
- 6.7.3 Wherever a network segment connects to another network segment with a different security level, an approved trusted point should control the connection between the two networks. No network equipment must be connected to a network segment that is not of the same security level where a trusted point could not be established.
- 6.7.4 The DoE GITO can choose to segment two networks of the same security level.

## **6.8 File Server security**

- 6.8.1 All file servers that host data and applications must be located in a physically secure environment in which access is strictly controlled.
- 6.8.2 Logical access to servers must be allocated on a need to know basis, in accordance with the access control policy of the DoE.
- 6.8.3 All servers must be loaded and protected with the latest approved anti-virus software. Updates must be implemented on a regular basis for patches, signature and upgrades.
- 6.8.4 Only one administrator must be given administrative rights on the servers. The administrator password must be kept secret, and only nominated personnel at the discretion of the GITO must have access to the password.
- 6.8.5 Data on the file servers must be backed up in accordance with the backup policy and procedures as outlined by the disaster recovery and backup policy.

## **6.9 Security of workstations**

- 6.9.1 All workstations must be located in a physically protected environment in which access control measures are in place and applied consistently. It must be ensured that unattended equipment has appropriate security protection.
- 6.9.2 Sensitive data must not be stored on local hard drives of workstations. All sensitive data that is processed using workstations must be saved on a secure network drive on a server.
- 6.9.3 A virus is a program that is secretly implanted on a computer and is designed to replicate itself until the entire machine and even any device connected to that machine is contaminated. All workstations should be loaded and protected by the latest approved anti-virus software. Users should under no circumstances-
  - (a) open any suspect or unknown emails;
  - (b) download any executable files from unknown websites;
  - (c) Make use of memory sticks on the LAN if it has not been scanned with the anti-virus software loaded on the departmental computer;
  - (d) Install any software on their work computers other than those sanctioned by the Department.

In the event of a suspected virus or undetermined growth in file sizes, the user should log a call to the SITA helpdesk, keep a print screen of

the error message and inform the technician about possible reasons for this problem.

- 6.9.4 It is the responsibility of the user to familiarise themselves with the appropriate security measures and the approved minimum information technology system security standards in the DoE to protect information stored on workstations.
- 6.9.5 Users should not leave their workstations unattended while accessing or processing information without appropriate protection like password-protected screen savers.
- 6.9.6 Workstations that are used to access sensitive information that is classified to be highly sensitive, must be protected by means of both a password-protected screen saver and a BIOS password.
- 6.9.7 It is the responsibility of the workstation user to ensure that his or her workstation is adequately protected from logical threats as well as physical environmental threats.
- 6.9.8 All users must log off from their workstations at the end of each business day.
- 6.9.9 No user is allowed to load a system that runs applications without the approval of the DoE GITO.

## **6.10 Security of Portable computers**

- 6.10.1 All portable computers (e.g. laptops, palmtops etc.) that contain classified data should be equipped with an access control and encryption capability that meets the prescribed security standard.
- 6.10.2 Users need to ensure that their portable computers are loaded with the latest anti-virus software by connecting it weekly to the DoE network and updating its platforms.
- 6.10.3 Users need to ensure that all data is backed up to the file servers on the network.
- 6.10.4 Any third party laptops connecting to the network must obtain approval from the relevant Manager before downloading any DoE information.
- 6.10.5 Stolen or lost portable computers must be reported to the Security and Asset Management Directorate.

## **6.11 Storage, removal and disposal of computers**

- 6.11.1 Hard disks of computers that contain secret and top secret information must be removed from the computer or formatted before the computer is disposed or repaired. If a hard disk cannot be removed, it must be presented to the GITO office to be physically destroyed. Storage media (i.e. stiffies, compact disks (CD), hard disks, Memory sticks) must be removed from equipment that is taken out for repairs.
- 6.11.2 Equipment that has been replaced by new equipment must be stored in a storage area for disposal. It is the responsibility of the owners of such equipment to copy any information they may need to their new equipment before the old equipment is initialised in readiness for disposal.
- 6.11.3 The GITO must certify equipment that is obsolete and is to be disposed of.

## **6.12 Information storage space**

- 6.12.1 Each user will be assigned a maximum of **50mb** for storage of information on the file server. Users who require more storage space should submit a written request to the GITO.
- 6.12.2 The size of data packets that are transmitted over the LAN is limited to the size of network throughput that is installed.

## **7. Access to application systems and system development policy**

### **7.1 User requirement specification**

- 7.1.1 User requirements for new systems and/or enhancements to existing systems must include the specific security requirements of the system, including the need for contingency arrangements.

### **7.2 Design specifications**

- 7.2.1 The preventative, detection and corrective security control requirements specified in the user requirement specifications that protect hardware, programs and data against deliberate or negligent changes, destruction, sabotage or espionage should be integrated into the system acquisition plan and incorporated into the design specification of the system. The following security controls must be considered:

(a) **System Architecture.** Security services and mechanisms must be

planned, designed, developed and tested in a way that correlates with the sensitivity of the application and or data and that complies with the guiding principles of this policy. The required security mechanisms (entity authentication; modification; detection; message authentication; profiles; encryption; audit facility; recovery mechanisms) for specific applications must be documented.

- (b) **Security grading.** The sensitivity of an application system must be explicitly identified and documented to allow for modular implementation of security mechanisms. Unnecessary security implementation must be avoided. If required, a high security application system must run in a dedicated (isolated) computer environment and only share resources with trusted application systems.
- (c) **Identification and authentication.** All users, data, programs, transactions, outputs and other system elements and sources must be uniquely and specifically identified during the design of the system and incorporated in a trusted information repository. Identification and authentication capabilities must be incorporated in the system design specifications to ensure verification of identities as well as individual accountability during system use.
- (d) **Non-repudiation.** Non-repudiation mechanisms must be incorporated in the system design specifications of sensitive and security classified systems.
- (e) **Confidentiality.** Provision must be made for encryption capabilities during the design phase of SECRET and TOP SECRET systems to ensure the confidentiality of data.
- (f) **Control.** The system must be designed in such a way that the various components (for example transaction modules, programs, operating system interfaces and databases) can exercise full control over the data or capabilities they share.
- (g) **Integrity.** The integrity requirements in respect of data, programs and their processing capability must be specified to ensure that the system performs its allocated functions within the time limit and precisely according to specifications. Security controls and integrity facilities must be incorporated in the design specifications to support system and data integrity. Hardware and software features must be provided to periodically test the correct operation of the hardware and firmware elements. Pre-determined self-checking routines must be built into software packages to ensure validation of data integrity, for example cyclic redundancy checks, modification detection codes and or message authentication codes.

- (h) **Recovery or availability.** The system design must ensure that there is no breach of security during system failures and that the loss of data or processing ability can be detected and repaired as soon as possible. It must be ensured that malfunction or failure of individual system components does not endanger the security of the system components and applications remaining active.
- (i) **Auditability or accountability.** All system and system interface activities must be identifiable and traceable. Appropriate controls (for example intruder alert) and audit trails or activity logs must be designed for application systems, including applications written by users. They must include the validation of input data, internal processing and output data.
- (j) **Separation of functionality.** System-related jobs should be structured to ensure that each has as little security exposure as is feasible for efficient operation. The intervention of more than one person must be required for the execution of critical tasks.
- (k) **Source data.** The source data must be accurate and complete in order to support the intended use. If new data sources are to be used, or if existing data is to be used for a new purpose, an in-depth study must be made of the additional requirement and application.

7.2.2 Detailed error handling procedures must be established.

7.2.3 Output control measures to verify the accuracy and integrity of processed information as well as the correct distribution of outputs must be implemented.

7.2.4 A backup system, which makes the recovery of data possible, must be in place. Backup and production data must be stored in geographically separate locations. The content of backup copies must be nullified before the medium (disc or tape) is used for other purposes.

7.2.5 A data disposal system must be established to ensure that archived data is disposed of in an orderly manner. Disposal must be performed in compliance with the National Archives of South Africa Act. Measures must be in place to ensure that sensitive information is not compromised in the disposal process.

7.2.6 Only authorised in-house and/or SITA technicians and/or developers/contractors with the appropriate security clearances must do system maintenance on hardware and software. All DoE system users must ensure that computer hardware and software are handled and used according to specifications.



### **7.3 Systems development**

- 7.3.1 Development requirements must be done in accordance with the SUMMIT methodology. Branch Heads must approve all system development and/or enhancement initiatives. Business units must submit the approved requirements/needs in the correct format to the ITC and BAC before it is considered by the Director-General. Procurement of services must be in accordance with the SITA Regulations.
- 7.3.2 Security requirements for the development of systems must be determined and the risks identified before the system is deployed for use.
- 7.3.3 Prior to live implementation of a system, SITA must review and certify -
  - 7.3.3.1 the security of the system; and
  - 7.3.3.2 its compliance to the Minimum Interoperability Standards for Government (MIOS).
- 7.3.4 No system will be put on production or hosted in the DoE production environment without -
  - 7.3.4.1 testing by the development team, in consultation with the GITO, SITA and the system owner. A security-testing plan must be drawn up for the testing of all the security features to ensure that the system operates as described in the documentation. The detail regarding what must be tested and what equipment should be used must be documented. ;
  - 7.3.4.2 acceptance and sign off by the GITO of all aspects of the system development life cycle (SDLC), including the testing results;
  - 7.3.4.3 completion of all system documentation and sign off by the GITO. All security aspects in respect of the system must be documented in full and the system administrator/controller, in liaison with the GITO, must update the documentation regularly.

### **7.4 System implementation**

- 7.4.1 All computer hardware and software must be implemented in terms of an acceptance/implementation plan that will ensure that the system is compliant to Government standards and compatible to the DoE infrastructure. The implementation plan must also address the activities related to the coordination and implementation of the security measures

and specify acceptance criteria to be met as well as compliance to the MIOS before the system is put into operation.

- 7.4.2 The implementation phase starts when the acquisition of the product or service has been finalised and ends when the system has been certified, accredited, implemented and accepted.
- 7.4.3 The implementation plan must also address the activities related to the coordination and implementation of the security measures and specify acceptance criteria to be met before the system is put into operation. Acceptance criteria must be clearly defined, agreed, documented and tested.

## **7.5 Configuration management**

- 7.5.1 In order to prevent fraud, sabotage, espionage, subversion and actions that endanger security, effective configuration management must be applied to systems that are in operation. Configuration items of a DoE system must be uniquely identified and controlled in order to determine and control the influence of a change to a configuration item on the system and system interfaces.
- 7.5.2 Configuration management must also ensure that any additions, omissions or changes that are made to the system are prioritize and do not compromise the set security measures.
- 7.5.3 Computer hardware and software must be implemented in accordance with an implementation plan. The implementation plan must address the activities that are related to the coordination and implementation of the security measures, and must specify acceptance criteria to be met before the system is put into operation.
- 7.5.4 Complete, updated manuals or documentation must be available to operators, programmers, system analysts, users and auditors, as applicable. Backup copies must be made of all electronic documentation and stored in a geographically separate location in a fireproof safe.
- 7.5.5 The use of system utility programs (e.g. monitoring or sniffing tools or debugging tools) that might be capable of overriding system and application controls must be restricted and tightly controlled.

## **7.6 Sensitive information**

- 7.6.1 Sensitive information must not be stored on unsecured media like local drives of workstations, removable disks/drives and/or the e-mail system

- 7.6.2 If needed, encryption technologies must be used to encrypt sensitive data that is stored on the network, e-mail and any electronic media.

## **7.7 Disaster recovery and backup**

- 7.7.1 The DoE must have a documented disaster recovery plan, approved and endorsed by senior management of the DoE for its systems, including information regarding transactions on transverse systems stored on DoE hardware. Disaster recovery plans must be tested, evaluated and continually updated.
- 7.7.2 The disaster recovery plans must be communicated to all parties that are responsible for the management and operations of the relevant IT infrastructure. The recovery plan must at least be classified CONFIDENTIAL.
- 7.7.3 Data backup procedures must be established and adhered to for all the information systems and operations.
- 7.7.4 Data backup devices must be kept in a safe off-site environment at separate buildings, in which it can be accessed with ease when needed.

## **7.8 Document security**

- 7.8.1 All documents, manual files and printouts must be classified in accordance with the prescribed information security classification of the DoE. It is the responsibility of the person accessing or using the documentation to understand the sensitivity of the material that is contained in the documentation.
- 7.8.2 Access to highly classified documents must be strictly controlled. Authorisation from the appropriate owner must be obtained. It is the responsibility of the owner to ensure that all requirements for access to the documentation are satisfied as outlined by the classification requirements and security status of the recipient.
- 7.8.3 Documents and sensitive data files must be kept in a safe environment. A backup procedure for all manual files and documents that are critical to the business of the DoE must be put in place to ensure the availability of information in the manual file system.
- 7.8.4 Sensitive documents must not be printed on network printers that are accessible to everyone.

- 7.8.5 Requests for access to highly classified documents must be scrutinised and logged if granted. All sensitive documents that are accessed must be accompanied by a business motivation and prioritised.
- 7.8.6 Systems and LAN documentation must be classified as SECRET. Access to this documentation must be strictly controlled. Only people that are prioritised to view, change or modify the system configurations must be allowed access to the documentation.
- 7.8.7 Documentation of systems and network operation must be kept and locked away in a safe place.

## **7.9 Change requests and approval**

- 7.9.1 The GITO must approve the following changes to IT resources:
  - (a) changes to network topology, new network equipment installation, upgrade to the network, network protocols, configuration;
  - (b) application and system configuration changes; and
  - (c) database changes.
- 7.9.2 A formal change management process must be established, including approval of change requests.
- 7.9.3 All changes must be made in accordance with an approved change management process of the DoE.
- 7.9.4 All approved changes must be monitored to ensure that it is implemented according to specifications.
- 7.9.5 The effects of changes must be analyzed before changes are approved and implemented.
- 7.9.6 It is the responsibility of the GITO to ensure that all approved changes to critical IT resources are at a minimal level of risk to the IT infrastructure.

## **7.10 Access to application systems**

- 7.10.1 The Account Managers (System Administrators/Controllers) of application systems must ensure that access to the system is granted to only those functions and assets for which subordinates must perform their assigned tasks.
- 7.10.2 The Account Manager must ensure that the service level agreements required are in place to manage the system include appropriate security and monitoring mechanisms with regard to the updating, maintenance and enhancement of the system software. These activities must conform

to system development and configuration management issues mentioned in paragraph 7.4 and 7.5 above.

- 7.10.3 The Account Manager of the system must ensure that the system has a secured authentication of login credentials and the system is able to monitor and report on unauthorized access.
- 7.10.4 Account Managers and System Controllers of transversal systems must have documented procedures in place to control user accounts, its profiles and activities. User accounts inactive for 30 days must be deactivated.
- 7.10.5 There must be an ongoing system monitoring process to maintain data integrity and to monitor access to the system.

## **8. Personnel security**

- 8.1 The employees of the DoE that access information systems, and the data that is processed by the systems, must meet the necessary security requirements as determined by the sensitivity of the information that is accessed. Access to the systems and data must be terminated immediately as soon as evidence of non-compliance with the security requirements is gathered.
- 8.2 IS security roles and responsibilities must be included in the job descriptions of all DoE employees who access IS systems/infrastructure.
- 8.3 All employees must sign a secrecy declaration and non-disclosure form not to disclose or reveal any sensitive information that they are privileged to access as a result of their job assignment.
- 8.4 Staff disclosing information to the media must do so with permission granted at an appropriate level of management in the DoE.

## **9. Access to the Internet**

### **9.1 Use of the Internet**

- 9.1.1 Use of the Internet is permitted and encouraged where such use is suitable for work purposes and supports the goals and objectives of the Department. Users are encouraged to take advantage of the following Internet services in the execution of their work:
  - (a) Sharing research and work related information among colleagues and like-minded individuals
  - (b) Communicating with others and transmitting files through the e-mail system.

- (c) Requesting and providing assistance on education related problems
- (d) Publicising products and services that promotes the interests of the department.

9.1.2 To ensure that the Government network resources are optimally used by government employees the Department of Public Service and Administration has instructed SITA to-

- (a) Monitor usage of the internet by employees;
- (b) Implement filters that will deny access to web content that is deemed inappropriate; and
- (c) Implement SPAM filters.

9.1.3 The DoE has migrated to a Virtual Private Network (VPN). In addition to the above monitoring and filtering the VPN will be configured to block the following live streaming:

Extension	Program and/or Extension Function	Specific Notes
MP3	MPEG Audio Stream, Layer III	Initial File Contents is for a file produced by the Xing Encoder. Note: This file type can become infected and should be carefully scanned if someone sends you a file with this extension.
AVI	Audio Video Interleave File	Recent files might be compressed with one or another codecs (compression standard). It can also be seen with QuickTime and RealPlayer (available for the Mac). A number of programs capture this file extension.
MPEG	MPEG 1 System Stream	
OGG	Ogg Vorbis Codec Compressed Multimedia File	Ogg is an open and standardized bit stream container format designed for streaming and manipulation. It was developed by the Xiph.Org Foundation. The file format can multiplex a number of separate independent open source CODECs for audio, video and text (e.g., subtitles). Ogg's various CODECs have been incorporated into a number of different free and commercial media players as well as portable media players from different manufacturers.
Wma	Windows Media Audio File	
Ra	Real Media Streaming Media	

9.1.4 The Department reserves the right to intercept and monitor access to the Internet by all staff. In compliance with Section 6(2) of the Regulation of Interception of Communications and Provisions of Communications-R Information Act (Act 70 of 2002), the above intent to filter and monitor the usage of the Government network (NGN) and the DoE VPN serves as notice to all DoE employees and other users (contractors, etc)

authorized to have access to e-mail services and the internet from the DoE and Government infrastructure..

## **9.2 Authority to access the Internet**

- 9.2.1 The Internet should be used in a manner that is consistent with the code of conduct contained in the Public Service Regulations and related Acts.
- 9.2.2 Access to the Internet is not a right and is limited to staff who use the Internet for work related functions. Approval to have permanent access to the Internet must be obtained from Director level or higher.
- 9.2.3 The Department has provided Internet access at the Resource Centre for staff who does not qualify for permanent access.

## **9.3 Conditions for use**

- 9.3.1 Employees are prohibited from publishing or reproducing or authorising the reproduction in any manner or form of all different types of works protected by the Copyright Act (Act 98 of 1978), as amended without prior consent of the copyright owner. This must include materials that have been copyrighted in other countries.
- 9.3.2 Employees are prohibited from importing in any manner or form all different types of works for which copyright exists without permission from the owner. This must include selling the works for monetary gain, letting, hiring or exposing such works for sale or hire, or distributing such works for any other purpose by which the copyright owner is prejudicially affected.
- 9.3.3 Employees are prohibited from broadcasting or transmitting or allowing public performance of works of any nature for which copyright exists and has not been granted to such employees. This includes patented works in a manner that prejudices the copyright owner.
- 9.3.4 The GITO will enforce the size of data packets allowed to be transmitted over the e-mail system in line with the size allocated to the network throughput by the internet service provider.
- 9.3.5 Employees are contractually bound to observe the policies, laws, regulations and practices of the Department.

## **9.4 Unacceptable practices on the Internet**

- 9.4.1 It is prohibited to knowingly access websites that contain obscene, defamatory or discriminatory material. It is prohibited to distribute child pornography, explicit violent sexual conduct, incitement to cause harm or explicit infliction of extreme violence, hateful speech or objectionable material, or material meant to annoy, harass or intimidate another person.
- 9.4.2 It is prohibited to knowingly send or receive unusually large e-mails or attachments which are not work related or are not related to employee benefits such as studies, research work, membership to approved interest groups, etc.
- 9.4.3 It is prohibited to use the Internet for private business activities for own enrichment to the detriment of the work of the Department.
- 9.4.4 It is prohibited to use the Internet for illegal activities, which are discouraged by the Constitution of the country, the South African School Act, the Public Service Regulations and related Acts. It is prohibited for staff to fraudulently manipulate electronic messages such that they appear as their own invention.
- 9.4.5 It is prohibited to make or post indecent remarks or jokes or objectionable materials. Accessing, uploading or transmitting commercial software or copyrighted material in violation of the copyright is not allowed. Downloading or accessing material such as those mentioned in paragraph 9.4.1 above is not allowed.
- 9.4.6 It is prohibited to intentionally interfere with the normal operation of the network, including the propagation of virus-infested messages or sustained high volume of network traffic, which substantially hinders others in their use of the network.
- 9.4.7 It is prohibited to intercept and or monitor other people's files, messages or software or revealing or publicising confidential or proprietary information which, includes, but is not limited to, financial information, strategic plans, database information and password information of other people without their prior consent.
- 9.4.8 Any person who causes or authorizes another person to use his or her own Internet login information for purposes that conflict with the conditions as set out in paragraphs 9.3 above must be deemed to have misused the Internet.



## **10 E-mail policy**

### **10.1 Use of electronic mail system (e-mail)**

- 10.1.1 The e-mail system is all the electronic mail systems and services provided by the DoE. It is a business communication tool and users are obliged to use the tool in a responsible, effective and lawful manner.
- 10.1.2 All DoE users must have access to the e-mail system, unless otherwise advised by the supervisor. It is the responsibility of the users to use the DoE e-mail service in a responsible, professional and ethical manner and to ensure that they are aware of the conditions for using the e-mail system.
- 10.1.3 Management must obtain access to users' official messages while they are off duty if it is deemed necessary.
- 10.1.4 Managers must report when a staff member is leaving the Department so that their access to the infrastructure can be terminated.

### **10.2 Unacceptable use of email**

- 10.2.1 If a user sends e-mail messages containing any libelous, defamatory, offensive, racist or obscene material or messages that may directly or indirectly lead to harmful behavior or material that may upset another person.
- 10.2.2 If a user sends/forward confidential and/or other classified information that can lead to premature disclosure of DoE classified information. Users must avoid sending confidential information by e-mail. If necessary and authorized, the information must be secured by including it in a file with password protection. The recipient must be provided with the password by means of other communication, e.g. by telephone.
- 10.2.3 If a user willfully sends an attachment that contains a virus with the intent to steal information and/or cause electronic harm.
- 10.2.4 If a user sends and/or open a virus infected file after notification of such types of e-mails and/or attachments.
- 10.2.5 If a user sends unusually large e-mails or attachments that are not work related, e.g. distributing chain letters, bitmaps and any other

material that add no value to official tasks and cause bottle-necks on the LAN/WAN.

- 10.2.6 If a user sends any e-mail that could lead to civil or criminal litigation against the DoE as the third party.
- 10.2.7 If a user uses the e-mail system for personal gain.
- 10.2.8 If a user intercepts and/or monitors other users messages.

### **10.3 User responsibilities and guidelines**

- 10.3.1 Users must notify their supervisors immediately when they receive e-mail containing libelous, defamatory, offensive, racist or obscene messages/attachments.
- 10.3.2 Do not forge or attempt to forge e-mail messages.
- 10.3.3 Do not send e-mail messages using another user's e-mail account without permission.
- 10.3.4 Do not disguise or attempt to disguise your identity when sending e-mail.
- 10.3.5 Do not use any form of Spam (the practice of e-mailing to all possible addresses, unsolicited and/or useless material).
- 10.3.6 Review e-mail messages on a weekly basis to remove the messages not needed.
- 10.3.7 Do not send announcements and circulars directly to group e-mail addresses such as "All Staff", etc. This should only be done by means of a "newsflash" through the Chief Directorate: Communications.
- 10.3.8 The DoE considers e-mail as an important means of communication and recognizes the importance of proper e-mail content and speedy replies in conveying a professional image and delivery of service. The following best practices could be considered when communicating via electronic mail:
  - (a) Write well-structured e-mails, use short descriptive subjects and sentences. Avoid writing messages in capitals.
  - (b) Avoid Internet abbreviations and characters such as smiley's.
  - (c) Signatures should include your name, job title and contact numbers.
  - (d) Do not send unnecessary attachments. Compress attachments larger than 1 MB.
  - (e) State clearly what action is expected when forwarding e-mails.
  - (f) Respond to e-mail received promptly.

- (g) Delete e-mail messages that you do not need a copy of and set your e-mail client to automatically empty your “deleted items” on closing.

#### **10.4 Personal use of e-mail services**

- 10.4.1 Although the DoE’s e-mail system is meant for business use, the reasonable personal/private use of the e-mail service is allowed on condition that:
  - (a) Personal use of e-mail should not interfere with work and should preferably be sent after work hours or during lunch time.
  - (b) Personal e-mails adhere to the guidelines and requirements of the policy.
  - (c) Personal e-mails are kept in a separate folder, named “Private” and deleted weekly.
- 10.4.2 The forwarding of chain letters, junk mail, jokes and executables and/or sending of bulk e-mails are strictly forbidden.
- 10.4.3 All messages distributed via the DoE’s e-mail system, including personal e-mails, are the property of the DoE.

#### **10.5 Retention and destruction of e-mail records**

- 10.5.1 Retention and destruction of electronic mail records shall be consistent with the Electronic Communications and Transaction Act (Act no. 25 of 2002), Section 16 with due consideration of the DoE’s infrastructure capacity and constraints.
- 10.5.2 The medium and/or method for retaining electronic mail records shall be determined and reviewed by the GITO, in accordance with the relevant applicable legislation.

#### **10.6 Limitations**

- 10.6.1 Users should take note that disk space, memory and LAN bandwidth are limited resources that should primarily be used for official communication.
- 10.6.2 The use of multimedia e-mail has a huge impact on the availability of the above-mentioned resources. Users must avoid sending large multimedia files via e-mail on the LAN/WAN. Receiving of private multimedia files (video clips, pictures and photos) is not allowed.
- 10.6.3 Users should under no circumstances download multimedia files.

- 10.6.4 Users should not send official correspondence via public mail services (e.g. Hotmail, Web-mail, etc.) unless pre-arranged with their supervisors.

## **10.7 Maximum message size**

- 10.7.1 The DoE's e-mail system is configured to allow a maximum message size of 3 MB for outgoing mail and 5 MB for incoming mail.
- 10.7.2 Users must use data compression utilities such as WinZip to send larger files.

## **10.8 E-mail storage quotas for staff**

- 10.8.1 Users are each allocated **50 MB** of mailbox storage space on the e-mail file server. The e-mail system must send alerts to staff whose mailboxes are over **45 MB** full. The e-mail system must automatically withdraw e-mail services if the mailbox is 95% full. Affected users must not be able to send and receive messages on their mailboxes.
- 10.8.2 Staff members who require more storage space on their mailbox should submit their requests to the GITO. A supervisor at least on the level of Director should approve such a request.
- 10.8.3 Users must manage and maintain their allocated disk space on the e-mail server. Users are expected to remove old e-mail messages from the "In box" and the "Deleted Items" folders at regular intervals. Attachments should be saved on the document storage area on the desktops or file server. The GITO must ensure the removal of e-mails that are older than three months at regular intervals as part of routine maintenance.

## **10.9 Monitoring of the e-mail system**

- 10.9.1 The DoE has the right to access a user's e-mail if there is sufficient justification for it to do so.
- 10.9.2 Passwords should not be given to other users and must be changed every 30 days. E-mail accounts inactive for 60 days will be deactivated and deleted.

## 10.10 Disclaimer

### 10.10.1 The following disclaimer will be added to each outgoing e-mail:

*'This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this email in error please notify the system manager. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the Department of Education. The recipient should check this email and any attachments for the presence of viruses. The Department of Education accepts no liability for any damage caused by any virus transmitted by this email.'*

## 11. File transfer protocols services (FTP)

### 11.1 File transfer protocol services (FTP) can only be considered with due consideration of the security of the VPN.

### 11.2 If allowed -

- (a) it must be hosted onto one FTP Server using one FTP platform and system;
- (b) account managers of applications/systems must apply for FTP services to the GITO providing a business case that justifies the need for the FTP service;
- (c) access to an FTP service must be controlled through the IT security credentials and the login credentials required to gain access to the application system;
- (d) the size and complexity of the files to be used in the FTP services must be determined by the capacity of the FTP file server;
- (e) the user of the FTP service must ensure that external FTP files are quarantined against viruses before an inbound transfer is initiated;
- (f) the account managers must control and manage an FTP session and must ensure that an FTP session is manually closed before they use information from the FTP files in their applications;
- (g) the GITO will remove all files that have been successfully sent or received on the FTP server after every five days as part of the maintenance of the FTP server; and
- (h) files on the FTP Server will not form part of the backup and disaster recovery procedures of the department.

## **12. Misconduct**

### **12.1 A person commits misconduct if he or she –**

- 12.1.1 intentionally accesses or intercepts any data without authority or permission to do so.
- 12.1.2 intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective.
- 12.1.3 utilises any device or computer program in order to unlawfully overcome security measures designed to protect such data or access thereto.
- 12.1.4 unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possess any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code, or any other similar kind of data with the intent to unlawfully utilize such item to contravene the contents of this policy.
- 12.1.5 commits any act described in this policy or any other Act in the country for the purpose of interfering with access to an information system so as to constitute a denial of service to legitimate users.
- 12.1.6 breaches any security measures/standards contained in this policy and/or other policies. It is the responsibility of account managers, system administrators/controllers to follow up all security incidents in an effort to ensure that they are appropriately dealt with according to the policies regulating discipline in the DoE.

### **12.2 Disciplinary procedure**

- 12.2.1 A person who commits misconduct contemplated in paragraph 12 above must be charged and prosecuted in terms of either the Employment of Educators Act (Act No. 76 of 1998) or the Public Service Regulations, as the case may be.

## **13. Risk management, audit and review**

- 13.1 The GITO must conduct a comprehensive risk analysis to determine the risk of the loss or disruption of information that requires protection against prioritised disclosure or loss or disruption.

- 13.2 The DoE reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
- 13.3 The audit findings and recommendations must be prioritised, and responsibility for implementation must be assigned.
- 13.4 Audit logs must be kept for all systems and applications. System administrators must review these logs on a regular basis. All suspicious activities that are identified must be reported and investigated.
- 13.5 The Department must implement a Network Monitoring System to regularly monitor compliance to the IT Policy. Deficiencies should be remedied within 24 hours.

#### **14. Disclaimer against liability**

- 14.1 The Department shall not accept liabilities from third parties if any of these policies have been transgressed for which third party claims are lodged against an employee. Equally, the Department shall not accept liability if employees transgress policies of third parties through the use of the IT infrastructure of the Department.