LIMPOPO

PROVINCIAL GOVERNMENT

REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF

EDUCATION

Limpopo Department of Education Information Technology Security Policy

Table of Contents

1. Introduction

1.1 since the democratic republic of south African government came into effect in April 1994 effect is given to the constitutional right of access to any information held by the state and any information that is held by another person and that is required for the exercise or protection of any rights, and to provide for matters connected therewith.

1.2 However the **PROMOTION OF ACCESS TO INFORMATION ACT NO 2 OF 2000(PAIA)** acknowledges the need for protection of sensitive information and therefore provide for justified exemption from disclosure of such information, that category of information which is exempted need protection.

1.3 Information in the wrong hands can damage operational relations between Government put people out of work, and can also result in declaration of war.

1.4 With the dawn of the computer age, people have a new technology to use and possible abuse.

1.5 The threat of espionage activities through theft of sensitive information and illegal eave dropping in South Africa is real. Widespread and the security of our information are at risk. Security hazards exist which are exploited by growing number of foreign hostile intelligence agents and unauthorised people.

1.6 The only way to counter the threat of espionage activities and unauthorised disclosure of sensitive information is to apply security measures in full. This Information Technology policy is aimed at providing the necessary procedures and measures to protect sensitive information from unauthorised disclosure. These procedures are not contrary to transparency, but indeed necessary for responsible government.

1.7 This policy document contains security guidelines, which are aimed at protecting the Government's assets, interests and activities, as well as classified matters and/or information about such matters, and the personnel involved. The procedures and measures taken up in this volume are based on general security principles and are in essence the minimum standard for handling classified information.

1.8 Apart from the above, it is important to note the philosophy stating that management (on all levels) must accept responsibility for security, and therefore become involved in protecting the assets of the Government, the so-called top-down approach. Generally it is the view that there can be no security –

- If there are no security standards or institutionalised policy on security.
- If these standards do not form a comprehensive system of measures;
- If this system of measures is not properly managed;
- If these measures are not adhered to or enforced; and
- If personnel are not security-conscious.

2.1. Allocating classification to information

2.1.1. **RESTRICTED:** Information must be classified as RESTRICTED when compromise thereof could hamper or cause an inconvenience to the Limpopo department of education or any institution dealing with the Department or individuals, but cannot hold a threat of damage. However, compromise of such information can frustrate everyday activities.

2.1.2. **CONFIDENTIAL:** Information must be classified CONFIDENTIAL when Compromise thereof leads to:

- The disturbance of the effective functioning of information & Operational systems
- Undue damage to the integrity of a person or Department or Dealing with a Department, but not entailing a threat of a serious damage. Compromise of such information, however, can frustrate everyday functions, led to an inconvenience and bring about wasting of funds.
- The inhibition of systems, the periodical disruption of administration (e.g. logistical problems, delayed personnel administration, financial relapses, etc) that inconvenience the Department, but can overcome; and the orderly, routine co-operation between institutions and / or individuals being harmed or delayed, but not bringing functions to a halt.
- The disruption of ordered administration within the Department and adverse effect on the non-operational Relations between institutions.

2.1.3. **SECRET** : information must be classified as SECRET when the compromise thereof:

- Can result in disruption of planning and fulfilling of tasks, i.e. the objectives of a Department or institution dealing with the Department in such a way that it cannot properly fulfill its normal functions ; and

- Can disrupt the operations co-operations between the Departments in such a way that it threatens the functioning of one or more of the Departments .

- Can damage operational relations between Departments and diplomatic relations between states.

- Can endanger a person's life.

2.1.4. **TOP SECRET** is used when the compromise of information results in:

(a) The functions of the Limpopo department of education being brought to a halt by disciplinary measures, boycotts or mass actions;

(b) The severing of relations between states can disrupt the effective execution of information or operational planning and / or plans;

(c) can seriously damage operational relations between Governments.

(d) Can lead to discontinuation of diplomatic relations between

States or Governments and can result in declaration of war.

2.2. Access to classified information

The rules and prescriptions as to who may have access to or inspect classified matters are as follows:

- A person who has an appropriate security clearance or who is by way of exemption authorized by the Accounting Officer of the Limpopo department of education or approval by security management and risk management unit

- The authorized person shall take prescribed oath and or declaration of secrecy.

- Persons who must necessarily have access to that classified information in the execution of their duties (the need to know principle) on condition that a suitable clearance has been issued or authorization has been granted , as explained above .

- Persons such as secretaries and personnel at smaller sections who in general do not have access to classified material and who do not have relevant security clearance, but are expected to have access to this information on an ad-hoc basis owing to the circumstances,will have access to such information on condition that the prescribed oath / declaration of secrecy was taken .

2.3. Handling of classified information

2.3.1. **Storage** of classified documents

- Classified documents that are not in immediate use must be locked away in a safe storage place.

- The doors of all offices in which classified documents are kept must at least be fitted with security locks, and must be locked when vacated, even for a short period, by the person (s) using the room.

- There must be proper control over access to and effective control over movement within any building or part of a building in which classified information is handled.

- All classified documents that are dispatched, made available or distributed, must be subjected to record keeping in order to ensure control thereof . This provision does not apply to documents that are classified as Restricted.

- When classified documents are not in use, it must be stored at records management registries in the following way :

  - **Restricted:** Normal filing cabinet
  - **Confidential:** Reinforced filing cabinets
  - **Secret:** Strong room or reinforced filing cabinet
  - **Top Secret:** Strong room, safe or walk-in safe

- The keys to any building , part of building , room , strong room , safe , cabinet or any other place where classified material is kept must be looked after with utmost care and effective key control must be instituted.

2.4. Removal of classified documents

- The removal of classified documents from office buildings is prohibited.
- Classified material (with the exception of restricted documents) shall not be taken home without the written approval of the Accounting Officer or his/her delegate; a list of the documents to be removed must be taken to a person in control of record keeping. Removal of classified documents form must be completed affected copy attached.

2.5. The typing of classified information

- Classified documents may be typed only by persons having appropriate security clearance or authority from the Accounting Officer of the Limpopo department of education. Such typing must be done in a manner that will ensure that the information is not divulged to unauthorised persons.
- Drafts of classified documents, copies and any storage media(memory stick, external hard drive, CDs, DVDs & etc) must at all times be treated as classified documents.

3. Purpose

The purpose of this Information Technology Security Policy Statement and its related policies, standards and procedures is to reduce the inherent risk of threats, whether internal or external, deliberate or accidental, to an acceptable level.

This document outlines Limpopo department of education's corporate policy for Information Technology Security and is supported by customized ICT policies, standards, procedures and guidelines to facilitate compliance to the requirements.

3.1. Objective	**This Information Technology Policy Statement is provided in order to:** • Define and document Limpopo department of education's policy with regards to Information Technology Security • Categorize the key Information Technology Security policy requirements for document Limpopo department of education users to comply with • Define and document department's Information Technology Security policies that would ensure compliance to the Information Security policy statement • Identify related documentation • Identify the persons responsible for maintaining the security requirements; and • Detail compliance requirements.
3.2. Definition	**Information Technology Security is defined as the preservation of the following three characteristics of information:** • Confidentiality – ensuring that information is accessible only to those authorized to have access. • Integrity – safeguarding the accuracy and completeness of information and processing methods. • Availability – ensuring that authorized users will have access to information and associated assets when required. In securing document Limpopo department of education's information, it is essential that the above characteristics be maintained at all times.

3.3. Applicability	This Information Technology policy applies to the entire Limpopo department of education and all its employees, including third Parties, temporary staff, contractors, service providers, and consultants. It covers the data networks, servers, personal computers and laptops located at Government and non-Government locations, as well as any other device used to process or facilitate processing Of department's data. This includes systems that are under the jurisdiction and/or ownership of Limpopo department of education, and all personal computers. This policy applies to the entire Limpopo department of education's information assets in any form including electronic or Paper based media. Additionally, any devices not owned by Limpopo department of education but containing the department's data are Subject to this policy.
3.4. Ownership and Responsibilities	Information Security is the responsibility of all Limpopo departments of education staff. Specific responsibilities include: • Limpopo department of education staff members must comply with the provisions of this policy and applicable other requirements and standards, such as the internet and e-mail usage Policies for Users of Information. • The Information Communication Technology Sub Branch (ICT Sub Branch - GITO) exists to ensure that risks associated with Information Technology Security are managed in an appropriate and cost effective manner. • The ICT Sub Branch (GITO) is also responsible for establishing and managing an Information Security

	governance function as well as ensuring through corporate Governance structures, enforcing adherence to Information Technology Security principles. • The Government Information Technology Officer (GITO) in collaboration with the National Intelligence Agency (NIA) is also responsible for maintenance of the Information Security Policy Statement and supporting policies, procedures, standards and guidelines.
3.5. Disciplinary Actions	Limpopo department of education adopts a zero tolerance stance and therefore failure to comply with this policy or any of the supporting and complimenting policies, standards and / or processes will be Viewed as negligence and could result in a security violation. Appropriate disciplinary action may be taken thereafter.

4. Policy statement

Limpopo department of education information and information system resources are business critical assets requiring a high level of protection. Sufficient measures, commensurate with the risk, shall be taken to protect these assets against accidental or unauthorized modifications, disclosure and/or destruction, as well as to ensure the confidentiality, integrity and availability Limpopo department of education's information resources. All measures taken by the department shall be in line with the regulatory framework applicable to Limpopo department of education.

In order to fulfill the Information Technology Security Policy Statement, the policies for the following user groups must be complied with:

1. Information Security Policies for Information Technology Operations; and

2. Information Security Policies for Users of Information.

It is the responsibility of all staff to understand the detailed policies listed below. Should anything contained within the

Policies be unclear the ICT Sub Branch will assist all members of staff in obtaining clarity around the

Requirements contained in the policy. If any concerns or conflict arises, they are to be addressed with the ICT Sub Branch without any delay.

The table below outlines the Information Technology Security policy sections (for users of IT) and the objective of each policy.

Information Security Policies	Objective
4.1. Access Control of Information Systems	To ensure that adequate access measures are in place to protect information and IT Resources from loss, unauthorized use/ viewing and denial of service.
4.2. End User Application Development	To ensure that information risks are identified and security controls are addressed and Documented as a standard component of product development. In addition, to ensure Changes are performed in a secure manner.
4.3. Security Organization and Classification	To manage Information Security within the organization and to maintain appropriate Protection of organizational assets.
4.4. Infrastructure and Protection	To ensure that the users preserve the integrity, availability and confidentiality of the Information Technology infrastructure.
4.5. Security Incident Management	To minimize the damage from security incidents and malfunctions by auctioning and Resolving reported issues and to monitor and learn from such incidents.
4.6. Internet and e-mail security	To ensure the confidentiality and integrity of electronic mail (e-mail) messages is protected at all times, the risk of e-mail misuse is minimized 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 minimize the threat posed by the Internet to Limpopo department of education's network infrastructure.
4.7. Information Classification	To ensure the protection of sensitive Limpopo department of education's 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 accordingly.
4.8. Information Security Wireless	To ensure the protection of sensitive Limpopo department of education's data, information, knowledge and Intellectual capital against improper disclosure.
4.9. Removable Media	To ensure the protection of sensitive Limpopo

	department of education 's data, information, knowledge and Intellectual capital when using removable media. This is intended to be achieved by establishing the requirements for maintaining effective information security over Removable media devices.
4.10. Acceptable Usage of IT equipments	To ensure user's accept responsibility for their desktops, laptops & other IT equipments work environment and understand that disciplinary action could occur if they do not adhere to information Security policies & procedures.
4.11. Mobile Computing	To ensure mobile computing devices, including but not limited to laptops, notebooks, PDAs and mobile phones that contain department's information is not compromised.

5. Information Technology Security Control Measures

5.1. Access Control of Information Systems – Users of Information Technology	
Purpose	To ensure that only authorized users gain access to Limpopo department of education information, applications and computer installations.
Scope	This policy applies to Limpopo department of education networks and systems.
Target audience	This policy applies to all Limpopo department of education staff members including third Parties, temporary staff, contractors, service providers, and consultants.
Summary of policy	This policy aims to restrict access to information or systems within Limpopo department of education's computer environment to authorized users as well as to prevent unauthorized use or viewing of information and IT resources. This policy focuses on password & user ID requirements, access to Limpopo department of education's computer systems and networks, and segregation of duties related to IT to ensure that IT users are Aware of their responsibility towards usage of information systems in order to minimize Possible information security risks. In addition, it covers remote, administrator and third party access.
Details of the policy	Details
	Password and Username Management 1. Users may only access the Limpopo department of education's computer systems, e-mail and Internet

	Facilities by means of their personal authorized usernames and passwords. Apart from the information security personnel authorized by management to access computer systems in the performance of their duties and responsibilities. 2. Passwords are never to be shared or revealed to anyone else, and should never be known by anyone other than the authorized user. Disclosure of passwords is Considered to be a dismissible offence. 3. Passwords should never be written down or stored on a computer in an unprotected form. 4. Users are responsible for all activities performed with their personal User IDs. Users must not use any other User ID or password other than the User ID assigned to them and password selected by the user. 5. In order to prevent the unauthorized access of the Limpopo department of education's computer system, passwords for logging on to the windows domain shall comply with the following standards: _ passwords are required to contain a minimum of 8 alphanumeric characters _ passwords must be changed every 30 days _ passwords must not be stored in a manner or format that is accessible to other users _ passwords may not contain the username, full name of the employee or other information that relates to the individual (such as car registration etc) _ passwords must contain elements from three of the four following types of characters: 1. English uppercase letters A,B,C,...Z 2. English lowercase letters a,b,c,...z 3. Numeric characters 0,1,2,...9 4. Special characters $,!,%,^.... 6. If a password is forgotten, the user must submit a request to the IT help desk that a new password be issued. Users must provide proof of identity when they require a Password reset from the IT help desk. 7. Users are required to log out of all systems, including the network, after hours.

	8. When a user is not making use of their computer, the user must lock the computer by using the password protected screen saver, locking the desktop or logging out of the Computer. 9. Users are required to report any misuse or unlawful use of User ID's and passwords to the IT Help Desk, who will record it as a security incident and escalate it to the ICT Sub Branch through the incident management process. 10. User passwords must be changed immediately if compromise is suspected. 11. Unsuccessful login attempts should be logged and investigations should occur where Unsuccessful login attempts are out of the normal range.
	Access Rights and Privilege Control 1. All employees and third parties such as contractors, consultants, business partners and outsourced staff must sign a confidentiality agreement as part of their initial Terms and conditions of employment. The signing of the agreement should take place prior to the employee gaining access to Limpopo department of education's systems and information. 2. Access to Limpopo department of education's computer systems and network from Government premises shall only be attempted by way of computer equipment made available by the department to users. Use of other computer equipment to access Government's network (e.g. Personal Digital Assistants (PDA's), mobile computer media, etc.) must Be specifically authorized by the GITO. If such use is authorized, Government information held on staff owned devices remains the property of Government and Therefore subject to the all applicable user policies. 3. Users are to access only files and data that are their own, are publicly available, or to Which authorized access has been granted. Under Government rules and regulations, the illegal access of confidential information shall be considered a Dismissible offence. 4. Upon termination of employment, individuals may not retain, give away, or remove from company premises any information, other than personal copies of

	information already disseminated to the public and correspondence related to the terms and Conditions of their employment. All other company information must be given to the Individual's supervisor at the time of departure. 5. Upon termination or expiration of their contract, all consultants, temporary employees and contractors must return all company property as well as company information Received or created during the contract.
	Remote Access and Connections (RAS) 1. Remote access shall be granted to users at the sole discretion of department and on the terms and conditions that the GITO may determine from time to time. 2. Remote access to department's computer systems from outside the premises shall only be attempted by way of remote facilities provided by Government utilizing the remote access procedure. 3. When establishing any alternate connection to any external network, users must ensure that their computers are disconnected from all Government networks. Such connections include but are not limited to 3G, GPRS, ADSL, Modems, Wireless, etc. 4. No RAS connections may be established from within the Government network. 5. Software on remote systems must be compliant with all Government standards Relating to operating system, anti-virus software and restricted applications. 6. Limpopo department of education employees or other personnel are prohibited from establishing simultaneous connections to both external networks and Government's networks. 7. All equipment (whether Government owned, personal or third party owned) that is used to connect to Government's networks shall meet the Government requirements for remote access (hardware and software). 8. All remote access usage will be logged with regard to the user, date and time, duration and all events. 9. All remote access logs will be monitored on a regular basis for failed access Attempts, user lockouts and unusual remote access times.

5.2. End User Application Development – Users of Information Technology

Purpose	To ensure that risks are identified and security controls are addressed and documented as a standard component of end user application development. In addition, to ensure that changes to applications are performed in a secure manner.
Scope	This policy applies to all IT applications within the Limpopo department of education
Target audience	This policy applies to all the Limpopo department of education employees, including third parties, temporary staff, contractors, service providers, and consultants.
Summary of policy	This policy aims to ensure that Limpopo department of education users are aware of application development requirements should they be involved in developing end user applications or changes within Limpopo department of education.
Details of the policy	Details
	User Development of Software 1. End users are discouraged from using programming languages such as C#, Visual Basic, Java etc only the application/software development sub directorates are authorized to utilize programming languages. 2. End users must not develop business critical applications. End users may develop only applications for personal or entity use, developed in e.g. Excel and Access. Formal request for IT application needed to support the business must be send to ICT Sub Branch General Manager:ICT(GITO)'s office 3. No End users is allowed to develop or purchase COTS(commercially Off The Shelve Software) without General Manager: ICT(GITO)'s approval 4. Users involved in system development or making changes to existing systems need to ensure that they follow Government's "System Development and Change Control IT" policy to help ensure that appropriate information security controls are considered and they have General Manager: ICT(GITO)'s approval 5. Users involved in system development or making changes to existing systems must at all times ensure that no third party rights are infringed upon. 6. When developing an application, software developer(s)/system analysts must ensure that: • The application is adequately tested before it is used (Line Management is responsible for ensuring that appropriate testing place); and • The application is adequately documented in: • technical program documentation;

	• that the application does not infringe the rights of third parties or opens Government to any criminal or civil liability; • end user documentation; and • Each system should have a formally appointed system owner.

5.3. Security Organization and Classification – Users of Information Technology

Purpose	To manage information security within the organization and to maintain appropriate protection of organizational assets.
Scope	This policy applies to all users, IT Staff and Third Parties who have access to department's Information and/ or are utilizing critical applications and computer installations.
Target audience	This policy applies to all the Limpopo department of education employees, including third parties, temporary staff, contractors, service providers, and consultants.
Summary of policy	The policy aims to ensure that all intellectual property rights, privacy rights and confidentiality rights are adequately protected within Government by all Government IT users, Third Parties, Contractors and Temporary Staff.
Details of the policy	Details
	Intellectual Property Rights 1. Any computer software developed by department's personnel through the use of Government or non-Government computer resources but within the scope of employment with Government whether within or outside normal working hours, remains the 'intellectual property' of Government and may therefore not be copied, sold, leased or removed without the express written consent of Government. 2. Government information, computer software and other information assets are to be used for authorized business purposes. Incidental personal use is permissible so long as it does not interfere with productivity and does not pre-empt any business activity. 3. All software on department's computers is protected by copyright laws. Commercial software purchased by Government is authorized for Government use only and must be utilized in accordance with contractual agreements and copyright laws. Unless specifically authorized within the license agreement, making copies of copyrighted software and related documentation for personal use is illegal and therefore Prohibited. Unauthorized software will be removed and the responsible person will be subject to disciplinary action. 4. Software vendor's license agreements and copyright holder's notices must be strictly adhered to. Whenever bundled systems are being procured, the source is required to provide written evidence of the software licenses. The agreements for all computer programs licensed from third parties should be periodically reviewed for compliance And additional licensed copies procured as required.

	5. Software used by Government employees must only be installed by the ICT Sub Branch. A valid license must be in place before any Software is installed. 6. Software that may further Government's business endeavors may only be installed by the ICT Sub Branch once Line Management approval is obtained. 7. Department's personnel must allow the completion of any network licensing scan check run which is activated upon their booting of workstation machines. 8. Users are prohibited from granting access to Government software for distribution to Independent contractors, clients or any third party.
	Data Privacy and Protection 1. Personal information of clients/staff can only be collected, processed, stored, and disseminated using Government information assets in order to meet a valid Government business need and after the individual's consent has either explicitly or tacitly been obtained 2. Department's users provide their consent to allow personnel, designated by the IT Function, to access, monitor or process any information that the user has created, stored, sent or received on Government information systems. Users shall be made aware that Government may, from time to time use human or automated means to monitor the use of its computer resources and Government computer facilities. 3. Should it be suspected that any user has transgressed any principle contained in the information security policies, Government reserves the right to access all documents and/or files on any computer to establish whether a policy has been transgressed. 4. Government makes all reasonable efforts to respect the privacy of information stored on Government information assets. However, the task of system administration and operation may occasionally lead to the unavoidable possibility of production support Personnel having access to such information. 5. With regard to data privacy and protection, the following laws are to be taken into account: _ Promotion of Access to Information Act (PAIA) Business secrecy laws prohibit any form of disclosure to, or use of certain

	business information by a third party (e.g. information concerning business activities, strategic planning, etc.). _ Regulation of Interception of Communication and Provision of Communication Related Information Act (RICA) Business monitoring and interception of communication can only occur in Accordance with the requirements defined in the act. _ Protection of Personal Information Bill (POPIA)/Data Protection Principles Data protection principles prohibit the disclosure, storage or use of personal data of an individual without the prior consent of that individual (e.g. name and Address, profession, financial statements, personal profiles, etc.).

5.4. Infrastructure and Protection – Users of Information Technology

Purpose	To ensure that the users preserve the integrity, availability and confidentiality of the Information Technology infrastructure.
Scope	This policy applies to all information, critical applications, computer installations, networks and systems under development.
Target audience	This policy applies to all the Limpopo department of education employees, including third parties, temporary staff, contractors, service providers, and consultants.
Summary of policy	The policy aims to ensure that users are aware of their responsibility towards virus management and modem use in order to protect the infrastructure. Additionally the policy outlines what information security monitoring regulations for users and lastly requirements for Removable computer media, for example Cellphones, removable storage, Personal Digital Assistants (PDA's).
Details of the policy	Details
	Hardware 1. Responsibility for an asset starts on physical receipt of that asset by the user. 2. All users (employees, contractors and incidental users) are strictly prohibited from making any hardware changes to any PC. If there is a business reason for making a hardware change, the user change request is to be submitted to the IT Help Desk. The ICT Sub branch will be notified and an engineer/ technician assigned to make the necessary, authorized changes. 3. Non-standard hardware configurations and security configurations for access to hardware must be approved by the ICT Sub branch 4. Internal or external items such as speakers, DVD drives, re-writable

	CD-ROM drives, Sound cards, graphics cards etc., which are non-standard Government computer equipment, will not be provided unless specifically requested and approved by executives. 5. Other computer equipment such as PDA's (Personal Digital Assistant), scanners and any other computer equipment is also non-standard Government computer equipment and will not be provided unless specifically requested and approved by executives.
	Virus Management 1 No employee may knowingly distribute viruses or bypass any detection systems in place. 2 Users are not allowed to open any e-mail if the source of the e-mail is unknown to the user. 3 Individuals receiving data media, from any source within or outside Government, have the responsibility for ensuring that it is checked for viruses before use. Similarly, individuals intending to pass on data media within Government or to external third parties must ensure that it is first checked for viruses.

5.5. Internet and E-mail Security – Users of Information Technology

Purpose	To ensure the confidentiality and integrity of electronic mail (e-mail) messages is protected in transit, the risk of e-mail misuse is minimized 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 minimize the threat posed by the Internet to Government's networks.
Scope	This policy applies to all users, IT Staff and Third Parties who make use of department's electronic mail system, Internet and Intranet.
Target audience	This policy applies to all the Limpopo department of education employees, including third parties, temporary staff, contractors, service providers, and consultants.
Summary of policy	This policy aims to set out the guidelines, which need to be followed when making use of Internet and e-mail services. This policy focuses on usage of Internet, Intranet and e-mail.
Details of the policy	Details
	Prohibitions 1. The use of a computer, e-mail or the Internet to receive, send, download or otherwise disseminate prohibited material is strictly prohibited. 2. Staff must be aware that they are prohibited from accessing or transmitting sexual, racist or religious information / images, which may be offensive; making obscene, discriminatory or harassing statements; which may be illegal or downloading illegal Material while using the Government e-mail system,

	Internet or Intranet, as this constitutes prohibited material. If circumstances arise whereby the transmission of such material is required, documented authorization from Line Management is required prior to such publication or transmission.
	Internet Usage 1. Access to the Internet is granted to employees based on their employment requirements, which is a privilege and is not to be abused. Users should be aware That tracking to sites visited occurs. All users give their consent that such tracking occurs. Access is furthermore denied to various offensive sites. 2. Only Government approved versions of Internet browsers are to be used with necessary cumulative updates or the applicable version at the time. Users are prohibited from changing any configuration properties of their web browsers. 3. Only authorized IT administrators are allowed to change web browser configurations. 4. Users may not browse the Internet for non-business purposes during working hours. Department heads may authorize and manage non-business use where it makes business sense, for example paying personal accounts via online banking, rather than taking time off from work in order to physically visit a bank or department store for the same reason. 5. While accessing the Internet resources from Government systems, users may not deliberately visit, view, download, print or disseminate any prohibited material from any web site. Users may also not attempt to probe other systems for security weaknesses, compromise other systems, possess or transfer data illegally or send offensive or abusive messages. 6. Posting any message on the Internet showing affiliation with Government is forbidden without permission from the HR Department 7. The downloading of software onto the company's system without the prior written consent of line management is prohibited. Software pertaining to direct business use, will be downloaded, scanned and installed with managerial approval. Downloaded software may only be used under the terms of its license agreement. The following conditions must be when downloading software: • All data are checked for viruses using an approved methodology and tools • before they are installed on Government's network; • All data are business-relevant, appropriate, are acquired and

	used in compliance with all Government's and legal requirements; • All programs or executable applications are approved by the relevant Line Manager and the Department ICT sub branch Office.
	E-mail Usage 1. The Department's e-mail system must be used primarily for legitimate business purposes in the course of assigned duties. Incidental and occasional limited personal use of Government's e-mail system is permitted, providing at all times that such use does not: • Interfere with the user's work or performance; • Interfere with any other user's work or performance; • Cause disruptions to the operations or resources of Government information • system resources; and • Violate any other provision of this policy or any other applicable policy of • Government. 2. The Department regards e-mail as private communication between sender and recipient(s) and must make a reasonable effort to respect and protect this privacy. If the Department's information system resources are used to create, send, receive or store private personal data, then in order to protect the privacy of any such data, the user shall designate such data as "Private". However, the Users' right to privacy in their personal communications is restricted by the need for the Department to pursue their legitimate business purposes. The Department reserves the right to access or delete the contents of a user's mailbox when it is in the best interests of the Department. 3. Users must show good judgment when utilizing e-mail and follow all relevant policies concerning the transmission of sensitive messages. 4. Any non-business related attachments (e.g. movies, images, etc.) are not permitted and will be removed and quarantined. Business or certain personal message attachments may be released on the request of the user.

	5. The use of automatic e-mail diversion to external e-mail addresses, unauthorized advertising and opening of attachments from unknown or non-trusted sources is prohibited. 6. Under no circumstances are any executable attachments (e.g. those with *.exe file Extensions) to be opened. 7. Sending of forged e-mail messages are expressly forbidden. Individuals are not to use an e-mail account that has been assigned to another user. All messages must clearly Identify the true author. 8. Unless the information owner/originator agrees in advance, or the information is clearly public in nature, users must not forward e-mail to any address outside Government's network. Blanket forwarding of e-mail messages to any outside address is prohibited. 9. To protect Government from such threats such as mail bombs, automatic forwarding of e-mail from external addresses to Government's e-mail systems is prohibited. 10. The Government's e-mail system may not be used for unauthorized or illegitimate purposes. Employees may not use e-mail to infringe the copyright or other intellectual property rights of Government or third parties, to distribute defamatory, fraudulent, harassing messages or otherwise to engage in any unauthorized or wrongful conduct. Use of both e-mail and Internet in this regard is expressly forbidden. This includes, but is not limited to: _ spam _ derogatory comments about a certain sex, race, religion, or sexual preference _ private or freelance business _ transmitting of pornographic, obscene or sexually exploitative material; offensive, obscene and abusive messages and images; and material that is defamatory, harassing or bullying in nature _ any act of discrimination contrary to the policy of equal opportunities or offensive to the dignity of people at work _ conducting political activities _ any breach of the company's information security policy, including the sharing of passwords _ threats _ defamatory remarks about products, services or other companies _ deliberate disclosure of confidential company information to unauthorized

	persons. 11. Government's e-mail systems provide limited message security. As a consequence, users should show good judgment and follow all relevant policies concerning the transmission of sensitive messages. 12. Business related e-mails should only be sent from Government's e-mail system and not sent from a private e-mail account. 13. E-mail messages and attachments sent outside of Government, should not contain information that may be damaging to Government or the recipient if intercepted by another party. 14. Sending bulk e-mail of a personal nature over Government's e-mail system is not allowed. 15. Chain letters should not be forwarded, created or circulated by the use of Government e-mail accounts. 16. E-mails can be used as evidence in legal proceedings and can create binding contracts. Keep a file copy of significant messages sent and received by e-mail. Users may not enter into any contractual agreement for or on behalf of Government using Government e-mail facilities. 17. E-mail users are personally responsible for taking all reasonable steps to prevent unauthorized use of their e-mail facility and consequently be held accountable for all activities under their login. 18. E-mail is to be checked on each working day and the standard email application (e.g. MS Outlook) is to be kept open so that incoming mail is immediately received. Emails requiring a reply should be addressed within one business day. 19. Confirmation of receipt is to be obtained for all important e-mails sent. 20. If staff will not be contactable on their e-mail for a period greater than two days, the out of office assistant must be used to indicate the length of absence and alternative contact details. 21. Employees must make use of the standard Government signature in all messages sent to anyone outside of Government. No background or images are to be used. 22. Limit the recipients to whom e-mails are copied (cc'd). Also ensure that any person receiving a particular e-mail needs to receive it. 23. E-mail communication is susceptible to misinterpretation. E-mails should be carefully considered to ensure that professionalism is maintained no

	misinterpretation occurs.

Approved/ not approved

ACCOUNTING OFFICER

DATE 7/4/2015