LIMPOPO

PROVINCIAL GOVERNMENT

REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF

TRANSPORT AND COMMUNITY SAFETY

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT)

VERSION 1

TABLE OF CONTENTS

PAGES

Table of Contents

1. Acronyms and Abbreviations..... 4
2. Executive summary..... 5
3. Introduction 6
4. Purpose and Objectives of the policy..... 5
5. Authority of policy 7
6. Legal framework 7
7. Scope of application 9
8. Definitions 10
9. Policy pronouncement 11

9.1.Acceptable Use 9

9.1.1. General use and wnership.....9

9.1.2. Security and proprietary nformation.....12

9.1.3. Personnel Security 10

9.1.4. Internet 10

9.1.5. Electronic mail....12
9.1.6. Accessing remote e-mail and internet....14
9.2. Unacceptable use 13
9.3. Classification scheme....15
9.3.1. Classification of data and systems 16
9.3.2. Classification and responsibilities. 16
9.4. Information system security....17
9.4.1. Network security 17
9.4.2. Servers 17
9.4.3. Workstations 17
9.4.4. Portable computers 18
9.4.5. Storage removal and disposal 19
9.4.6. Configuration management 19
9.5. Allocation of Equipment 20
9.5.1. Laptop or Notebook Computer 20
9.5.2. Desktop Computers 21
9.5.3. Printers, Memory Sticks and Peripherals 21
9.5.4. Data Projectors 21
9.5.5. Wireless Data Cards and Tablets 22
9.5.5.1. Procedures....23
9.5.6. Usage of the wireless data card....23
9.5.7. Abuse of the wireless data card....24
9.6. Custodianship of Equipment Usage and Security 24
9.7. Replacement of Equipment 26
9.8. Requisition of Equipment 26
9.9. Transfer of Equipment 26
9.10. Condition of use of ICT Equipment....27
9.11. Call logging Procedure....27
10. Default/Non-Compliance 27

11. Inception Date 26

12. Termination and Review conditions 26

13. Enquiries 27

14. Appendix A 27

1. ACRONYMS AND ABBREVIATIONS

DTCS	Department of Transport and Community Safety
GITO	Government Information and Technology Office
THE DEPARTMENT	Limpopo Department of Transport and Community Safety
NETWORK DEVICES	computers and devices interconnected by communications channels that facilitate communications among users.
MBSA	Microsoft Baseline Security Analyzer.
IT	Information Technology.
ICT	Information Communication Technology.
E-mail	Electronic Mail
WSUS	Windows Server Updates Services
ICTS	Information and Communication Technology Security
PST	Personal Storage Table
SCM	Supply Chain Management

2. EXECUTIVE SUMMARY

Information and Communication Technologies (ICTs) are now widely accepted by developing countries as a critical tool in their efforts to eradicate poverty, enhance human development, and achieve development goals. The impact that ICTs had on our daily lives has influenced daily routines and the way business is conducted. Governments and private businesses have invested in the usage of ICTs for their day to day operations.

While the use of Information Technology is crucial to boost overall productivity and improving service delivery to the public, DTCS can/may incur unnecessary costs and be subject to legal liabilities arising from misuse of IT Infrastructure. The aim of this policy is to ensure that the Department influences the investment in its IT infrastructure.

To ensure that critical business activities take place and prevent loss, damage or compromise of critical assets or data, IT Infrastructure should be protected from various security threats and environmental hazards. This policy has been developed to prevent loss of assets and crucial data which may results in an IT risk in the department.

3. Introduction

The Department of Transport and Community Safety encourages the use of electronic communications to share information and knowledge in support of the department's mission and to conduct the department's business. To this end, the department supports and provides interactive electronic communication services and facilities such as telephones, electronic mail, electronic publishing services such as the Internet. This policy recognizes this convergence and establishes an overall policy framework for electronic communications.

This policy establishes new procedures where existing policies or legislation do not specifically address issues particular to the use of electronic communications.

This policy must be read together with the departmental ICT Security Policy Version 1.0.

4. Purpose and Objectives of the Policy

The purpose of this policy is to enable the DTCS to apply an effective and consistent level of security and management to all information systems that process electronic information of the department.

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

i. The assets of the department are secured against loss by theft, fraud, malicious or accidental damage, or breach of privacy or confidentiality, and
ii. The department is protected from damage or liability resulting from the use of its facilities for purposes contrary to the law of South Africa.
iii. To provide guidelines in the provision and allocation of desktop computers, laptops and peripherals for use by employees as a work facility.
iv. To create awareness on best practices, effective use and conditions of use of internet and e-mail facilities provided by the DTCS.
v. To provide a regulatory framework on the provision and usage of wireless data cards for remote access to e-mail and internet facilities
vi. To establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

5. Authority of Policy

The authority of this policy lies within the Office of the Accounting Officer of the Department of Transport and Community Safety.

6. Legal Frameworks

Any third party who has a contractual relation with the Department and contravenes the provision of the policy will be dealt with in terms of the penalty clause of the agreement entered into by and between him/her and the Department.

Employees who violate this policy will be disciplined in terms of measures contained in or published in one or more of the following acts, regulations and policy prescripts (this list is by no means exhaustive):

i. Minimum Information Security Standards (MISS).
ii. State Information Technology Act (Act no. 88 of 1998) as amended.
iii. SACSA/090/1(4) "Communication Security in the RSA".
iv. Protection of Information Act (Act no. 84 of 1982).
v. Information Act (Act no. 70 of 2002).

vi. Promotion of Access to Information Act (Act no. 2 of 2000).
vii. Electronic Communication and Transactions Act (Act no. 25 of 2002).
viii. Electronic Communications Act (Act no. 37 of 2007) as amended
ix. Intergovernmental Relations Act (Act no. 3 of 2005)
x. National Intelligence Act (Act no. 39 of 1994).
xi. Copyright Act (Act no. 98 of 1978).
xii. National Strategic Intelligence Act (Act no. 39 of 1994).
xiii. National Archives of SA Act (Act no. 43 of 1996).
xiv. Public Service Act (Act no. 103 of 1994).
xv. Public Finance Management Act (Act no. 1 of 1999).
xvi. Basic Conditions of Service Act
xvii. Regulation of Interception of Communications & Provision of Communication Related Information Act
xviii. Labour Relations Act
xix. Information Security Management Practice
xx. SITA Regulations
xxi. Public Service Regulations
xxii. Treasury Regulations
xxiii. Protection of Personal Information Bill/Act
xxiv. Cobit, ITIL
xxv. ISO27001/2/3, ISO38500
xxvi. PRINCE II
xxvii. Disciplinary Codes and Conducts
xxviii. Public Service Act, 1999
xxix. Public Service Regulations 2001 as amended
xxx. Public Finance Management Act, 1999 (Act No.1 of 1999)
xxxi. Treasury Regulations issued in terms of PFMA, 1999
xxxii. State Information Technology Act (Act no 88 of 1998)
xxxiii. Protection of Information Act (Act no 84 of 1982)
xxxiv. Minimum Information Security Standards (MISS), Second Edition March 1998
xxxv. Any other applicable legislature and ICT policies of the Department

7. Scope of Application

This policy applies to all employees, contractors, consultants, visitors and other workers in the DTCS, including all personnel that are affiliated with third parties. This policy applies to all

equipment and electronic systems that is owned or leased by the department. The ICT policy is intended to support, protect, control and manage departmental electronic information resources.

8. Definitions

Accountability

- Ensuring that the actions of an entity/individual may be traced uniquely to that entity/individual, who may then be held responsible for that action.

Authentication

- Establishing the validity of a claimed entity/verification of identity of an individual or application.

Availability

- Being accessible and useable upon demand by an authorized entity.

Confidentiality

- The principle that information is not made available or disclosed to unauthorized individuals, entities or processes.

Information Technology

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

Audit

-Actions that are taken to detect and investigate events that might represent a threat to security. To conduct the independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedure, and to recommend any indicated changes in controls, policy or procedures.

Domain

-Refers to those aspects of an information system that are relevant only to its ability to support its authorised users in achieving a uniform business objective. All its components are protected according to controls that are specified in a single security plan, and the domain is managed on a day-to-day basis by a single management authority (system manager).

Department

-Limpopo Department of Community Safety.

Non-SITA third party

-Any organisation/institution/department other than SITA, a national department, provincial administration or organisational component listed in schedules 1 and 2 of the Public Service Act, 1994.

9. Policy Pronouncement

Employees are expected to abide by DTCS ICT policy in a responsible manner that does not in any way hamper productivity, disrupt official activities, cause harm to another information system or the confidentiality, availability and integrity thereof.

9.1. Acceptable use

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

9.1.1. General use and ownership

i. While the DTCS desires to provide a reasonable level of privacy, users must be aware that the data they create on the corporate systems remains the property of the department. All employees are responsible for exercising good judgment regarding the reasonableness of personal use towards ICT resources; this includes personal use of Internet, E-mail, and processing and computer equipments.

ii. Without specific written exceptions, all programs and documentation that are generated or provided by employees, consultants or contractors, for the benefit of the DTCS, remain the property of the DTCS.

iii. The DTCS 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 DTCS reserves the right to access this information without prior notice whenever a genuine business need exists.

iv. All equipments connected to the network of the DTCS should run up-to-date approved licensed anti-virus scanning software and authorised licensed software.

v. The DTCS reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy. The department reserves the right to remove any unlicensed software found in any IT equipment connected to DTCS network.

vi. However Server Administrator/s are the ones with full administrative rights while IT officials will have limited administrative rights, and finance officials using Basic Accounting System (BAS) and other officials requiring local rights will be given local administrative rights.

9.1.2. Security and proprietary information

i. Employees shall take all necessary steps to prevent unauthorised access to classified information.
ii. Provisioning of information, lists of DTCS employees to parties outside the department is prohibited, unless authorised by Accounting Officer.

9.1.3. Personnel security

i. The employees of the DTCS who accesses 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.
ii. Access to the systems and data shall be immediately terminated as soon as evidence of non-compliance with the security requirements is gathered.
iii. All employees shall sign a secrecy declaration and non-disclosure form not to disclose or reveal any sensitive information that they are privileged to access as a result of their job assignment to any unauthorised personnel through Security Management.
iv. Employees disclosing electronic information to the media, press or anyone shall do so with permission granted by the Accounting Officer.

9.1.4. Internet

Connection to the Internet introduces new opportunities for new risks. In response to the risks, this policy describes the policy of the DTCS regarding Internet security. This section should be read and applied in conjunction with the ICT Security Policy version 1.0. of the DTCS. The following are expectations of internet usage:

i. Access to the Internet shall be granted to all employees as one of ICT services with expectations of promoting access to information.
ii. To protect the DTCS from profane material and to allow economic use of bandwidth, all Internet usage shall be monitored by Websense software. In an event of over utilization of bandwidth certain sites may be blacklisted.
iii. Websense software shall prevent users from accessing all web sites that contain sexually explicit, online gambling, profane and other potentially offensive and harmful material shall be blocked out via web content filtering tool. When official require to access blocked or blacklisted site, the relevant director shall provide a written motivation and GITO to assess the risk(s) before unblocking the site.

It is the responsibility of the user to ensure that the above sites mentioned in roman figure iii are not accessed, in a situation that the Websense Software

iv. was unable to block any of the above sites the user will be held responsible if found accessing such sites.

v. Misrepresenting, obscuring, suppressing or replacing the identity of a user on the Internet or any DTCS communication systems is forbidden.

vi. Users shall not publicly disclose internal DTCS information via the Internet, which could adversely affect the department, customer relations or public image.

vii. At any time and without prior notice, DTCS management reserves the right to examine Web browser cache files, Web browser bookmarks and other information that is stored on or passing through the computers of the DTCS. Such management access assures compliance with internal policies, assists with internal investigations and assists with the management of internet services.

viii. The following terms and conditions of internet usage using DCS resources shall apply to all employees:

a) Access and use of the internet must be in direct support of the official business of the department and for information gathering. The internet is a work facility and must be respected and treated as such.

b) Retrieval and downloading of material should be restricted to information that is valuable to a specific task or project to be done. Games, pornographic material, music, movies, racially inciting material, material that is disparaging to ethnic groups or religious beliefs, etc. shall not be downloaded from the internet.

c) No employee in his or her official capacity may enter into any procurement transactions on the internet on behalf of the department, without written authorisation from the Head of the Department.

d) As soon as an employee finishes his or her task on the internet, he or she should close the session immediately to allow bandwidth to become available for other users and applications to operate at maximum speed.

e) When the user uses the Wi-Fi connection is their responsibility to ensure section 10.1.4 (iii and iv) are complied with.

9.1.5. Electronic mail

i. As a productivity enhancement tool, DTCS encourages the business use of electronic communications. Electronic communication systems, and all messages that are generated on or handled by electronic communications systems, including backup copies, are considered to be the property of DTCS.

ii. E-mail enquiries shall be answered except in instances which would constitute a breach of security or confidentiality of classified data and information.

iii. DTCS electronic communication systems generally shall be used mainly for business activities.

iv. Misrepresenting, obscuring, suppressing or replacing the identity of a user on an electronic communications system is forbidden. The user name, electronic mail address, organisational affiliation and related information that are included with electronic messages or postings must reflect the actual originator of the messages or postings.

v. DTCS management shall when required monitor the content of electronic communications. Content and usage of electronic communications may be monitored to support operational, maintenance, auditing, security and investigative activities.

vi. Recognising that some information is intended for specific individuals and shall not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. DTCS sensitive information shall not be forwarded to any party outside DTCS without the prior approval of the Director responsible for Records Management or Information Officer.

vii. Users shall be allocated fixed size electronic mail space on the server. Users must manage their emails and periodically store emails with attachments to their external storage and/or request IT official to achieve old e-mails through the PST.

viii. Messages that are no longer needed for business purposes should be periodically cleaned by users from their personal e-mail boxes.

ix. Users must abide by the guidelines for electronic mail etiquette as in Annexure A.

x. All Email messages sent from DTCS mail servers may have the Disclaimer Notice:

"Privileged/Confidential information may be contained in this message. If you are not the addressee indicated in this message (or responsible for the delivery of the message to such a

person), you may not copy or deliver this message to anyone. In such case, you should destroy this message and kindly notify the sender by reply e-mail. Please advise immediately if you or your employer do not consent to e-mail messages of this kind. Opinions, conclusions and other information in this message that do not relate to the official business of Limpopo Department of Transport and Community Safety shall be understood as neither given nor endorsed by the department."

9.1.6. Accessing remote e-mail and internet

i. Government regulations restrict users from connecting remotely onto the government network due to security reasons.

ii. Officials accessing e-mail remotely using wireless data cards must first establish an internet connection.

iii. Having established this, the official must then use web mail (an internet based e-mail application) to access their e-mail.

iv. The GITO will be responsible to configure web mail accounts and train users on how to access this application.

v. Web mail requires an official's user name and password (present user name and password that is used to gain network access at the office).

vi. It is the responsibility of an official to safeguard his/her username and password. DTCS S Policy is applicable to this policy.

9.2. Unacceptable use

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

i. Accessing, including browsing, downloading or forwarding material that is obscene, offensive and/or of a sexual nature, religious intolerance in any format - whether in word or audio file.

ii. Accessing, including browsing, downloading or forwarding material that is racist, discriminatory, incites hatred or promotes violence.

iii. downloading, copying and sending anything that constitutes an infringement of copyright, including images, music files and video in any format;

iv. contributing to Internet newsgroups or chat rooms on behalf of DTCS without being authorised to do so;

v. signing up to e-mail bulletin boards or news groups that require payments from the DTCS, unless specific written authorisation was obtained for such a business-related cost;

vi. making any personal comment outside the DTCS using office facilities or as a representative of the office, except where authorised to do so as part of the duties of the employee;

vii. making any defamatory or derogatory comments;

viii. creating or forwarding chain e-mail letters, or any advertising material or any non-business-related material, except where authorised to do so as part of employee's duties;

ix. using the Internet/e-mail for personal gain or profit during working hours of the office, or soliciting employees of other departments for any non-departmental business purposes;

x. making fraudulent offers of products, items or services;

xi. Making statements about any warranties or guarantees that are offered by the DTCS, unless it is as a part of the duties of the employee.

xii. Transmitting externally any DTCS confidential information without the appropriate approval from line management.

xiii. On receiving any unacceptable material, a user must delete such material immediately, regardless of content. Failure to delete such material shall mean that the employee accepts and owns the material. The employee is advised to instruct the sender to stop sending such material and, should the sender continue to do so ICT management should be advised as soon as possible so that appropriate action can be taken.

xiv. Any material that contains graphical images and multimedia files use significant office ICT storage and system resources, and should only be stored, scanned or incorporated in electronic messages for legitimate business purposes.

xv. Any activity that is illegal under local, state or international law while utilising ICT resources that are owned by the department.

xvi. Violating any person or company that is protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the

installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the DTCS.

xvii. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are in the scope of regular duties. "Disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, cyber threats and forged routing information for malicious purposes.

xviii. Executing any form of network monitoring that will intercept data that is not intended for the host of the employee, unless this activity is a part of the normal job/duty of the employee.

xix. Revealing any account passwords to others or allowing use of the account of the employee by others. This includes colleagues, family and other household members when work is being done at home or even at the office.

xx. Using the DTCS computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the local jurisdiction of the user.

xxi. News of death or injury, unless authorised by Accounting Officer and the next of kin has been informed.

xxii. Questions or information involving litigation or which might lead to litigation.

xxiii. Information that has not been cleared by the appropriate responsible authority.

xxiv. Junk mail, chain mail or spamming shall neither be generated nor distributed.

xxv. Private marketing or sales for personal gain or for gain of a private company using the departmental e-mail facility.

xxvi. Distribution of hoax messages (e.g. bomb threats, riots, etc) as this may cause panic and lead to disaster.

9.3. Classification scheme

The purpose of this policy is to give detailed guidelines for classification of IT resources and information processed. This policy applies to all information, systems and computer equipment that are owned by the department. It is the responsibility of resource users to ensure that resources are classified accordingly.

9.3.1. Classification of data and systems

Systems and data shall be divided into three sensitivity classifications with separate handling requirements: CONFIDENTIAL, SECRET and TOP SECRET. This standard data sensitivity classification system shall be used throughout the DTCS.

These classifications are defined below as follows:

i. **CONFIDENTIAL** is the classification that is allocated to all information that may be used by malicious/opposing/hostile elements to harm either the objective or functions of the department or an individual.
ii. **SECRET** is the classification that is allocated to all information that may be used by malicious/opposing/hostile elements to disrupt the objective and functions of the department and an individual.
iii. **TOP SECRET** is the classification that is allocated to all information that may be used by malicious/opposing/hostile elements to neutralise the objective and functions of the institution and/or state.

9.3.2. Classification and responsibilities.

It is the responsibility of the user to:

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

9.4. Information system security

This policy is intended to give necessary direction regarding the protection of the availability, integrity and confidentiality of information assets and systems of the DTCS. This section must be read in conjunction with the "Access Control" in the ICT Security Policy version 1.0.

9.4.1. Network security

The office shall provide network security to the ICT infrastructure that includes:

i. Any networks (wired and wireless) to which the DTCS network equipment is connected, which includes the LAN, WAN connections and satellite connections.
ii. All equipment that is connected to the networks.
iii. Network administrators and service providers that manage the equipment.
iv. All users that utilise equipment that is connected to the network.
v. Any service provider that accesses DTCS network to render a service, shall adhere to the security measures in place.

9.4.2. Servers

i. All servers that host data and applications shall be located in a physical secure environment, in which access is strictly controlled. A server room access register shall be kept. Biometric shall be utilized to gain access.
ii. Logical access to servers shall be allocated on a need to know basis, in accordance with the access control in ICT Security policy version 1.0 of the DTCS.
iii. All servers must be loaded and protected with the latest approved antivirus software. Updates shall be implemented on a regular basis for patches, signature and upgrades.
iv. Changes or updates to software or application systems shall also be recorded in a software update register.
v. All critical servers shall be replicated to the Departmental Disaster Recovery Site.

9.4.3. Workstations

i. All workstations shall be located in a physically secured environment, in which the user is responsible for ensuring the office is locked when unattended.
ii. All workstations should be loaded and protected by the latest approved antivirus software.

iii. It is the responsibility of the workstation user to ensure that appropriate security measures and practices are adhered to. Protection of the data that is stored on workstations is the responsibility of the workstation user.

iv. Users shall not leave their workstations unattended while accessing or processing information without appropriate protection like password-protected screen savers.

v. Workstations that are used to access sensitive information like finance or human resource data that is classified to be highly sensitive, users shall lock their workstations when moving away from the workstation.

vi. Users shall not share workstation passwords and user accounts with anyone including fellow colleagues.

vii. It is the responsibility of the workstation user to ensure that his/her workstation is adequately protected from logical threats as well as physical environmental threats.

viii. All users shall log off from their workstations at the end of each business day or for extended periods of absence from their workstations.

ix. As a security alert and computer access control, all users are supposed to access their own computers unless otherwise a request is forward to GITO for approval to avoid mismanagement of computers and information security.

9.4.4. Portable computers

i. All portable computers (e.g. laptops, palmtops, tablets etc.) that are allocated to users must be secured by relevant users.

ii. Users need to ensure that their portable computers are loaded with the latest antivirus software by connecting to the network and updating its platforms.

iii. Users also need to ensure that all data is stored on Desktop and/or My Documents to be backed up on the network.

iv. Any third party laptops connecting to the network must obtain approval from GITO office before down loading any DTCS information.

v. All laptop users must ensure that they receive a lockup cable form IT office and further ensure they lock their laptops using the allocated cable.

9.4.5. Storage removal and disposal

If a hard disk/storage medium or any equipment containing departmental information needs to be removed from the DTCS premises, in the form of auction, donation and/or repairs it shall be formatted before being sent out, and the files of equipments to be returned shall have to be saved and kept in a safe place before the equipment is released from the department.

9.4.6. Configuration management

In order to prevent fraud, sabotage, espionage, subversion and actions that endanger security, effective configuration management policies shall be applied to systems that are in operation. Configuration items of DTCS system shall 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.

i. Configuration management policy must ensure that any additions, omissions or changes that are made to the system are authorised and do not compromise the set security measures.

ii. Computer hardware and software shall be implemented in accordance with an implementation plan. The implementation plan shall address the activities that are related to the coordination and implementation of the security measures, and shall specify acceptance criteria to be met before the system is put into operation.

9.5. Allocation of Equipment

9.5.1. Laptop or Notebook Computer

i. Laptops shall be provided to the MEC, HOD, members of the Senior Management Service, Deputy Directors and District Officials working offsite as a standard work tool/facility.

ii. Employees who carry out secretarial duties for high level management committees such as the Top/Executive Management meetings.

iii. Employees that do not fall into the category as stated in the above-mentioned point 10.4.1(i) and 10.4.1(ii) may be issued with laptops. Laptops may only be issued to such employees provided that the responsible Chief Director or Chief Financial Officer of such employee's submit written motivations for the required laptop.

iv. The motivation must be submitted to the GITO, who will then consider the request. Approval can only be granted by the GITO/HOD and no deviations will be allowed unless such a function has been delegated by the GITO.

v. GITO shall be responsible for providing pool laptop when officials without laptops are supposed to attend workshops or related activities requiring laptop. Request must be done in writing accompanied by invitation of such workshop.

vi. GITO has a right to re-allocate working laptops that reached their life span or provide a newly procured laptops to lower managerial level such as Assistant Directors. However point 10.5.1(i) still apply if the allocated laptop can malfunction the official can be allocated with a Computer.

vii. No employee is to have a desktop computer and a laptop, except the MEC, HOD and any other persons that has approval from the HOD, to have both laptop and a desktop computer.

9.5.2. Desktop Computers

i. Desktop computers are provided to employees (including in-service students/interns) who are office bound by the very nature of their jobs, permanently employed, contracted and authorized third parties by the department in relevant posts of administrative, financial and office management duties as a standard work tool.

ii. Cleaners, labourers and general workers may also be issued with desktop computers or out of date laptops, which will be for shared use amongst themselves. These posts do not require such employees to work full time on desktop computers, but the facility will empower these employees within ICT to access e-leave, email, internet and general word processing functions which may be required.

iii. Clause 10.5.1(i) will also be applicable to employees that seldom require the sole use of a desktop computer.

9.5.3. Printers, Memory Sticks and Peripherals.

i. Standalone desktop printers will be issued to the MEC, HOD and SMS Members as a standard work tool/work facility.

ii. Standalone printers may be issued to employees working in Finance, Procurement, Human Resource Management and Budget sections.

iii. Employees working with confidential information e.g. Supply Chain, Labour Relations, Job Evaluation, EWP, Security Management etc. may also qualify for a standalone desktop printer provided that their respective Directors submit a motivation for such request. The request must be made in writing to the GITO for consideration.

iv. Employees that do not qualify for a standalone desktop printer will be connected to a network printer on their floor. The ratio of connecting users to a network printer is that users will be connected to 1 or 2 network printers on the same floor. These printers are high end and are meant for network printing tasks. Printing costs are reduced when users share network printers.

v. All printers that are purchased from GITO will be laser technology printers (black), and depending on the job functions and type of printing required, a color laser printer may be purchased.

vi. Every employee that perform administrative duties automatically qualifies for memory stick. Employees shall be allocated with encrypted USBs using windows bitlocker.

9.5.4. Data Projectors

i. GITO shall have a centralised Data projector to be loaned whereby a directorate has a function that need projection.

ii. Every directorate shall be provided with a Data Projector to be used for functions within the directorate.

iii. Requests for data projectors should be made with the GITO at least two days before the function.

iv. A data projector register shall be kept in IT office.

v. Employees shall sign the register when collecting and returning.

9.5.5. Wireless Data Cards and Tablets

Wireless data cards shall only be acquired by GITO, and shall be acquired through National Treasury Transversal Contract RT15/2016 or any preceding contract.

9.5.5.1. Procedures

i. Users will fill application forms through their supervisors, and or Directors and Chief Directors, Chief Financial Officer.
ii. All applications are subject to approval strictly by the Accounting Officer or any official duly delegated to do so by the Accounting Officer
iii. After approval has been granted Information Technology will send an official letter to the service provider as application for the device.
iv. Once GITO has received the wireless data card/modem, the requesting official must be notified. The official must acknowledge receipt of delivery of the wireless data card from the issuing officer.
v. The official should then log a call at the GITO Helpdesk to connect and configure the wireless data card/modem.
vi. The GITO is not responsible for logistical functions with regards to acquiring, monitoring and disposal of wireless data cards.
vii. The GITO is only responsible for installation and configuration.

9.5.6. Usage of the wireless data card

i. The primary purpose of a wireless data card is to enable remote access to e-mail and internet facilities. The recommended package allow for sufficient data transfer per month.
ii. Under no circumstances shall officials send Short Message Services (SMS), make video calls, voice calls or subscribe for any other functionality of the wireless data card/modem.
iii. These are billable services from the service provider and the Department will be charged accordingly for these services in addition to the normal subscription fees.
iv. Officials who do not comply with point 10.4.6 (iii) shall be required to reimburse the department. Further to this, the department shall withdraw such officials wireless data cards/modem.
v. Logistics will monitor the monthly usage of each card. If there is indication that officials are under utilizing the facility over a time period, such officials will be required to relinquish their card.

9.5.7. Abuse of the wireless data card

i. Any official not complying with point (5.3) as stated above will be in violation of this policy.

ii. The rules and guidelines as stipulated in the DTCS section XXXX Internet and E-mail usage are applicable to officials issued with wireless data cards (downloading information and sending e-mail).

9.6. Custodianship of Equipment Usage and Security

i. All equipment and information stored in them belongs to the department and not to any employee. When equipment is assigned, it is assigned to an employee in a particular post. The employee occupying that post is the responsible person for that particular equipment that has been assigned to that post until such time the employee resigns, transferred to another post, etc.

ii. Officials should always ensure that the wireless data card is securely kept to prevent damage, theft or loss.

iii. The rules and guidelines of the DTCS Computer, Laptop and Peripheral Policy are applicable to officials issued with wireless data cards.

iv. Employees that have been allocated laptops, memory sticks or any other mobile device must take the utmost care in preventing theft, damage or loss of the equipment.

v. In the unfortunate instance where any equipment has been stolen, the responsible employee must report the matter to the South African Police Services (SAPS) within 24 hours. The case number and a report detailing the incident must then be submitted to Security and Risk Management and to Asset Management. Equipment that is lost must be reported to Asset Management and the GITO in writing within 48 hours.

vi. If any equipment is lost/stolen due to the employee's negligence (leaving the equipment in an unlocked office, visible areas in motor vehicle, not locked to workstation, etc.), or damaged (broken laptop screens, keyboards, etc) due to mishandling, the employee shall make good the loss financially.

vii. If the loss is incurred within 36 months of allocation of the equipment, the value shall be equal to the replacement value of new equipment of the same make and type. If

the loss is incurred after 36 months of allocation of the equipment, then the depreciation value shall be taken into account when determining the value of the equipment following SCM frameworks.

viii. Any deviation from this can only be made in writing by the Head of Department.

ix. No person other than the employee may have access to the computer equipment. The exceptions are IT officials and 3rd party contracted support service providers.

x. No employee may use any of the government issued equipment for financial gain.

xi. Employees are encouraged to handle all equipment with care and respect for government property. Mobile equipment should be transported in their appropriate carry bags. Regular cleaning should also be done by the employee that has been issued with such equipment. This should be enforced by the employee's respective supervisors. If there is any evidence of an employee deliberately damaging equipment, then clause 10.5(iv) will be enforced. It is the responsibility of each employee to care for the equipment that has been assigned to him/her.

xii. All laptops are to be locked with a locking device which makes the equipment hard to steal and move away from the desk that it has been fixed to. The GITO shall be responsible for providing employees with such locking devices. The department shall not be responsible for a loss of laptop stolen from the vehicle due to unlocked vehicle. Officials must keep in mind the technique of gate remote control that prevent vehicles to lock, it is the responsibility of the asset holder to ensure the vehicle is locked before leaving the vehicle.

9.7. Replacement of Equipment

i. The general trend in replacing laptops and desktop computers is every 36 month period. The department has also opted to follow this as IT Best Practices. Only equipment that is dysfunctional or does not support individual job description will be replaced before the 36 month period. Equipments that GITO feels are still functional after 36 months period can still be utilized by such employees and can be reallocated to lower management when newer equipments are procured.

ii. Redundant equipment will be sent for refurbishing and donated to a public institution or sold (in line with the Supply Chain Management (SCM) disposal principles).

iii. Printers will be replaced every 54 months. Only dysfunctional or unsuitable printers will be replaced before the 54 month period.

9.8. Requisition of Equipment

Equipment requisitions must be made in writing by the respective Director to the GITO, briefly describing the reason for the equipment, the employee that will be using the equipment and the location of the equipment, before the requisition could be considered. **No verbal requests for equipment will be processed.**

9.9. Transfer of Equipment

i. An employee who vacates or relinquishes a position by virtue of which she or he had been allocated specific computer equipment must hand over the equipment to Asset Management and inform GITO about the movement.

ii. The employee must ensure that they receive acknowledgement of receipt on handing-over of the equipment to Asset Management and/or GITO.

iii. No employee shall move or transfer equipment from one office to another or one location to another without properly informing Asset Management. Only after Asset Management has done the proper entries in the asset register, then only will the GITO officials assist in configuring such equipment for an employee.

9.10. Condition of use of ICT Equipment

i. Employees are to collect all equipment that has been approved by the GITO, from the department stores. The serial numbers, make, model and asset tags must be recorded in the asset register before any equipment is issued to an employee. The employee collecting the equipment must sign the stores register to acknowledge receipt of such equipment.

ii. Employees are advised to ensure the security of their assigned equipment. Special care must also be given in the daily use of the equipment.

iii. Computers and laptops must be shut down after the employee has finished work at the close of business. This gives the equipment a chance to cool down and refresh

its memory.

iv. This policy should be applied in line with all relevant departmental ICT policies.

v. Each employee should have either a hard copy or electronic soft copy of this policy as a reference and guide. The policy can also be obtained from the Government Information Technology Office (GITO)

9.11. Call Logging Procedure

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

i. The user identifies the problem and prepares the following: equipment type, model, serial number, the user's name, office number and location.

ii. The user can log calls using the following Telephone number 0800115575 or speed dials provided by IT officials dependent on district/location

iii. The GITO or SITA contracted official shall attend to the user to solve the problem.

iv. If the equipment is broken the equipment shall be sent for repairs. A loan equipment shall be allocated in the meantime.

10. Default/Non-compliance

This policy is subjected to every employee of DTCS and its contractors. Failure to comply with this policy shall be subjected to appropriate disciplinary action in accordance with DTCS disciplinary code and procedures.

Non DTCS personnel found in contravention of this policy shall be denied access to the DTCS infrastructure. Depending on the severity of non-compliance a criminal case may be opened.

Fraud cases shall be reported to the police and legal proceedings may be instituted against the responsible individuals.

11. Inception Date

This policy come into effect from the 1st day of the next month after date of approval.

12. Termination and Review conditions

This policy and its annexures shall be reviewed every 36 months from the inception date. The policy will remain in force until and unless is necessary to be amended or reviewed.

13. **Enquiries**
All enquiries related to this policy should be directed to GITO as the custodian of this policy.

RECOMMENDED/NOT RECOMMENDED

19/3/21

ACCOUNTING OFFICER **DATE**

APPROVED/NOT APPROVED

30/03/2021

MEMBER OF EXECUTIVE COUNCIL **DATE**

Annexure A: Guidelines for Electronic Mail Etiquette

This section presents some simple guidelines for electronic mail etiquette. It does not try to mandate any particular style or rules: it is instead an attempt to highlight important issues affecting the clarity of the electronic mail we send. After all, electronic mail is about communication, so clarity should be our goal.

1. Addresses and Personal Names

A personal name is an arbitrary string many mailers shall allow you to define that is attached to your e-mail address.

Always **provide** a personal name if your mail system allows it - a personal name attached to your address identifies you better than your email address can on its own.

Use a sensible personal name: AGuess who@ or other such phrases are annoying as personal names and hinder the recipient's quick identification of you and your message.

If your mail system lets you use **personal names** in **the addresses to which you send mail**, try to use them. This shall often help a postmaster recognize the real recipient of the message if the address is invalid.

E.g. the address ab32@isp.co.za conveys less information than if it were written as security@isp.co.za

2. Subject Lines

2.1 **Always include a subject line** in your message. Almost all mailers present you with the subject line when you browse your mailbox and it is often the only clue the recipient has about the contents when filing and searching for messages.

2.2 Make the **subject line meaningful**. For example, sending a message to WordPerfect Technical Support with the subject Word Perfect is practically as unhelpful as having no subject at all. Something like Spell Checker Not Responding shall be much more helpful and indicates exactly what the subject of your message is.

2.3 if your are **replying** to a message but are changing the subject of the conversation, **change the subject** too - or better still, **start a new message** altogether. The subject is usually

the easiest way to follow the thread of a conversation, so changing the conversation without changing the subject can be confusing and can make filing difficult.

3. Message length, Content and Format

3.1 Try to match your **message length** to the tenor of the conversation: if you are only making a quick query, then **keep it short and to the point.**

3.2 In general, **keep to the subject** as much as possible. If you need to branch off onto a totally new and different topic then it is often better to send a new message, which allows the recipient the option of filing it separately.

3.3 Don=t type your message in all upper case - it is extremely difficult to read (although a short stretch of upper case may serve to emphasise a point heavily). Try to **break your message into logical paragraphs** and restrict your sentences to **sensible lengths.**

3.4 Use **correct grammar and spelling**. Electronic mail is all about communication - poorly worded and mis-spelled messages are hard to read and potentially confusing. Just because electronic mail is fast does not mean that it should be slipshod. If your words are important enough to write, then they are also important enough to write properly.

3.5 **Avoid public Aflames@** - messages sent in anger. Messages sent in the heat of the moment generally only exacerbate the situation and are usually regretted later. Settle down and think about it for a while before starting a flame war. Avoid quotes that might offend people on the grounds of religion, gender, disability, politics, parenthood or childlessness.

3.6 If your mail program supports **fancy formatting** (bold, italic and so on) in the mail messages it generates, make sure that the recipient has a mail program that can display such messages. At the time of writing, most Internet mail programs do not support anything other than plain text in messages, although this shall change over time.

3.7 **Be very careful** about including **credit card numbers** in electronic mail messages. Electronic mail can be intercepted in transit and a valid credit card number is like money in the bank for someone unscrupulous enough to use it.

4. Replies

4.1 Include enough of the original message to provide a context. Remember that electronic mail is not as immediate as a telephone conversation and the recipient may not recall the contents of the original message, especially if he or she receives many messages each day. Include the **relevant section from the original message** helps the recipient at place your reply in context.

4.2 **Include only the minimum** you need from the original message. One of the most annoying things you can encounter in e-mail is to have your original 5 page message quoted back at you in its entirety, with the words AMe too@ added at the bottom. Quote back only the smallest amount you need to make your context clear. Exclude attachments if they are not necessary.

4.3 Use some kind of **visual indication** to distinguish between text quoted from the original message and your new text - this makes the reply much easier to follow **A>@** is a traditional marker for quoted text, but you can use anything provided its **purpose is clear** and you use it **consistently.**

4.4 Pay careful attention to where your reply is going to end up: it can be embarrassing for you if a personal message ends up on a mailing list and it is generally annoying for the other list members.

4.5 Ask yourself **if your reply is really warranted** - a message sent to a list server that only says Al agree@ is probably better sent privately to the person who originally sent the message.

5. Signatures

A **signature** is a small block of text appended to the end of your message which usually contains your **contact information**. Many mailers can add a signature to your message automatically. Signatures are a great idea but are subject to abuse: balance is the key to a good signature

5.1 **Always use a signature** if you can: make sure it identifies who you are and includes alternative means of contacting you (phone and fax are usual). Your signature must contain your identification information and the website of the Office only.

5.2 Keep your signature **short** - four to seven lines is a handy guideline for maximum signature length. Unnecessarily long signatures waste bandwidth (especially when distributed to lists) and can be annoying.

5.3 Avoid adding **random strings** to your signature. You should consider the following basic rules though.

6. Courtesy

Electronic mail is all about communication with other people and as such some **basic courtesy** never goes amiss.

6.1 If you are asking for something, don=t forget to say **Aplease@**. Similarly, if someone does something for you, it never hurts to say **Athank you@**. While this might sound trivial, or even insulting, it is astonishing how many people who are perfectly polite in everyday life seem to forget their manners in their e-mail.

6.2 **Don=t expect an immediate answer**. The fact that you don=t get an answer from someone in ten minutes does not mean that he or she is ignoring you and it is no cause for offence. Electronic mail is all about dealing with your communications when you are able to do so.

6.3 Always remember that **there is no such thing as a secure mail system**. It is unwise to send very personal or sensitive information by e-mail unless you encrypt it using a reliable encryption. Remember the recipient - you are not the only person who could be embarrassed if a delicate message falls into wrong hands.

6.4 **Include enough information**. If you are sending in a question to which you expect a response, make sure you include enough information to make the response possible. For example, sending the message "My spreadsheet program doesn't work" to Technical Support really does not give them very much to work with. Similarly, sending the message "What has happened to my order?" to a vendor is also unhelpful. When requesting technical support, include a **description of the problem** and the version of the program you are using. When following up on an order, include **the order number, your name and organisation** and any other details that might assist in tracing your order.

7. The Bottom Line

Above all else, remember that electronic mail is about communication with other people. When you compose an e-mail message, read it over before sending it ask yourself what your reaction would be if you received it. Any time spent on making our e-mail clearer is time well-spent, so let's start taking the time.