education
DEPARTMENT: EDUCATION
MPUMALANGA PROVINCE

DEPARTMENT OF EDUCATION

MANAGEMENT INFORMATION AND TECHNOLOGY

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY (ICT POLICY)

MARCH 2022

1.0

DOCUMENT CONTROL

education DEPARTMENT: EDUCATION MPUMALANGA PROVINCE	**POLICY:** **ICT POLICY**	**Department**	MIT
		Division	ICT
	MIT-ICT-	**Section**	
		Revision #	1.0
Issue Date:	**MARCH 2022**	**Last Reviewed:**	MARCH 2022
Policy Owner:	MIT	**Head of Education Approval:**	

TABLE OF CONTENTS

POLICY STATEMENT **6**

1. PURPOSE **8**

2. OVERVIEW **8**

3. LEGAL COMPLIANCY **8**

4. DEFINITION OF TERMS **9**

5. APPLICABILITY **10**

6. POLICY STATEMENT **10**

6.1. ACCESS AND SECURITY 10
6.2. APPLICABLE RULES ON USING MIT INFRASTRUCTURE 11
6.3. SOFTWARE USAGE 11
6.4. HARDWARE USAGE 12

7. E-MAIL USAGE **13**

7.1. ACCEPTABLE USE OF E-MAIL 13
7.2. UNACCEPTABLE USE OF E-MAIL 13
7.3. E-MAIL STORAGE 14
7.4. MAILBOX MAINTENANCE 14
7.5. E-MAIL FILTERING AND LIMITATIONS 14
7.6. E-MAIL IDENTIFICATION AND DISCLAIMER 15

8. INTERNET USAGE **15**

8.1. APPROPRIATE USE 15
8.2. PROHIBITED USE 15
8.3. INTERNET USE ETIQUETTE 16
8.4. MONITORING AND FILTERING 16

9. BRING YOUR OWN DEVICE (BYOD) **17**

10. USER ACCOUNT MANAGEMENT PROCEDURES **17**

10.1. GENERAL 17
10.2. TYPES OF USER/NETWORK ACCOUNTS 17
a) Creating User Accounts *17*
b) Password Management *18*
c) Managing inactive user Accounts *18*
d) Removal of resigned or suspended users *19*
e) User movement in AD *19*
f) Enabling an account *19*
10.3. ACCOUNT HOLDER ENTITLEMENTS 19

11. USER ACCOUNTS MANAGEMENT PROCEDURES **19**

11.1. CREATING USER ACCOUNTS 19
11.2. ACCOUNT MANAGEMENT 20
11.3. ACCOUNT CLOSURE AND DELETION 20
11.4. MANAGING INACTIVE USER ACCOUNTS 21

12. PASSWORDS **21**

12.1. TECHNICAL REQUIREMENTS 21
12.1.1. Operating System Passwords *21*
12.2. PASSWORD REUSE 22
12.3. PASSWORD COMPLEXITY 22
12.4. PASSWORDS MUST NEVER BE WRITTEN DOWN 22
12.5. PASSWORD SHARING PROHIBITION 22
12.6. ELECTRONIC STORAGE OF PASSWORDS IN READABLE FORM 22
12.7. ENCRYPTION OF PASSWORDS 23
13. AWARENESS REGARDING THE USE OF ACCOUNTS 23
14. STANDARDIZING OF COMPUTER SPECIFICATIONS 23
14.1. COMPUTER USE CLASSIFICATION. 23
14.1.1. Computer specifications *23*
15. SECURITY 25
15.1. ROLES AND RESPONSIBILITIES 25
15.1.1. The ICT Sub directorate *25*
The ICT Sub directorate is responsible for maintaining the ICT Policy, distributing the policy to all Directorates and for supporting the Director of ICT Sub-Directorate in the enforcement of the policies where necessary *25*
15.1.2. SENIOR MANAGEMENT *25*
15.1.2. ICT SECURITY MANAGER *25*
15.2. SECURITY INCIDENTS *25*
5.2.1. ICT SECURITY INCIDENT RESPONSE TEAM 26
5.2.2. ROLE OF ICT SECURITY INCIDENT RESPONSE TEAM *26*
5.2.3. USER ROLES AND RESPONSIBILITIES *26*
5.2.4. PHYSICAL SECURITY *27*
5.2.5. VISITORS *28*
5.2.6. EQUIPMENT SECURITY *28*
5.2.7. PHYSICAL ACCESS CONTROL *28*
15.3. DATA ACCESS CONTROL SECURITY *28*
15.3.1. DATA ACCESS CONTROL 29
15.3.2. USER IDENTIFICATION *29*
15.3.3. USER PRIVILEGES MANAGEMENT *29*
15.3.4. NETWORK ACCESS CONTROL *29*
15.3.5. LOGGING *29*
15.3.6. REMOTE DESKTOP ACCESS *29*
15.4. DATA SECURITY *30*
15.4.1. OVERALL DATA CONFIDENTIALITY 30
15.5. APPLICATION SECURITY *30*
15.5.1. APPLICATION DEVELOPMENT & MAINTENANCE 31
15.6. NETWORK AND COMMUNICATION SECURITY *31*
15.6.1. GENERAL NETWORK PROTECTION 31
15.6.2. MOBILE AND HOME COMPUTING USAGE *31*
15.6.3. PROTECTION AGAINST COMPUTER VIRUS, INTRUSIONS AND MALICIOUS CODE *31*
15.6.4. SOFTWARE AND PATCH MANAGEMENT *31*
15.6.5. WIRELESS SECURITY *32*
15.6.6. SOFTWARE INSTALLATIONS *32*
16. INCIDENT MANAGEMENT RESPONSE 32

16.1. INCIDENT REPORTING 32
16.2. MONITORING AND REPORTING AN INCIDENT 33
16.3. DOCUMENTATION 33
16.4. DISABLING ACCOUNTS/NETWORK CONNECTIONS 33
16.5. COMMUNICATION / CONTROL 33
16.6. OBTAINING EVIDENCE 33
16.7. PRESERVE CONFIGURATION 33
16.8. QUERY EXTERNAL RESOURCES 34
16.9. LIAISON WITH THIRD PARTIES 34
16.10. FOLLOW-UP ACTIONS 34
16.11. RECORDS OF SECURITY INCIDENTS 34
16.12. MISUSE OF MDOE FACILITIES 34
16.13. STAFF AND THIRD PARTIES 34
17. EXTERNAL CONSULTANTS 34
18. PRIVACY 35
19. FAILURE TO COMPLY 35
20. STANDARDS APPLICABLE TO THIS POLICY 35
APPENDIX A: PROCEDURES 36
ANNEXURE B: NETWORK ACCESS 37
ANNEXURE C: INFORMATION SECURITY INCIDENT FORM 38

Policy Statement

- Information is a critical asset of Mpumalanga Department of Education hereafter referred to as 'the Department'. Accurate, timely, relevant, and properly protected information is essential to the success of the Department's academic and administrative activities. The Department is committed to ensuring all access to, uses of, and processing of Department information is performed in a secure manner.
- Information Communication Technology Sub-Directorate hereafter referred to as 'ICT Sub-Directorate' plays a major role in supporting the day-to-day activities of the Department. The ICT Sub-Directorate include but are not limited to all infrastructure, networks, hardware, and software, which are used to process, transport or store information owned by the Department.
- The object of this ICT Policy and its supporting technical requirements is to define the security controls necessary to safeguard the Departments Information Systems and ensure the security confidentiality and integrity of the information held therein.
- The Policy provides a framework in which security threats to the Departments Information Systems can be identified and managed on a risk basis and establishes terms of reference, which are to ensure uniform implementation of Information security controls throughout the Department
- The Department recognizes that failure to implement adequate information security controls could potentially lead to:
  - Financial loss
  - Irretrievable loss of Important Departmental data
  - Damage to the reputation of the Department
  - Legal consequences
- Therefore, measures must be in place, which will minimize the risk to the Department from unauthorized modification, destruction or disclosure of data, whether accidental or deliberate. This can only be achieved if all employees observe the highest standards of ethical, personal and professional conduct. Effective security is achieved by working with a proper discipline, in compliance with legislation and Departmental policies, and by adherence to approved Departmental Policies
- The Information Communication Technology Policy applies to all employees of the Department and all other users authorized by the Department.
- The Information Communication Technology Policy does not form part of a formal contract of employment with the Department, but it is a condition of employment that employees will abide by the regulations and policies made by the Department from time to time. Likewise, the policies are an integral part of the Regulations for Employees
- The Information Communication Technology Policy relates to use of:
  - All networks connected to the Department's backbone
  - All Departmental-owned/leased/rented and on-loan facilities.
  - To all private systems, owned/leased/rented/on-loan, when connected to the Department's network directly, or indirectly.
  - To all Departmental-owned/licensed data/programs, on Departmental and on private systems.
  - To all data/programs provided to the Department by sponsors or external agencies.
- The objectives of the Information Communication Technology Policy are to:
  - Ensure that information is created, used and maintained in a secure environment.

- Ensure that all of the Department's computing facilities, programs, data, network and equipment are adequately protected against loss, misuse or abuse.
- Ensure that all users are aware of and fully comply with the Policy Statement and any relevant supporting policies and procedures.
- Ensure that all users are aware of and fully comply with the relevant legislation.
- Create awareness as and when required that appropriate security measures must be implemented as part of the effective operation and support of Information Security.
- Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle.
- Ensure all Department owned assets have an identified owner /administrator

- The Director of ICT Sub-Directorate and his/her delegated agents will enforce the Information Communication Technology Policy and any associated supporting policies.

1. PURPOSE

The purpose of this policy is to institutionalise the ICT governance as an integral part of corporate governance within the Mpumalanga Department of Education (MDoE) as defined by the Corporate Governance of ICT Policy Framework. The purpose is also to set out the minimum principles and procedures that govern the computer security systems with respect to acceptable use of its Management Information and Technology (MIT) infrastructure within the Department of Education (DoE). This policy has been created in order to preserve the integrity, availability and confidentiality of the Department's information systems. MDoE retains the right to amend this policy at any time and any modification shall be automatically effective to all computer users when adopted and approved.

2. OVERVIEW

The Department of Education relies on computer networks, systems and software to carry out its daily operations. Computer users are located in several buildings, districts and circuits in the province. In order to facilitate communication and the exchange of information amongst the dispersed users, MDoE owns and maintains local area networks (LANs) and wide area networks (WANs).

The computer systems and all related computer equipment used by all personnel, remains the property of MDoE and users must use these systems mainly for official or business-related purposes. Computer resources are made available to users for the purpose of executing Mpumalanga Department of Education's business and as such, access to said systems and related infrastructure may be revoked at any time if it is deemed to be in the best interest of MDoE. Improper use of any of these systems is a violation of MDoE's policy, and transgressors will be subject to disciplinary action, that will be instigated and carried out by the individual user's departmental/line management.

3. LEGAL COMPLIANCY

Computer users shall not post, transmit, re-transmit or store material on or through any of the services or products which in the sole judgment of MDoE:

a) Is in violation of any local or non-South African law or regulation;
b) Is threatening, obscene, indecent, defamatory or could otherwise adversely affect any individual, group or entity (collectively, "Persons"); or
c) Is violating the rights of any person, including rights 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 users. Users shall be responsible for determining what laws or regulations are applicable to the use of MDoE's services and resources.

4. DEFINITION OF TERMS

"Chain e-mail" - e-mail sent to successive people. Typically, the body of the note has direction to send out multiple copies.

"Computer system" is any interconnected equipment that is used in the automatic acquisition, storage, manipulation, management, control, display, switching, interchange, transmission, or reception, of data or information. The term includes computers; ancillary equipment; software, firmware and similar programs; services, including support services; and related resources.

"DoE"- Department of Education.

"E-mail" - any electronic message that depends on computing facilities to create, send, forward and reply for purpose of asynchronous communication across computer network system between or among individuals or groups.

"E-mail attachment" – files attached to your e-mail.

"E-mail disclaimer" – a footnote releasing the employer (DoE) of any liability as a result of the e-mail and defines terms and conditions of use.

"E-mail signature" – an endnote of an e-mail consisting of an individual's work contact details.

"ICT" is Information and Communication Technology

"Junk mail" – all non-work related mail that adversely affects productivity at work.

"MIT"- Management Information and Technology.

"Networks" include communication capabilities that allow one user or system to connect to another user or system. Networks can facilitate communication between computers within a system, or between computers in different systems. Examples of networks include Local Area Network (LAN) or Wide Area Networks (WAN), including public networks such as the internet. These are large computer networks of information resources that interconnect innumerable smaller groups of linked computer networks worldwide.

"Phishing" – an e-mail fraud scam conducted for the purposes of information or identity theft.

"SPAM" – unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple individuals, or newsgroups, junk e-mail etc.

"Users (system users, computer users)" are all Department of Education employees, contract employees (internal and external), interns and learners, who use, manage, operate or supply services to the Department's computer systems.

"Virus warning" - E-mail containing warnings about virus or malware. The overwhelming majority of these e-mails turn out to be a hoax and contain bogus information usually.

5. APPLICABILITY

This policy applies to all MDoE employees, contract employees (internal and external), interns and anyone in the learnership programme of the MDoE and (all the users who connects to the MDoE's network remotely.

With the exception of access to material intended for the general public, use of information systems and networks shall be restricted to registered users only.

6. POLICY STATEMENT

It is the policy of the Mpumalanga Department of Education to ensure the security of its computer systems, including their physical components and the information stored therein. The security requirements and procedures in this document is intended to eliminate or reduce the risk of security threats to the Department's systems to an acceptable level and to protect the Department against the financial and other costs that result when information is lost, compromised or unavailable when needed.

6.1. ACCESS AND SECURITY

Authorized Access: Access to networks and computer systems will be executed by Systems Administrators of those systems. A user will be granted access to systems and services based on the employee's business needs.

Employees are given access to the computer network to assist them in the performance of their duties. Thus, data created, stored, sent or received by utilizing the DoE's computer network should not be considered as private or secure. Users expressly waive any right to privacy in the data they create, store, send or receive on the computer or through the internet or any other computer network. MDoE, through any of its designated employees, reserves the right to access data created, stored, sent or received on its computer network without prior notification to the user/group concerned.

Unauthorized Access is not allowed. Users who abuse their access privileges by attempting to gain unauthorized access into restricted systems; files; e-mail and networks of DoE or any other entity will be subject to appropriate disciplinary action, which will be carried out by the individual's department/line management. Reactivation of unauthorized users profile will only be done by the MIT directorate.

User's responsibility to minimize security risks: Every user is responsible for minimizing MDoE's data security risks by taking reasonable precautions when accessing the Internet or any other computer and network resource. This duty includes the prevention of unauthorised access into MDoE's networks and the prevention of virus introduction into MDoE's networks and systems.

6.2. APPLICABLE RULES ON USING MIT INFRASTRUCTURE

a) Use of MIT infrastructure for private or personal purposes is allowed within reason e.g. internet banking, sending of personal emails, limited private word processing and other related private files – of which the latter must be stored on the C drive of the Laptop/Desktop. The MIT directorate uses MIT resources to perform its duties in terms of all applicable laws and internal policies. Every official electronic interaction creates a legal responsibility for MDoE and may lead to legal accountability, exposure and risk.

b) MIT Administrators must not create new network accounts without the approval of the immediate supervisor.

c) Users are only allowed to access information they have been authorised to use;

d) Users must not attempt to gain access to information they are not authorised to access;

e) Passwords must always be protected. Users may not give their passwords to any person, including senior staff or the service desk staff; and the screen locks the desktop after 10 minutes of no activity;

f) Users must choose and change passwords in accordance with the appropriate procedures (refer to section 12: Passwords);

g) Users must take reasonable measures to avoid introducing viruses into the Department of Education's network;

h) Users are not allowed to download, install or run security programs or utilities – such as password cracking programs – that reveal weaknesses in the security of the system, on the Department's computer systems. Security vulnerability tools are to be used by approved personnel ONLY and such use must be limited to a pre-approved period of time.

6.3. SOFTWARE USAGE

DoE purchases software packages under license agreements including site licenses, volume licensing agreements, concurrent-use licenses and individual copy licenses. These license agreements restrict the right to make copies of the software and/or the way in which the software is used. Any unauthorized duplication of software, except for backup and archival purposes, is contrary to the DoE's policies and may be a violation of copyright or other laws. Any such back-ups may only be made by MITs network administrators; no other official in the DoE may do so.

Compliancy with laws and license agreements: Software must be used in accordance with the terms of license agreements; copyrights; and all other applicable laws. The Department of Education will not tolerate the use of any unauthorized copies of software on DoE systems. Licensed software will be provided to all employees to perform DoE duties.

Purchasing of software: Software must be purchased in accordance with the standards set by the MIT directorate, and users may not agree to a license or download any material for which a registration fee is charged or purchase any software application without first obtaining the express written permission from the MIT directorate.

Software misuse: Without prior written authorization of the MIT directorate, users may not do any of the following:

- Copy software for use on their home computers;
- Provide copies of software to any independent contractors, consultants or customers of the MDoE or to any third party;
- Install software on any of the Department of Education's workstations or servers;
- Modify, revise, transform, recast, or adapt any software;

Employees who become aware of any misuse of software or violation of copyright law should immediately report the incident to the Service Desk.

Use of non-standard software: The MDoE has standardized software utilization. A list of standard software is available from the MIT directorate. A written permission from the MIT directorate is required for the purchasing and utilization of software which is not part of the MDoE's software standards.

Internal development of software: Any internally developed software shall be done on a test environment and not on the MDoEs production environment. Internally developed software must first be approved by the MIT directorate prior to distribution.

6.4. Hardware Usage

Computer equipment and infrastructure such as cabling must be purchased in accordance with the standards set by the MIT directorate. No computer equipment, desktop computers, laptops, monitors, printers, scanners and tablets/iPads must be procured without first obtaining approval from MIT. Hardware users of DoE are expected to:

a) have a shared responsibility for protecting their computers from theft, damage or abuse;
b) take reasonable steps to safeguard computer equipment against waste, loss, abuse, unauthorised use, and misappropriation;
c) Use only the equipment that they have been authorised to use;
d) NOT eat, drink or smoke near computer equipment or media in a manner that would endanger the equipment or media;
e) NOT store highly combustible materials near a computer;
f) NOT move or remove a PC, laptop, or other computer hardware from their workstation without proper permission from Asset Management;
g) Promptly report missing computer equipment to Asset Management, the police and to MIT within 24 hours; and
h) NOT allow anyone without proper identification and authorisation to perform maintenance on computer equipment.

7. E-MAIL USAGE

7.1. Acceptable use of e-mail

a) All users of Department of Education electronic resources are expected to utilize such resources in a responsible, ethical and legal manner consistent with applicable government laws and policies.

b) Each user shall be provided with an e-mail account for conducting official business. This account shall be the only account the employee or contractor may use to conduct official business.

c) Reasonable private use of email may be allowed, provided that the user does not create an impression that he is communicating on behalf of MDoE. Such use must adhere to all policies of MDoE.

d) All e-mail messages created and stored on the Department's computers or networks are the property of the MDoE and may be accessed by the MDoE's users.

e) The content and maintenance of an e-mail mailbox is the responsibility of the person to whom the e-mail account is assigned.

f) All employees must use e-mail as they would any other type of official Mpumalanga Department of Education communications tool.

g) The Department may provide access to e-mail to non-Department of Education personnel, such as contractors, temporary employees, or other government agencies, provided there is written approval from the relevant supervisor.

h) Mpumalanga Department of Education reserves the right to review and monitor all employee e-mail communications. Electronic mail messages may be retrieved by MDoE even though they have been deleted by the sender and the reader.

i) Only authorized e-mail software may be used for conducting the Mpumalanga Department of Education business.

j) All e-mail messages must contain the name and e-mail address of the sender and a subject heading that reflects the content of the message without divulging highly-sensitive information.

k) Shared/Office e-mail boxes may only be used to receive e-mail. Senders must be identified as an individual, whenever possible.

l) Broadcast messages (messages to multiple offices) may only be sent by pre-approved designees.

7.2. Unacceptable use of e-mail

a) Use of Mpumalanga Department of Education's e-mail system that could cause congestion, delay, or disruption of service to any government system (for example, video, sound or other large file attachments can degrade the performance of the entire network).

b) Using private e-mail accounts for official Mpumalanga Department of Education business.

c) Using the Department of Education e-mail system for business purposes other than Department of Education business, including using the system for private commercial activities;

d) Using or sending anonymous e-mail for any purpose (E-mail communications must accurately identify the sender);

e) Using the e-mail system to intentionally misrepresent oneself or the MDoE;

f) Using the e-mail system to participate in any non-work related "chat room;"

g) Using the e-mail system to send or forward any information that can be interpreted as sexually implicit or explicit, or derogatory toward any racial, religious, or ethnic group. Harassing or obscene material shall also not be sent, printed, requested, displayed, or stored. Also, the system shall not be used for any mass mailing, such as, SPAM, chain letters, and/or JUNK MAIL.

h) Using e-mail to improperly disclose sensitive information or to communicate unethical information or information that could be perceived to be a conflict of interest;

i) Using e-mail for unlawful activities, including any communication that violates security policies, government laws, or regulations;

j) Using e-mail to send classified or proprietary information;

k) Using E-mail for malicious activities, such as, knowingly activating and/or propagating computer viruses, or other malicious codes, or purposefully disguising the true content of an E-mail message with a subject or title that is not reflective of the message content; and

l) Joining electronic discussion groups, e.g., listservs or Usenet newsgroups that are not related to Department of Education business.

m) Permitting others (e.g. supervisors, secretaries, assistants, or any other subordinate) to use your email accounts as their own.

7.3. E-Mail Storage

Storage is an expensive commodity and therefore limits are placed on the allocations of storage to users.

Mailbox Sizes
Users are provided with a standardized mailbox size

Should a user exceed the approved size limitations, the mailbox in question needs to be archived. It is furthermore the responsibility of the user to perform the necessary mailbox clean up actions.

The size limitation that is set out in this policy is the MIT directorate standards for acceptable usage. Should a user be in need for more storage it can be obtained through the approval of the MIT directorate.

7.4. Mailbox maintenance

a) It is recommended that users delete old and obsolete mails from their mailbox, which includes the sent items folder, calendar items, tasks and other mail folders.

b) All unnecessary messages should be manually deleted, within 30 days, to prevent messages from being archived.

c) It is recommended that any attachments, wanting to be kept, should be saved outside of the e-mail system.

7.5. E-Mail Filtering and Limitations

All e-mail entering and leaving the Department will be filtered for, amongst others, content, spam, worms, viruses and malicious code.

7.6. E-Mail Identification and Disclaimer

To ensure that e-mail message is properly identified, apart from the sender's e-mail address it is compulsory that all e-mail leaving the Mpumalanga Department of Education include an e-mail signature as well as an e-mail disclaimer.

8. INTERNET USAGE

The requirements for complying with this policy are set out in the following sections:

8.1. Appropriate Use

Users are encouraged to use the Internet to further the objectives of the MDoE. The types of activities that are encouraged include:

a) MDoE's internet access facility is intended to support the Department's legitimate business requirements.
b) Users must ensure that they use the internet legally at all times.
c) Occasional and reasonable use of the internet for personal purposes is acceptable provided that:
   - Internet access is not used for private business or other commercial purposes including the sale or purchase of goods and services.
   - Personal internet usage does not interfere with the performance levels of the user's duties.
   - There is no additional cost to the Department in using the internet for personal use.
   - There is no breach of any of the provisions of this policy, as well as those of the E-Mail Policy.

8.2. Prohibited Use

Unacceptable and forbidden user behaviour regarding access to the internet and the use of internet services encompass:

a) Individual internet use must not interfere with others' productive use of internet resources.
b) Users must not violate the network policies of any network accessed through their MDoE account.
c) Internet use at the MDoE must comply with all government laws, all Mpumalanga Department of Education policies, all Mpumalanga Department of Education contracts and all provincial policies.
d) In keeping with the confidentiality agreements, no Mpumalanga Department of Education software, documentation or other types of information may be sold or otherwise transferred to any non-departmental parties for any other than business purposes by any employee.
e) If sensitive information is lost, divulged to unauthorized parties or suspected to be lost / divulged, the MIT directorate should be notified.

f) The internet must not be used for profane, obscene, pornographic or other graphic pictures, which may be offensive and/or defamatory to others.

g) Using the Internet to search, access, disseminate, store or retrieve information that is racist, violent, offensive, sexually explicit (sexually explicit content includes e.g. Cartoons, text messages as well as photographs) are not allowed and disciplinary actions will be followed. In a case where a need arises to access such material during a disciplinary action, the relevant or affected sites will be made accessible for the period specified.

h) The internet must not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, illegal financial/non-financial trading, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses).

i) The internet must not be used in any way that violates MDoE's policies, rules, or administrative orders. Use of the internet in a manner that is not consistent with the mission of the Department, misrepresents the Department, or violates any Department policy is prohibited.

j) Mpumalanga Department of Education prohibits use of mass unsolicited mailings, access for non-employees to the Mpumalanga Department of Education resources or network facilities, uploading and downloading of files for personal use, access including attempted access to pornographic sites, gaming, competitive commercial activity unless pre-approved by the MDoE, and the dissemination of chain letters.

k) Users must not establish Mpumalanga Department of Education computers as participants in any peer-to-peer network, unless approved by management.

l) Users must not view, copy, alter, or destroy data, software, documentation, or data communications belonging to the Mpumalanga Department of Education or another individual without authorised permission.

m) Use of proxy websites to evade filtering, unblock, and bypass restricted or prohibited sites.

n) Use of File Sharing Programs (FTPs) without the written approval of the MIT Directorate.

8.3. Internet Use Etiquette

Users must abide to network etiquette rules. These rules include, but are not limited to the following:

a) Refrain from revealing personal particulars about themselves or other users to anyone else on the internet.

b) Refrain from revealing credit, credit checking accounts or identification numbers across the internet.

c) Refrain from disrupting the use of Mpumalanga Department of Education network.

d) Refrain from attempting to gain illegal access to system programs or computer equipment.

e) Refrain from using instant messaging.

8.4. Monitoring and Filtering

The MIT directorate must monitor any internet activity occurring on the Mpumalanga Department of Education equipment or accounts. Mpumalanga Department of Education currently employs filtering software to limit access to sites on the internet. In the event Mpumalanga Department of Education discovers activities which do not comply with applicable laws or Mpumalanga Department of Education policies, records retrieved must be used to document the wrongful content in accordance with due processes.

9. BRING YOUR OWN DEVICE (BYOD)

MDoE network users may only directly access MDoE network with Departmental equipment. MDoE network users that needs to access information from outside the office through their mobile devices are only allowed to do so through the provided web interface (e.g. OWA web mail access).

10. USER ACCOUNT MANAGEMENT PROCEDURES

10.1. General

- The MDoE Management Information and Technology (MIT) directorate is responsible for ensuring that the user account management procedure is adhered to.
- All authorized users will be provided a unique User/Network account for official use.
- All accounts must be uniquely identifiable by an assigned user name.
- All accounts must have a password that complies with the ICT policy.
- Accounts will be administered by an MIT designated account administrator.
- A user must use an account for the purpose provided.
- Unauthorized access to the MDoE network, resources or its applications is prohibited.

10.2. Types of User/Network accounts

Domain User Accounts

Domain user accounts are the primary and preferred method of providing access to the MDoE MIT resources. Users are accountable for their actions and can be audited by the systems to which they have access rights. Users must adhere to the terms and conditions of use set forth in the MDoE MIT policies.

Administration (Privileged) Accounts

Administrative privileges are the highest level of permission that is granted to a computer user. In business and networked systems, this level of permission normally allows the user to install software, and change configuration settings. Only MIT administrators are granted administrative privileges. MIT administrative staff can be granted privileged accounts that permit elevated access rights for specific rights for a specific system of application support and maintenance. Generic/built-in privileged accounts (e.g. Windows domain and local administrator, etc.) shall not be used for daily systems administration, administrators shall use a MDoE privileged account.

MIT administrator's activities are monitored through an audit quarterly. All reviews must be formally documented and signed off by the MIT Director. Logon violations by the administrators will lead to disciplinary action by the Accounting Officer.

a) Creating User Accounts

- A new administrator must complete the document ICT200-003 = New User Request . **This application must be approved by the Director: MIT**
- The user account is then created by the designated administrative user. User accounts must conform to the naming standards found in ICT180-002 = MDOE Naming convention
- Upon first logon the new administrator is prompted to change his\her password to ensure the user is the only person who knows the password.

b) Password Management

- All administrative user passwords are set to expire after 38 days.
- Administrative users have the right to change passwords at any time.

- The document ICT200-001 = Request to Reset a Password should be completed when the need arise to reset a password. The completed form must be submitted to ICT. The ICT personnel member that receives the form must physically verify the identity of the person submitting the form. The password will then be reset. On first logon the user is prompted to change his\her password. Administrative user passwords can only be changed by another administrator.

- Auto account lock-out has been set to lock an account after five unsuccessful logon attempts.
- Locked accounts can only be unlocked by an administrator.

c) Managing inactive user Accounts

- Administrator accounts that become inactive, must be disabled immediately.
- Administrator accounts disabled for 6 months must be deleted.

d) **Removal of resigned or suspended users**

- When an administrative user leaves\transfers from a Directorate, the Directorate must complete the form ICT200-012 = User Login Termination Request. **The document must be submitted to the Director: MIT**, who will instruct an administrative user to terminate the user access on the network. Access to the account may be granted to a nominated person from the directorate for the purpose of collecting all relevant data and e-mail from the account.
- No administrative user will be removed or deleted without a completed form.

e) **User movement in AD**

- When an administrative user moves to a different physical location, the user must complete the form ICT200-005 = User Movement Request to enable ICT to move the user object to the relevant container in AD

f) **Enabling an account**

- Disabled accounts will only be re-activated after ICT has received a completed ICT200-006 = User Enable Request form. **This form must be approved by the Director: MIT.**

Application-Specific Accounts

An application specific account controls access to individual applications available on the network. Access rights and privileges are programmed/configured within the application. These accounts must never be used for individual access to the network.

10.3. Account Holder Entitlements

MDoE provides an extensive range of computing and networking facilities to user account holders, including email, internet access, file servers, applications and access to other systems integrated within the MDoE account system. Access to these services is based on the privileges of the account's type and any individual system's access assigned to the individual account holder.

Exceptions to the standard privileges that apply to an account may be permitted where a request is made in writing and accepted by the MIT Director or its delegated persons.

11. User Accounts management procedures

11.1. Creating User Accounts

- Any request for a new account to be created must be submitted to the MIT office.
- MIT service desk will supply the requester with the "New User Request Form (ICT200-003). The form must be filled and submitted back to the service desk. For an account to be created, the form must be completed correctly and in full. The form must be signed by the account requestor as well as his/her supervisor.

- The user account is then created by the relevant MIT personnel, only MIT designated Account Administrators are allowed to create, disable or delete an account. User accounts must conform to the naming standards found in the MDoE Naming Conversion (ICT 180-002).
- A new user is not permitted, under any circumstances, to inherit the User/Network ID that was originally assigned to another user.
- Each account is created with a unique username and is based on the account holder's name.
- The MIT designated Account Administrator shall create the user account with a temporary password; the Account Administrator must ensure that "Password must be changed at first logon" option is enforced. This will allow and force the user to change his/her password at first logon to a password only they will know.
-

11.2. Account Management

Primary responsibility for account management belongs to the designated Account Administrators. The Designated Account Administrators shall:

- Modify user accounts in response to events like name changes, permission changes and office transfers.
- Should the need arise to change\amend the user information on Active Directory; the user must complete the "User Detail Update Request Form" (ICT200-002).
- In the event a user moves to a different physical location, the user must complete the User Movement Request Form (ICT200-005).
- Disabled accounts will only be re-activated once MIT has received completed User Enable Request Form" (ICT200-006).
- Periodically review existing accounts for validity.
- Cooperate fully with an authorized security team that is investigating a security incident or performing an independent audit.

11.3. Account Closure and Deletion

- A user's supervisor must immediately notify MIT or HR of changes in a user's employment status (departure, extended leave, suspension and termination).
- The designated Account Administrator will then disable or remove all associated User/Network accounts.
- Closure of an account means the account is frozen, i.e. the password is revoked, until such time as the account is reinstated or has been deactivated for six months, at which time the account is deleted.
- In the event of irregular activity being reported or suspected, MIT in consultation and cooperation with the relevant directorate, reserves the right to revoke any access privileges to any computing and networking facilities account at any time. In such cases, reinstatement of the account must be approved by MIT.

11.4. Managing Inactive User Accounts

- Accounts that are inactive for a period of 45 days will be disabled. MIT will perform this function on a monthly basis.
- Accounts disabled for a period of 6 months will be deleted. MIT will perform this function on a monthly basis.
- The Account Administrator will ensure that disabled User/Network IDs are not re-issued to new users.
- The Account Administrator will remove redundant User/Network accounts that are no longer required.

12. PASSWORDS

It is the policy of the Mpumalanga Department of Education to limit access to the Department's computer systems to authorized users and to control access to its systems (domain and applications), the Department shall issue passwords to all system users and shall use access control methods contained within and controlled by the operating systems, security subsystems, or database management systems (e.g., file attributes, access control lists, security rules, object-oriented security labels, and database schemes).

Each system user must be provided with a User ID, where after the user must create his own unique password, which must be used to access the Department's computer systems. All Mpumalanga Department of Education's MIT communication devices including supporting devices must be protected by any means of password to prevent unauthorized entry into the Department's information systems.

Users must take reasonable precautions to protect their passwords and IDs and must not share them with any person and must never display their passwords on the monitor. MIT reserves the right to monitor compliance with its password policy.

12.1. Technical Requirements

12.1.1. Operating System Passwords

a) An initial password for accessing the network must be issued to each user by the Account Administrator. After accessing the system with the initial password, the user must select a new password. Passwords must be alpha-numeric;

b) Shall be suspended after 5 invalid logon attempts; the account will be locked for a minimum of 60 minutes. and

c) The system shall force users to change passwords every 38 days (maximum password age), and

d) The document ICT200-001 = Request to Reset a Password should be completed when the need arise to reset a password. The completed form must be submitted to ICT. The ICT personnel member that receives the form must physically verify the identity of the person submitting the form. The password will then be reset. On first logon the user will be prompted to change his\her password.

A user operating systems password:

a) Must have a minimum length of 8 characters;
b) Must not contain individual names or account names;
c) Must contain at least one of the following four character groups:

- Uppercase characters (A through Z)
- Lowercase characters (a through z)
- Numeral (0 through 9)
- Non-alphabetic/special characters (such as *, @, #, %)
  - Example: **Nompi12***

12.2. Password Reuse

While the specific generation retention depends on the computer system, users on all systems are prohibited from re-using a password when prompted to change it by the system. Account Administrators and other users with similar access privileges are prohibited from using the same password on multiple systems. Active Directory will save the password history for 24 months, during which time users will not be able to reuse a password.

12.3. Password complexity

Users are required to choose passwords that are hard to guess, alpha numeric (**Nompi12***). Password must not be easily predictable words or characters such as the user's first or last name, spouse's name, name of pet, a sequence of numerals or letters, or any word found in a standard English dictionary. To this end Password Complexity will be enabled in Active Directory.

12.4. Passwords must never be written down

Users must not write down or otherwise record their passwords in readable form near the system to which the password pertains. For example, a user must not write his/her password on a note and tape it to his/her computer.

12.5. Password sharing prohibition

Passwords secure an individual account on the system. Each account must be used only by the individual formally assigned to that account. Therefore, passwords must not be exchanged or shared.

12.6. Electronic storage of passwords in readable form

Passwords must not be stored in plain text or in other readable forms in places where unauthorised parties might recover them, including, but not limited to: batch files; login scripts; computers without access control; terminal function keys; or in software macros.

12.7. Encryption of passwords

Passwords must always be encrypted when held in storage for any significant period of time or when transmitted over networks. This will prevent them from being disclosed to wire tappers, technical staff that is reading systems logs, and other unauthorised parties.

13. Awareness Regarding the Use of Accounts

When a user logs on to the system, the user accepts the logon disclaimer, stating the user's responsibilities for protecting their accounts. The disclaimer will include areas such as not sharing accounts and individual responsibilities for any access made with an account.

14. STANDARDIZING OF COMPUTER SPECIFICATIONS

The MDOE procures desktop and laptop computers for the departmental officials via a SITA contract. This memo seeks to standardize the specifications to be used when obtaining quotations as per the prescribed SITA contract procurement process.

This document defines computer specifications to be used when procuring desktop or notebook computers for the Department.

14.1. Computer use classification.

Departmental users are classified as either normal users or high-end users.
The following category of users are classified as high-end users:

- HOD
- DDG
- Chief Director

Technical users:

- Infrastructure
- ICT
- EMIS
- Communications (graphic designers)
- Any user with specific/special technical needs

14.1.1. Computer specifications

Computer specifications must be standardized to the following:

Desktop computers:

Normal user:

- Core I5 CPU
- 16 Gb RAM
- 500Gb SSD
- 21" monitor
- On-board graphics

High-end user:

- Core I7 CPU
- 32 Gb RAM
- 1 Tb SSD
- Dedicated graphics adaptor
- 24" monitor

Laptop computers:

Normal user:

- Notebook 15,6"
- Core I5 CPU
- 16 Gb RAM
- 500Gb SSD
- Bag
- Cordless mouse

High-end user:

- Notebook 15,6"
- Core I7 CPU
- 32 Gb RAM
- 1 Tb SSD
- Dedicated graphics adaptor
- Bag
- Cordless mouse

15. SECURITY

15.1. ROLES AND RESPONSIBILITIES

15.1.1. The ICT Sub directorate

The ICT Sub directorate is responsible for maintaining the ICT Policy, distributing the policy to all Directorates and for supporting the Director of ICT Sub-Directorate in the enforcement of the policies where necessary.

15.1.2. SENIOR MANAGEMENT

Managers are required to familiarize themselves with the policies. Where a policy breach is highlighted all managers must co-operate in ensuring that appropriate action is taken.

Senior Managers are obliged to ensure that all ICT systems under their remit are formally administered either by an administrator appointed by the Senior Manager or centrally by ICT Sub-Directorate.

Senior management of MDoE shall have an appreciation of ICT security, its problems and resolutions. Management has responsibilities, some of which are listed below:

a) Direct and enforce the development of security measures;

b) Ensure participation at all levels of management, administrative, technical and operational staff, and provide full support to them;

c) Working with the director of MIT as the overall supervisor and coordinator of ICT security;

d) Provide user training and awareness as and when required in order to enable them to discharge their responsibilities and perform their duties relating to ICT security; and

e) Advising all users of their ICT security responsibilities upon being assigned a new post, and as and when required throughout their term of employment.

15.1.2. ICT SECURITY MANAGER

For effective administration of Information security functions The ICT Senior Manager shall delegate, in writing, the Chief Data Technologist or an equivalent employee to be an overall ICT Security Manager.

In de-centralized offices, The ICT Senior Manager shall delegate, in writing, the Senior Data Technologist or an equivalent employee to be the ICT Security Manager for a specified jurisdiction.

The ICT Security Manager (ITSM) is responsible for ICT security within MDoE. The roles and responsibilities of the ITSM shall be clearly defined which will include, amongst others, the following:

a) Implement and maintain an ICT security programme;

b) Lead in the establishment, maintenance and implementation of information security policies, standards,guidelines and procedures;

c) Establish incident detection and monitoring mechanism to detect, contain and ultimately prevent security incidents;

d) Ensure that system logs and other supporting information are retained for the proof and tracing of security incidents;

e) Ensure that ICT security risk assessments and audits are performed;

f) Assist with investigations and rectification in case of ICT security breaches;

g) Render advisory services on ICT security within MDoE;

h) Ensure that ICT staff have unescorted access to Information Systems and resources by selecting and making them aware of their responsibilities and duties, and formally notifying them of their authorization;

i) Ensure that security protection is responsive and adaptive to changing environment and technology; and

j) Enforce the least privilege principle when assigning ICT resources and privileges to users

k) Review Security controls and Systems as and when required or when the need arises.

15.2. SECURITY INCIDENTS

All security incidents whether affecting the entire network or affecting only a single user, are to be logged and processed in conjunction with MIT. Reference is made to the standard operating procedures for ICT services.

5.2.1. ICT SECURITY INCIDENT RESPONSE TEAM

The ICT Security Incident Response Team is the central focal point for coordinating the handling of IT security incidents occurring within MDoE. The Team (Provincial and de-centralised offices) shall consist of the ISMC and the line manager affected by the security incident.

5.2.2. ROLE OF ICT SECURITY INCIDENT RESPONSE TEAM

a) Provide overall supervision and co-ordination of ICT security incident handling for all information systems within the Department;

b) Make decisions on critical matters such as system recovery, the engagement of external parties (including law enforcement agencies) and the extent of their involvement;

c) Determine service resumption logistics after recovery; and

d) Provide management endorsement on the provision of resources for the incident handling process

e) Document all incident handling processes undertaken.

5.2.3. USER ROLES AND RESPONSIBILITIES

1. SECURITY ADMINISTRATORS

ICT security administrators are responsible for providing security and risk management related support services. They also assist in identifying system vulnerabilities and performing security administrative work of the system. Their responsibilities further include:

a) Maintaining control and access to the system;

b) Checking and managing audit logs; and

c) Maintaining user accounts.

ICT Security Administrator may or may not be a technical person, but should not be the same person as the system administrator. There should be segregation of duties between the ICT security administrator and the system administrator.

The activities of System administrators shall be monitored and reviewed on a quarterly basis by the ICT Senior Manager or his/her designee.

2. INFORMATION OWNERS

Information owners are the collectors and the owners of information stored in databases and data files. Their primary responsibility is to determine the security requirements and security classifications usage and protection of the information.

3. USERS OF INFORMATION SYSTEMS

Users of information systems are the staff who use the information and will be accountable for all their activities. Information system users' responsibilities include:

a) Knowing, understanding, following and applying all prescribed security procedures as set out prescribed MDoE ICT Policy; and

b) Preventing unauthorized access to their computers and/or workstations.

c) Knowingly using devices (USBs, CD/DVDs etc.) that may introduce virus/malicious code to their Computer and the MDoE network.

d) Not sharing account details (username and password) with other employees or non-employees.

e) Taking additional cautionary measures in protecting the integrity of transversal systems' user-account assigned to them by the Department.

f) Not propagating/transmitting files including e-mails on the MDoE network that may cause security related hazards.

5.2.4. PHYSICAL SECURITY

1. SECURE ENVIRONMENT

a) Data centres and computer rooms shall have good physical security and strong protection from disaster and security threats, whether natural or caused by other reasons, in order to minimize the extent of loss and disruption.

b) Data centres and server rooms shall have sufficient environmental control systems to provide cooling, fire and power-surge protection.

c) Media containing business essential and/or mission critical information shall be replicated to an alternative site.

5.2.5. VISITORS

a) Visitors shall be supervised and their date and time of entry and departure recorded.
b) Visitors are only to be granted access for specific, authorized purposes and shall be issued with instructions on the security requirements and emergency procedures.
c) Contractors/Consultants/Contract employees shall obtain permission to access Data centres and Computer rooms from the relevant ICT manager.

5.2.6. EQUIPMENT SECURITY

a) Staff in possession of laptop, portable computer, personal digital assistant, or mobile computing devices for business purposes shall safeguard the equipment in his or her possession, and shall not leave the equipment unattended without proper safeguard of the equipment.
b) ICT equipment shall not be taken away from MDoE premises without approval from Asset Management.

5.2.7. PHYSICAL ACCESS CONTROL

a) A list of persons who are authorized to gain access to data centres, computer rooms or other areas supporting critical activities, where computer equipment and data are located or stored, shall be kept up-to-date and be reviewed periodically;

b) All visitors to data centres or computer rooms shall be monitored at all times by an authorized staff member of MDoE;

c) Automatic protection features (e.g. password protected screen saver, keyboard lock) in servers, computer terminals, workstations or microcomputers should be activated if there has been no activity for a predefined period of time to prevent illegal system access attempt. Alternatively, the logon session and connection should be terminated. Also, user workstation should be switched off, if appropriate, before leaving work for the day or before a prolonged period of inactivity;

d) All staff should lock the doors to their offices when offices are not in use; and

e) The display screen of an Information System on which classified information can be viewed shall be carefully positioned so that unauthorized persons cannot readily view it.

15.3. DATA ACCESS CONTROL SECURITY

15.3.1. DATA ACCESS CONTROL

a) Access to data shall not be allowed unless authorized by the relevant information owners;
b) Data access rights shall be granted to users based on the principle of least privilege.
c) Data access rights shall be clearly defined and reviewed periodically and
d) Access to an Information System containing CONFIDENTIAL or above classification information (BAS, Persal, Logis) shall be restricted by means of logical access control.
e) Where single systems have multiple levels of information security classifications then the highest level of security clearance shall be required to access all of the application software and data on the system.
f) By login into the MDoE network, users of ICT systems are formally acknowledging their obligations and responsibilities for security and maintenance of confidentiality.

15.3.2. USER IDENTIFICATION

a) Each user identity (user-ID) shall uniquely identify only one user;
b) Users are responsible for all activities performed with their user-Ids; and
c) Users should not share or allow other staff members to make use of their user- ID's and passwords.

15.3.3. USER PRIVILEGES MANAGEMENT

a) User privileges shall be reviewed periodically and the process undertaken shall be clearly outlined and documented;
b) All related Information Systems privileges shall be promptly terminated when a staff member ceases to provide services to the Department. The outgoing officer shall be responsible for the handover of IT equipment to his or her supervisor; and
c) The use of special privileges shall be restricted, controlled and reviewed.

15.3.4. NETWORK ACCESS CONTROL

Prior approval from ICT is required to connect a Departmental Information System with another Information System under the control of another Government Department. The security level of the Information System being connected shall not be downgraded.

15.3.5. LOGGING

a) MDoE shall implement logging of activities of ICT under their control according to the business needs and data classification.

The following audit policies will be logged:
Audit level

- Audit account logon events = Success, failure
- Audit account management = Success, failure
- Audit directory service access = Success, failure
- Audit logon events = Success, failure
- Audit object access = Failure
- Audit policy change = Success, failure
- Audit system events = Success, failure

b) Any log kept shall provide sufficient information to support comprehensive audits of the effectiveness of, and compliance of security measures;
c) Logs shall be retained for a period commensurate with their usefulness as an audit tool. During this period, such logs shall be secured such that they cannot be modified, and can only be read by authorized persons;
d) Regular checking on log records, especially on system or application where classified information is processed or stored, shall be performed, not only on the completeness but also the integrity of the log records;
e) All system and application errors which are suspected to be triggered as a result of security breaches shall be reported and logged; and
f) Clocks should be configured to ensure the synchronization of system time.

15.3.6. REMOTE DESKTOP ACCESS

a) Only authorized ICT personnel may access a Computer remotely using remote desktop access functionality;
b) Unless authorized by the ICT Security Manager or higher authority, the user whose Computer is being accessed remotely shall be informed prior to the remote connection;

15.4. DATA SECURITY

15.4.1. OVERALL DATA CONFIDENTIALITY

a) Data about information systems that may compromise the security of those systems shall not be disclosed to users, or any other third parties. Exceptions must be authorized by the Department's ICT Security Officer;
b) A staff member shall not disclose information about the individuals, Department or specific systems that have suffered from damages caused by computer crimes (hacking, cyber-fraud etc.) and computer abuses, or the specific methods used to exploit certain system vulnerabilities, to any people other than those who are handling the incident and responsible for the security of such systems, or authorized investigators involving in the investigation of the crime or abuse; and
c) A staff member shall not disclose to any unauthorized persons the nature and location of ICT, and the information system controls that are in use or the way in which they are implemented.

15.5. APPLICATION SECURITY

15.5.1. APPLICATION DEVELOPMENT & MAINTENANCE

a) Application development staff shall include security planning and implement the appropriate security measures and controls for system under development according to the systems' security requirements;
b) Documentation and listings of applications shall be properly maintained and restricted;
c) Formal testing and review on the security controls within new applications shall be performed prior to implementation;
d) The integrity of an application shall be maintained with appropriate security controls such as version control mechanism and separation of environments for development, system testing, acceptance testing, and live operation; and
e) Application development staff shall not be permitted to access production information unless necessary.
f) Application development staff shall sign a non-disclosure agreement with the Department to enforce confidentiality on the nature and functions of MDoE production and security systems.

15.6. NETWORK AND COMMUNICATION SECURITY

15.6.1. GENERAL NETWORK PROTECTION

Staff members are prohibited from connecting workstations to external network by means of communication device, such as dial-up modem, wireless interface, or broadband link, if the workstations are simultaneously connected to a local area network (LAN) or another internal communication network, unless with the approval of ICT.

15.6.2. MOBILE AND HOME COMPUTING USAGE

Staff members that are eligible for a laptop, personal digital assistant, tablet or equivalent mobile device used to access the MDoE's network or information resources whilst travelling or from home or any other location are required to follow the MDoE's policies and guidelines to secure and protect these devices.

15.6.3. PROTECTION AGAINST COMPUTER VIRUS, INTRUSIONS AND MALICIOUS CODE

MDoE's information systems shall be protected from computer viruses, intrusions and malicious codes. Virus signatures, malicious code definitions as well as their detection and repair engines shall be updated regularly and whenever necessary.

15.6.3.1. Anti-virus protection

a) All servers, workstations, and mobile computing devices shall contain an approved up-to-date anti-virus application.
b) Only an approved official anti-virus application shall be permitted on the MDoE network.
c) Only ICT personnel is permitted to install and/or un-install application software.

15.6.4. SOFTWARE AND PATCH MANAGEMENT

ICT shall be protected from known vulnerabilities by applying the latest security patches recommended by the product vendors or implementing other compensating security measures.

Software that no longer receives official security updates and patches from vendor(s) shall be discontinued since it poses security risks.

15.6.5. WIRELESS SECURITY

ICT shall document, monitor and control wireless networks with connection to MDoE's internal network. Proper authentication and encryption security controls shall be employed to protect data communication over wireless networks with connection to the MDoE's internal network.

Users shall not share authentication keys/passwords with non-employees in order to obtain access to the MDoE wireless network

15.6.6. SOFTWARE INSTALLATIONS

a) Only business related, legal and licensed software is allowed to be installed on any computing devices;
b) Users requiring software to be installed on their computers must log a call at the service desk;
c) Requests for software installation must be approved before it can be installed;
d) The installation of the software shall be installed only by ICT; and
e) Under no circumstances should unlicensed software be installed on any of MDoE's ICT equipment or e-devices.
f) Remote software installation shall be performed under strict and controlled conditions by ICT.

16. INCIDENT MANAGEMENT RESPONSE

In the event of a security incident occurring, it is important that all Departmental employees are aware of their responsibilities and the procedure by which incidents can be most effectively and efficiently brought to a satisfactory conclusion. The procedures as defined below are best practice within Mpumalanga Department of Education.

Where investigation of a security incident indicates misuse of ICT facilities approved disciplinary procedures will be implemented as defined in this policy.

16.1. Incident Reporting

The types of incidents that must be reported include, but are not limited to:

- Incidents reported from Systems and Networks (system failures, unusual activity)
- Incidents that affect Senior Management (threats, gossip, leaks)
- Risk Management (unusual or suspicious behaviour noted in logs or activity reports)
- External sources (threats, customer queries, complaints, press)
- Incidents observed by network users (on local PC's or servers)

- All breaches of MDoE ICT policies.

16.2. Monitoring and Reporting an incident

All observed or suspected security incidents; weaknesses or threats to the network/ICT systems should be reported, immediately, to the ICT Security Officer.

In no instance should any user attempt to prove a suspected weakness as this could lead to a potential misuse of the system. Where users note that any software does not appear to be working correctly, i.e. according to specification, they should report the matter to the ICT Service desk.

Where a user suspects that the malfunction is due to a malicious piece of software e.g. a computer virus, they should stop using the computer immediately, note the symptoms and any messages appearing on the screen and report the matter to the ICT Service desk.

16.3. Documentation

At all stages of the incident handling process adequate documentation must be maintained. Users are required to complete the ICT Incident Reporting Form.

16.4. Disabling Accounts/Network Connections

ICT may disable user accounts and/or network connections:

- Pending investigation of a security incident or where investigation of an incident
- To contain a confirmed security breach and prevent other MDoE network devices from becoming affected by the incident.

16.5. Communication / Control

After validating that an incident has taken place MIT must escalate the incident to the IT Security Officer. The IT Security officer will contact any relevant staff and inform them of the incident. All persons briefed on the issue should be clear as to the sensitivity level and made aware of the consequences of an information leak.

16.6. Obtaining Evidence

It is vital that affected systems should be quickly identified and isolated from the network. Information should be retrieved from these systems in the best available manner, with actions being taken by as few people as possible, preferably only the lead incident contact.

Incorrect gathering and handling of collected evidence may have serious consequences in the successful prosecution of an incident. Collected evidence therefore should be handled correctly so as to preserve integrity and all transfers should be documented and validated. Where possible collected data should immediately be stored on write-once media. Write-once media is defined as any media such as CD that once the data is written to it cannot be edited, amended or appended.

16.7. Preserve Configuration

The configuration and contents of all affected systems must be preserved to the greatest extent possible, so that the issues involved can be demonstrated at a later date. This may be covered by the

method of obtaining evidence but may also involve manual backups of data. This must include all system configuration data as well as any scripts / data / files stored on the system.

16.8. Query External Resources

Where external resources are of use their outputs must always be recorded, preferably on a write-once media. This is particularly important for DNS lookups, whois / rwhois output, etc. which may change at a later stage. If personal contact is made with external agencies, details of all conversations/ correspondence must be recorded in the relevant incident notes.

16.9. Liaison with third parties

If necessary, the ICT Security Officer must notify third-party partners of the incident. The decision to involve law enforcement should only be made by the accounting officer and details of all conversations / correspondence with the relevant law enforcement units should be recorded.

16.10. Follow-up Actions

The immediate appointed incident team should draw up a change report detailing further changes required, including the priority and impact of each change. Approval for follow-up actions may be given by the accounting officer or delegated senior management or via normal change control process. The lead contact is responsible for tracking follow-up changes.

A detailed incident report must be prepared, including remedial action taken in the short and medium term, to help restore confidence in the systems affected.

16.11. Records of Security Incidents

These records will be encrypted and stored securely for six months after which time information pertaining to individuals will be removed. The records will then be held in this anonymous format for a further two years for statistical purposes. The ICT Security Officer will collate and analyze records of security incidents and will report to the ICT Committee any trends which emerge and recommend any additional action which should be taken Department wide to try to prevent their occurrence in the future.

16.12. Misuse of MDoE Facilities

Where investigation of a security incident indicates misuse of ICT facilities approved disciplinary procedures will be implemented as defined in this policy.

16.13. Staff and Third Parties

Where MDoE Staff members or Third parties are found to have misused MDoE ICT facilities the Director MIT or his/her delegated official will inform the appropriate Department authorities who will determine what further action should be taken.

17. EXTERNAL CONSULTANTS

External Consultants appointed by MDoE are allowed to use their own computer equipment, such as laptops on the MIT network, but under strict conditions. Under no circumstances is an external consultant allowed to plug his/ her computer into the network without prior approval by the MIT directorate.

18. PRIVACY

MDoE's management reserves the right to examine all information stored in or transmitted by MDoE in accordance with MIT policies.

19. FAILURE TO COMPLY

Responsibility to take disciplinary action against users not complying with the use of MDoE computer systems as stipulated in this policy lies with the respective Senior Managers. If violations in the use of MDoE computer systems are identified, the MIT directorate will block access to the system for the user in question. All violations will be forwarded to the respective Senior Manager who is expected to take the necessary disciplinary action. Access to MDoE computer systems will only be reinstated once written instruction to that effect is received from the respective Senior Manager.

20. STANDARDS APPLICABLE TO THIS POLICY

PFMA
ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT (Act no. 25 of 2002)
Minimum Information Security Standards (MISS)
Minimum Interoperability Standards (MIOS)
State Information Technology Agency Act
Corporate Governance of ICT Policy Framework
National Intelligent Act (Act No. 39 of 1994)
Copyright Act (Act No. 98 of 1978)
Protection of Information Act (Act No. 84 of 1982)
Protection of Personal Information (POPI) Act No. 4 of 2013
Promotion of Access to Information Act (Act No.2 of 2000)
National Archives and Record Services of SA Act (Act No. 43 of 1996)
LOSS AND DISPOSAL POLICY
NATIONAL EDUCATION INFORMATION POLICY

NETWORK ACCESS

Access to the MDoE network will be granted to users by means of creating a network account. No network account of the new employee will be created without approval from the immediate supervisor.

Procedure:

- Users must Log a call with service desk requesting to create the network account;
- Application for windows and outlook access will be provided by service desk;
- The form must be fully completed and signed by the immediate supervisor and send to service desk.

CONSULTANTS ACCOUNT REQUEST

Procedure to request for approval

- External consultant must log a call with service desk;
- The consultant will be contacted to bring his equipment to MIT for the necessary security and virus checks prior to receiving access;
- Consultants will receive temporary domain accounts on the network to ensure the latest virus patches are updated at all times on such equipment;
- Under no circumstances will any computer user be allowed to be connected to the network without being logged onto the MDoE domain; and
- Consultants should ensure that their desktops/laptops do not harm or broadcast any viruses to the Department's network.

ICT200-003

education
DEPARTMENT: EDUCATION
MPUMALANGA PROVINCE

Sub-Directorate Information Communication Technology

Litiko leTemfundvo Umnyango wePfundo Departement van Onderwys Umnyango wezeMfundo

Request to Create a New User 5.0

In gaining access to the Mpumalanga Department of Education's online services you agree to abide by the Departments Information Communication Technology policies and guidelines available online at:
http://intranet.mpuedu.gov.za/ict/Policies/Forms/AllItems.aspx

Hand the completed form in at the Head Office ICT Office or your nearest District ICT Office

Required User Informations:

Surname:		**Preferred Name:**	
Username:	To be assigned by ICT	**E-mail:**	To be assigned by ICT
Persal No:		**District:**	
Office \ Site:		**Branch:**	
Directorate:		**Sub Directorate:**	
Tel Office:		**Tel Cell:**	
Position (designation):			
Login Expiration (for temporary employee or contractor) (Date):			

List any e-mail groups the employee should be a member of
(each employee is automatically added to the departmental e-mail group):

Applicant requesting:	**Director Approving:**
Print Name & Surname: _____	Print Name & Surname: _____
Signature _____ Date _____	Signature _____ Date _____

Office Use Only:

Request Received:	**Request Processed:**
Print Name & Surname: _____	Print Name & Surname: _____
Signature _____ Date _____	Signature _____ Date _____

ICT200-003 = New_User_Request_5.0.doc

Annexure C: Information Security Incident Form

education
DEPARTMENT: EDUCATION
MPUMALANGA PROVINCE

Sub-Directorate Information Communication Technology

Information Security Incident report 1.0

In gaining access to the Mpumalanga Department of Education's online services you agree to abide by the Department's Informatio Communication Technology policies and guidelines available online at:
http://intranet.mpuedu.gov.za/ict/Policies/Forms/AllItems.aspx

Hand the completed form in at the Head Office ICT Office or your nearest District ICT office

Details of Person Reporting Incident	
Persal number:	
Full name:	
Cell phone:	
E-mail:	
Directorate:	

Details of Incident		
Date of Incident:		
Time of Incident:		
Is incident still in progress?	Yes	No
Do you need assistance from ICT:	Yes	No
Has the incident been reported to the ICT Service Desk?	Yes	No
If yes, provide Service Desk call number:		

Comments

Reported by:		**Request received:**	
Name & Surname		Name & Surname	
Signature	Date	Signature	Date