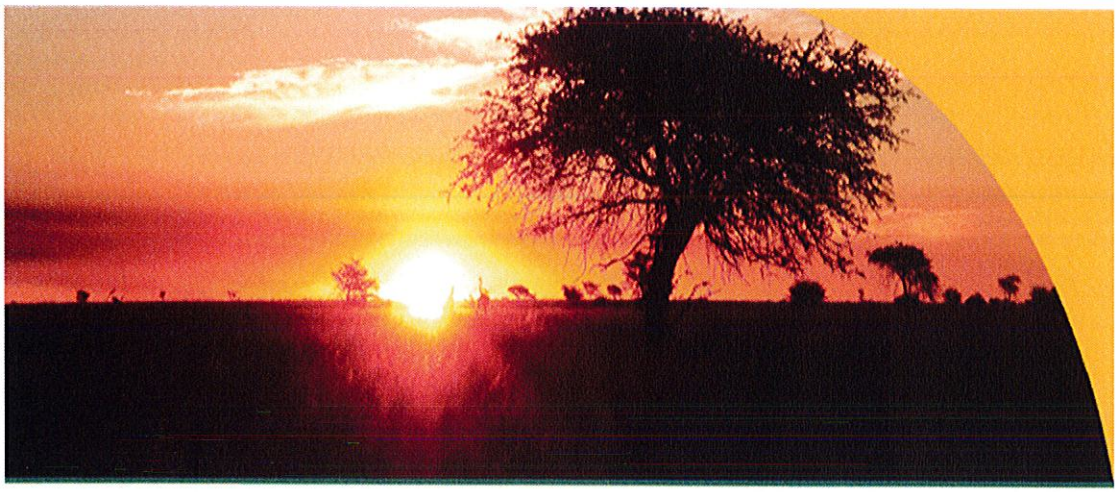

DCSR POLICY: INFORMATION SECURITY POLICY

DOCUMENT INFORMATION AND LOG

FILE NAME	INFORMATION SECURITY POLICY
ORIGINAL AUTHOR	DEPARTMENT OF CULTURE, SPORT AND RECREATION
REVIEW DATE	2019

In the age of the information society information in all its forms has become, more than ever before, the currency of everyday interactions, debate, enlightenment, education, commerce, controversy and concern.

In acquiring this level of importance in society, information has naturally accrued a culture of rights and responsibilities which has in many cases - such as the protection of personal data, and intellectual property and the need for public transparency - been formalised by both legislation and regulatory requirements.

Where information is a concern in the Department, we are expected to ensure that we have proper regard and integrity to it's:

- Confidentiality – to the extent that the nature of the information requires this.
- Integrity - so that confidence can be demonstrated in the information's origin, content, relevance and accuracy.
- Availability - such that appropriate individuals and groups can access, update, read, interpret or monitor the information.

Information security management is the means by which we ensure that we are taking account of these three factors.

The aim of this policy is to ensure that all staff members and all related stakeholders of the Department of Culture, Sport and Recreation understand the importance of Information Security Management as defined above and in the policy as it relates to the information they gather, process and store and the legal and ethical responsibilities that are incumbent on them both as individuals and as members of the Department staff.

With this aim in mind, we commend this policy to you and ask to have proper regard to it in your daily working lives and your daily activities.

Table of Contents

1. ABBREVIATIONS AND ACRONYMS

GCCN	Government Core Communication Network
DCSR	Department of Culture, Sport and Recreation
ITC	Information Technology Committee
IS	Information Systems
ISS	Information System Security
ITB	Information Technology Bureau
LAN	Local Area Network
MISS	Minimum Information Security Standard
SACSA	South African Communication Standard Authority
SITA	State Information Technology Agency
SDLC	Systems Design Life Cycle
WAN	Wide Area Network
RMC	Risk Management Committee
CRO	Chief Risk Officer
COO	Chief Operations Officer

2. DEFINITIONS

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.
Configuration Management	The management of changes made to hardware, software, firmware and documentation of a system throughout the development and operational life cycle of the system.
Department	Means the Department of Culture, Sport and Recreation (DCSR)
End user	Is the person who is using the information technology devices, network and information of the Department.
ICT Operational Committee	The ICT hands on stakeholders that are responsible for implementing the strategies devised by the ICT Steering Committee. It comprises of the GITO as chairperson, ICT technicians, Transversal system controllers and the ICT Internal Audit.
ICT Steering Committee	The ICT strategic committee that is responsible to drive the ICT strategic objectives of the Department. It consists of the chief directors, key players in program one, ISO and the GITO.
Incident	Any event that has actual or potential effect on the information and information systems resulting from fraud, abuse, loss of property, information and any other that may be regarded as such.
Incident Management Team	This is a departmental incident management team that deals with all security incidents and responsible for investigating those incidents

	and report to the Accounting Officer. In this document, it is also referred to as IT Incident Management Team.
Information Security Officer	Is the designated official who is responsible for the monitoring, management and coordinating of IT needs in the Department. Also known as IT Technologist or Data Technologist.
Information system security	To preserve the availability, integrity and confidentiality of information systems and information according to affordable security practices.
Information systems	Applications and systems to support the business while utilising information technology as an enabler or tool.
Information technology	All aspects of technology that are used to manage and support the efficient gathering, processing, storing and dissemination of information as a strategic resource.
IT Assets	All information technology hardware devices and software including their licenses.
IT Manager	This refers to the Security Manager or any delegated IT official, like the Information Security Officer.
ITB	Means the Information Technology Bureau aka Department of Finance (Provincial Treasury)
Local area network	A high-speed communication infrastructure that enables users to share resources such as hardware, software, data or Wide Area Network (WAN) communication in a cost-effective manner.
Monitoring	Performance measurement to ensure the confidentiality, availability and integrity of operational systems and information.
RMC	Risk Management Committee, the committee responsible for the ICT risk assessments and management of Risk registers.
System Owner	A system owner is defined as the person who has the authority and control to provide access rights or otherwise authorises changes to the system, authority to acquire systems. Generally from business administration.
Third party	Any organisation/institution/department, a national department, provincial administration or organisational component listed in schedules 1 and 2 of the Public Service Act, 1994.

3. INTRODUCTION

The purpose of this information technology security system policy is to enable the Department of Culture, Sport and Recreation to apply an effective and consistent level of security to all information and information technology security systems of the department.

The Department of Culture, Sport and Recreation critically depends on information and information systems and seeks to protect its information and information technology security systems from loss, misuse and damage.

- The objectives of the policy is to ensure, as far as reasonably possible, that: -
- The assets of the department are secured against loss by theft, fraud, malicious or accidental damage, or breach of privacy or confidence, and any matter related to it.
- The department is protected from damage or liability resulting from use of its facilities for purposes contrary to any law of South Africa.

This policy applies to employees, contractors, consultants, temporaries (that's includes internship and learner ship) and other workers at the department of Culture, Sport and Recreation, including all personnel that are affiliated with third parties. This policy applies to all computers and network systems that is owned or leased by the department.

Non-compliance to this policy shall be considered as misconduct and depending on the circumstances and seriousness of the offence, disciplinary action shall take place, which may include dismissal.
The framework, in which the department of Culture, Sport and Recreation of information technology system security policy is discussed, is set out under the following headings:

- A Security policy that identifies the motivation for security, describes information security principles and terms, defines the scope of information security and lists the titles/responsibilities of the various role players in the department.
- A Security Policy
- Specific Security Policies and procedures

4. INFORMATION TECHNOLOGY SECURITY CHARTER

4.1. Scope

The Information Security Charter sets the tone and presents the philosophy of information security within the department of Culture, Sport and Recreation. The purpose of the Information Security Charter is to:

- Identify the business need for security.
- Define the scope of the security policy.
- List the titles/responsibilities of the various security functions.
- Define the scope of contingency and disaster recovery.
- Specify legal, regulatory, or audit requirements that must be met.

4.2. Principles

The principles of the policy provide the ethical and moral essence and fundamental basis on which the department's good business practice, policies and planned action are based.

4.2.1. Proportional Cost vs. benefit:

All security measures should be appropriate and proportional to the cost and benefit of implementing such measures for which they are designed to protect.

4.2.2. Adversary:

All security measures should be established in the anticipation of natural disaster, harmful intent and hostile attack.

4.2.3. Least Privilege:

Access to any IT system will be granted on the basis of business need to access the facility. In other words, the need-to-know basis.

4.2.4. Segregation of duties:

Job functions must be divided amongst co-workers. System users should be given access to perform a single duty on the system. For example no person may have access to both add employees to the Human Resources System and authorise payment for these people. N/o one person may have access to place an order and pay a supplier.

4.2.5. **Ethics:**

In the implementation of this policy, the Department adheres to an ethical code of conduct in relation to monitoring and accessing of user accounts. An ethical judgement in this regard may need to be made.

4.2.6. **Timeliness:**

Employees and Third Party/s will act or respond within a reasonable time period to any identified risk or security breach.

4.2.7. **Confidentiality:**

Unauthorised disclosure of information is prohibited.

4.2.8. **Integrity**:

Unauthorised modification of information is highly prohibited.

4.2.9. **Availability:**

Refers to both Data and Service. Data and information systems must be accessible when required.

4.2.10. **Controlled Access:**

Information assets shall only be used for business purposes and for the business purpose intended. Policies will be defined in accordance to business processes to control access to information resources.

4.2.11. Levels of Protection/Assurance of protection:

In accordance with MISS, the following levels of classification will determine the levels of protection –

- Restricted
- Confidential
- Secret
- Top Secret

4.2.12. Protected measures baseline:

The department and its information is an important asset that shall be protected at all cost, and according to its value and degree of damage that could result from its misuse, unavailability, destruction, unauthorised disclosure or modification. This implies that information is identified as the most important assets shall be identified, valued, assessed for risk and protected cost effectively from identified threats in accordance with the principle of Cost Vs Benefit.

4.2.13. Continuity of Protection:

The department's information is an important asset that shall be protected on a 24/7/365 basis.

4.2.14. System stability

The department's information is an important asset that shall be available as and when required. This entails a 24/7 availability unless otherwise stipulated.

4.2.15. Survivability:

The department's information is an important asset that shall have the ability to be sustained in the event of a disaster. Disaster Recovery Plans will established and structured walk-through testing will be done. Implementation of the plans will be managed on a project-to-project basis.

4.2.16. Individual Accountability:

Every individual is accountable for the security of the Departmental IT assets under their control. The delegation of responsibility for security is assigned to each and every official within the department. Mechanisms such as User ID's are in place to ensure individual accountability.

4.3. Information Classification

The following table provides a summary of the information classification levels that have been adopted by the IOE and which underpin the 8 principles of information security defined in this policy. Detailed information on defining information classification levels and providing appropriate levels of security and access is provided in the Data Security Policy.

Security Level	Definition	Examples
Confidential	Normally accessible only to specified members of DCSR staff	Sensitive personal data; salary information; bank details; draft research reports; passwords Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.
Secret	Sensitive information that can cause harm to the Department when accessed by malicious/opposite/hostile elements.	Internal correspondence, final working group papers and minutes, committee papers, information held under license Subject to scrutiny in relation to appropriate exemptions/ public interest and legal considerations
Top secret	Highly sensitive information that can be used to neutralise the functions and objectives of the Department when accessed by malicious/ opposite/ hostile elements.	Internal and external documents related to political influence. High profile contract documents with service providers.

4.4. Accountability and Responsibilities

4.4.1. Accounting Officer

The Head of Department is accountable for information system security and must therefore ensure adherence to this and any other security policies within his/her respective areas of responsibility.

4.4.2. Chief Operations Officer (COO)

The Chief Operations Officer in his/her capacity as the appointed ICT Governance Champion is responsible and accountable for the implementation and enforcement of this policy as well as secure operations and management of the departmental information systems. He/she must also ensure that ownership and security responsibilities for all systems are defined.

4.4.3. Managers

Managers are responsible and accountable for information system security on systems falling directly under their control and must therefore ensure adherence to this and any other security policies within their area of responsibility.

4.4.4. System owners

System owners are responsible for ensuring that appropriate security controls are embedded in their information systems a tat appropriate processes are put in place to ensure integrity and security of data. The overall security and data integrity of a system lies with the defined systems owner.

4.4.5. ICT Steering Committee

The ICT Steering Committee should ensure compliance of the Information Security Controls with the approved standards/best practices. The Committee is also responsible to ensure the proper review is made periodically of this policy.

4.4.6. Risk Management

Risk Management should ensure that weaknesses observed by the audit process are made available to discuss with stakeholders to mitigate identified risks. Risk Management should also ensure that IT Risk Register is maintained to mitigate risk associated with information security processes.

4.4.7. Information Technology Bureau (ITB)

The ITB should provide technical services and ensure that all systems are maintained and regularly serviced to ensure security breaches are averted. They should also advice in regard to the implementation of technical security controls.

4.4.8. Security Management

Security management should ensure that all IT security related incidents should be reported to the Accounting Officer.
All security incidents handled by the IT and security section should be recorded and reported to the Accounting Officer and Chief Risk Officer on quarterly basis.

4.4.9. ICT Operational Committee

This committee should be chaired by the GITO and responsible of implementing resolutions from ICT Steering Committee, provide input into the development of ICT Plan, ICT Implementation Plan, ICT Operational Plan, Governance of ICT Framework and ICT Project Program, and manage day-to-day operations and services.

4.4.10. Information Security Officer

The Information Security Officer shall implement information security systems and processes.
The Information Security Officer shall also implement specific policies for incidents response following natural disasters and also keep a consolidated record of all security incidents relating to IT security.

4.4.11. Individual Accountability

Any person who uses the department information systems shall be responsible and accountable to follow recommended procedures and to take all reasonable steps to safeguard the information handled by that system and any sensitive assets involved. All information systems involving financial transaction and all information systems acquired or upgraded by June 2004 shall provide a means, which can hold individually accountable for their actions.

5. GENERIC SECURITY POLICY

5.1. Security Management

5.1.1. Information security shall be coordinated and supported at TOP MANAGEMENT level in the department. It is the responsibility of management to support and ensure that the necessary ISS endeavours and initiatives are coordinated and enjoys the necessary privileges.

5.1.2. An IT Security and Risk Management Committee responsible for all IT security related issues should be put in place. This shall be composed of representatives from the IT section, Risk Management Unit, Security Manager and Internal Audit Representatives from the Business Units can be co-opted as and when required.

5.1.3. The following IT security management aspects shall be addressed by the Security Committee:

- Manage the department's IT security program
- Examples: IT security awareness, BCP, DRP and IT risk assessments.
-

5.2. Personnel Security

5.2.1. The employees of the department accessing information systems and those who are processing financial transactions, should meet the necessary security requirements as determined by the sensitivity of information accessed.

5.2.2. Access to the systems and data may be immediately terminated as soon as evidence of non-compliance with the security requirements is obtained.

5.2.3. Information security roles and responsibilities shall be included in approved job descriptions where required.

5.2.4. All employees who use IT services are required to acknowledge acceptance of and intention to comply with the Acceptable Use policy by signing the Department's INFORMATION TECHNOLOGY USER DECLARATION AGREEMENT. Any employee found to have violated this policy could be subjected to disciplinary action.

5.2.5. All third-party organisations are required to sign a non-disclosure agreement (NDA) before access to any IT resource (s) is/are permitted. Any party found to have violated this agreement could be subjected to a termination of his/her contractual agreement with the Department.

5.3. Physical and Environmental Security

5.3.1. The MISS applies. Mpumalanga Government Protection Services shall be consulted for additional regulations. All security areas/buildings where computer related equipment is used shall be classified according to its criticality in terms of risk and be protected to conform to the applicable standard of security.

5.3.2. Where feasible access to the server and patch rooms shall be strictly controlled and restricted to authorized personnel. Authentication controls like swipe cards or PIN shall be used to authenticate and validate access. An audit trail shall be securely maintained.

5.3.3. Where feasible fire prevention standards and procedures shall be established and adhered to in order to prevent fire from starting spontaneously due to negligence or as a result of arson. Firefighting equipment, sensitive to electronic environments and thermal shock on magnetic media, shall be deployed in high-risk areas. Fire detecting sensors (heat and smoke) shall be linked to an alarm system and shall be regularly tested.

5.3.4. Firefighting and evacuation procedures shall be adhered to and personnel shall be trained in the effective execution of these procedures. Regular simulations shall be conducted.

5.3.5. An access control system and procedures shall be implemented to control the access to systems on a twenty-four-hour basis.

5.4. Risk Management

5.4.1. Risk management is responsible for ensuring that IT risks identified by audit are mitigated to avoid any future information security risks.

5.4.2. Risk management is also responsible for ensuring that audits and reviews are conducted on a regular basis to:

- Ensure integrity, confidentiality and availability of information and resources (s),
- Investigate possible IT security incidents to ensure conformance to the Department's security policies,
- Monitor user and system activity where appropriate.

5.4.3. Users, system owners and identified participants shall cooperate with the audit team to accomplish the desired goal.

5.4.4. The audit findings and recommendations shall be prioritised and responsibilities for implementation shall be assigned.

6. SPECIFIC SECURITY POLICY

6.1. Acceptable Use

6.1.1. General Use and Ownership

6.1.1.1. The Department respects the individual privacy of employees. However, employee privacy does not extend to the employee's work related conduct or to the use of Government provided equipment, resources or supplies.

6.1.1.2. In general, the Department's computer and communication systems are intended for business purposes only. Incidental personal use is nonetheless permissible if the use does not consume more than a trivial amount of resources that could otherwise be used for business purposes, does not interfere with worker productivity, does not pre-empt any business activity, and does not cause distress, legal problems, or morale problems for other workers. Permissible incidental use of a personal computer would, for example, involve responding to an electronic mail message about a luncheon, electronic banking through the Internet, obtaining study material from a bona fide educational institution that the employee is registered with or intends registering with, news updates of major events.

6.1.1.3. Offensive material that might cast the Department in a bad light, including sexist, racist, violent, or other content, is strictly forbidden from all Departmental personal computers, email and servers.

6.1.1.4. Without specific written exceptions, all program data and documentation that are developed by employees, consultants or contractors, for the benefit of the DCSR, will be provided to the Department. Responsible management shall ensure that all workers providing such programs or documentation sign a statement allowing the department to change the program data, as and when required.

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

6.1.1.6. All equipment connected to the network, shall run the current approved anti-virus scanning software.

6.1.1.7. The department reserves the right to audit networks and systems on aperiodic basis to ensure compliance with this policy.

6.1.1.8. For security and network maintenance purposes, authorized individuals within the department may monitor equipment, systems and network traffic at any time.

6.1.1.9. All work related files must be backed up onto a departmental server for Disaster Recovery purposes. In the event that an employee is absent and his files need to be accessed to continue business operations, an administrator may access the files upon receipt of an authorised change control form.

6.1.2. Security and Proprietary Information

6.1.2.1. Each employee shall be granted access to information as is needed to perform his or her assigned function, but employees shall not be given access to information otherwise requiring protection unless and until such access is needed and formally authorised.

6.1.2.2. Authorized users are responsible for the security of their password and accounts.

6.1.2.3. All external communication regarding the department security and proprietary information must go through the Directorate of Communications, Legal and Security Management.

6.2. Unacceptable Use

6.2.1. System and Network Activities

6.2.1.1. Under no circumstances may an employee of the department be authorized to engage in any activity that is illegal under local, provincial or international law while utilizing IT resources owned by the department.

6.2.1.2. Violations of the rights of any person or company 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 department.

6.2.1.3. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan Horses, e-mail bombs, etc.).

6.2.1.4. Effecting IT 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 authorized to access, unless these duties are within the scope of regular duties. "Disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

6.2.1.5. Executing any form of network monitoring which shall intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

6.2.1.6. Revealing your account password to others or allowing use of your account by others. This includes and other household members when work is being done at home.

6.2.1.7. Circumventing user authentication or security of any host, network or account.

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

6.2.1.9. Port scanning or security scanning is expressly prohibited unless prior notification to IT is made.

6.2.1.10. Using any program/script/command, or sending messages of any kind, with intent to interfere with or disable, a user's terminal session, by any means, locally or via Internet/Intranet/ Extranet.

6.2.1.11. Engage in any activity for personal gain or personal business transactions.

6.2.1.12. Downloading of material off the internet that is not related to business.

6.2.1.13. Conduct any activity without the written consent or authorisation of the Accounting Officer

6.2.2. Email/Internet and Communication Activities

6.2.2.1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material.

6.2.2.2. Any form of harassment through email, telephone or paging, whether through language, frequency or size of messages.

6.2.2.3. Unauthorized use, or forging, of email header information.

6.2.2.4. Use of unsolicited email originating from within DCSR's network of other Internet/Intranet service provider on behalf of any service hosted by DCSR or connected through DCSR's network.

6.2.2.5. Posting the same or similar non-business-related messages to large numbers of DCSR employees or Usenet newsgroups (newsgroup spam). Use of chain email messages.

6.2.2.6. Interception of data, spoofing, masquerading, line tapping and or Denial of Service attacks is unacceptable.

6.2.2.7. Attempts to subvert network security, to impair functionality of the network, or to bypass restrictions set by the network administrators. Assisting others in violating these rules by sharing information or passwords is also unacceptable behaviour.

6.2.3. Software usage

6.2.3.1. Under no circumstances shall unlicensed software, privately owned software, games, public domain software, and freeware, shareware or demonstration software be loaded on official computer equipment without prior written consent from the IT Manager.

6.2.3.2. A written request for loading of such software must be submitted to the IT Manager, stating the reasons for the loading of the software and the duration that it shall be required.

6.2.3.3. The IT Manager reserves the right to authorize removal of any such unlicensed software without prior notification to the user.

6.3. Internet Policy

6.3.1. Access to the Internet shall be granted to employees that have a legitimate need for such access, the user needs to apply for access formally through the respective Accounting Officer must approve the request.

6.3.2. All internet connections shall be via the approved Internet service provider of the Department. Any other connections are prohibited.

6.3.3. Use of Internet is a privilege, which constitutes the acceptance of responsibilities, and obligations that are subject to government policies and laws. Acceptable use must be legal, ethical, and respectful of intellectual property, ownership of data, systems security mechanism and individual rights to privacy from intimidation, harassment and annoyance.

6.3.4. All users, connected via the DCSR computer network, shall authenticate themselves at ITB proxy server before gaining access to the Internet. This authentication process shall be achieved by logging on to the Internet via user name and password system.

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

6.3.6. Users shall not publicly disclose internal DCSR and ITB information via the Internet, which could be adversely affect DCSR and ITB, customer relations or public image.

6.3.7. The ITB content filtering software shall prevent users from connecting to certain non-business web sites. All websites that contain sexually explicit content, profane and other potentially offensive material shall be blocked out via the proxy server.

6.3.8. Users shall be subject to limitations on their use of the Internet as determined by the appropriate supervising authority.

6.3.9. At any time and without prior notice, the Department management reserves the right to examine all web browsers' cache files, web browsers' bookmarks and other information that is stored on or passing through the computers of the Department. Such management access assures compliance with internal policies, assists with internal investigation and assists with the management of the Department.

6.4. Electronic Mail

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

6.4.2. The Department's electronic communications systems generally shall be used only for business activities. Employees are reminded that the use corporate resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.

6.4.3. 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 shall reflect the actual originator of the messages or postings.

6.4.4. The department's management shall regularly monitor the content of electronic communications. Content and usage of electronic communications shall be monitored to support operational, maintenance, auditing, security and investigative activities.

6.4.5. Recognizing 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. The Department's sensitive information shall not be forwarded to any party outside DCSR without prior approval of the Accounting Officer.

6.4.6. Users must be aware of the classification of any information contained in data files or correspondence which they are transporting using email communication and do not exchange information in un-encrypted form which is confidential.

6.4.7. The Department shall occasionally monitor the content of electronic communications and any suspicious malicious acts detected or found, necessary disciplinary action will be taken.

6.5. IT Access Control

6.5.1. Access by Internal Staff

6.5.1.1. The designated owner of the information asset shall take responsibility for all access granted. The owner of the information resource shall ensure that all access to the resource granted is appropriate and justified.

6.5.1.2. All of department information systems privileges shall be promptly terminated at the time when an employee, consultant or contractor or any other temporary worker ceases to provide services to the department. All data in the possession of the person terminating service must be backed up by the person and handed to the IT Manager who will sign a Gate Release Voucher.

6.5.1.3. The management of the department reserves the right to revoke the privileges of any user at any time.

6.5.1.4. Any conduct that interferes with the normal and proper operation of the Department's information systems, which adversely affects the ability of others to use these information systems, or which is harmful or offensive to others shall not be permitted.

6.5.1.5. The use of generic user accounts is not permitted on any system that handles any financial transaction or confidential personal details. Read-only generic access accounts are only permitted on systems as a means of reducing cost of ownership or where an express need is required for shared access.

6.5.2. Third Party Access

6.5.2.1. Third party organizations shall be given access privileges to the IT resources after the department's management has determined that they have legitimate business need. These privileges shall be enabled only for the time period required to accomplish approved tasks.

6.5.2.2. Any third party organization given access to the IT resources of the department, shall have signed a non-disclosure agreement to protect the confidentially of systems, information they access.

6.5.2.3. Third party access shall be monitored and reviewed on regular basis by the relevant section.

6.5.2.4. Third Party Organization shall provide any information reasonably necessary for the department to evaluate security issues relating to any authorized Third Party's employee.

6.5.2.5. The Third Party organization shall notify the department in writing promptly upon a change in the user base for the Network connection or whenever the department is of the opinion that a change in the connection and/or functional requirements of the Network connection is necessary.

6.5.3. Visitors Access

6.5.3.1. No visitors shall be allowed access to any of the information electronically of the department unless a written approval from Accounting Officer or delegated authority is obtained. The hosting party/person shall be responsible for ensuring that required approval is obtained before any access is granted.

6.5.3.2. Visitors shall not be allowed any access into the server and/or patch rooms unless accompanied by the hosting personnel and monitored by personnel responsible for the server or patch room. Reasons for access shall be justified by line management and approved by the ISO or officially delegated personnel regarding Head Office and the Regional Manager regarding the Regions.

6.5.4. Physical Access

6.5.4.1. Where feasible physical access to the computer room where servers and other IT equipment are stored shall be protected by an access control system. The system shall be implemented with the necessary control measures.

6.5.4.2. Physical access to IT resources shall be granted in accordance with a formally defined procedure. Only authorized personnel shall have physical access to IT equipment. Line management shall be responsible for approving and allocating access to resources.

6.6. Network Security

6.6.1. The SITA GCCN (Government Common Core Network) security Policy shall apply for the WAN connections to the Department's Head Office and Regional sites to ensure the safeguarding of information in networks and the protection of the supporting infrastructure.

6.6.2. A LAN administrator shall be appointed and shall be responsible for the design and configuration management of the LAN and maintenance of the existing LAN. Currently managed by ITB.

6.6.3. The utilization of the Administrator privileges shall be strictly limited and controlled by the LAN Administrator. Defaults accounts (guest, supervisor or administrator) shall be disabled.

6.6.4. The connection of unauthorized equipment to the Department's LAN is prohibited. Authorization must be obtained from the IT Manager.

6.7. Server Security

6.7.1. Where feasible all servers hosting data and applications shall be located in a physically secure environment where access is strictly controlled. All server or patch rooms shall be regarded as high-risk security areas and access to these areas shall be strictly controlled.

6.7.2. Logical access to servers shall be allocated on a need-to-know basis, in accordance with the access control policy of the Department.

6.7.3. All servers shall be loaded and protected with the latest approved Anti-Virus software. Updates for patches and upgrades shall be implemented regularly when required.

6.7.4. Only an authorised administrator shall be granted administrative rights to the servers. Administrative password shall be kept a secret and only nominated personnel at Management's discretion shall have access to the password.

6.7.5. Servers shall be backed up in accordance with the Department's backup policy and procedures.

6.8. Workstation Security

6.8.1. All workstations shall be located in a physically protected environment where access control measures are in place and applied consistently. It shall be ensured that unattended equipment has appropriate security protection.

6.8.2. Classified data shall not be stored on the local drive of workstations. All classified data processed using workstations shall be saved on a secured network drive on a server.

6.8.3. All workstations shall be loaded and protected by the latest approved Anti-Virus software.

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

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

6.8.6. Workstations used to access classified, secrete or top secret, information must at least be protected by two-factor authentication. For example, encryption, smart cards or tokens.

6.8.7. Users shall not share workstation passwords and user accounts with anyone, even if they are on leave.

6.8.8. 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.

6.8.9. Users must ensure that all systems and data are properly backed-up and that local and network drives are synchronised.

6.9. Data Media Handling and Security

6.9.1. Information classified as confidential, secret and top secret shall not be stored on unsecured media, like local drives of workstations, floppy disks, removable disks, mobile hard drives, CD's and email systems.

6.9.2. If needed encryption technologies shall be used to encrypt classified data stored on the network, email, and any electronic media.

6.9.3. Access to data media or facilities housing data media shall be controlled.

6.9.4. Data media shall be archived or disposed of according to system design specifications and the State Archiving policy and procedure.

6.10. Disaster Recovery & Backup

6.10.1. The Department shall have a documented Disaster Recovery Plan, which is approved and endorsed by Senior Management of the Department.

6.10.2. Disaster Recovery Plan shall be tested, evaluated and continually updated.

6.10.3. The DRP shall be communicated to all parties responsible for the management and operations of the IT infrastructure.

6.10.4. The Disaster Recovery Plan shall at least be classified confidential.

6.10.5. Data back-up procedures shall be established and adhered to for all the information systems and operations.

6.10.6. Data backup devices shall be kept in a safe offsite environment where they can be accessible with ease when needed.

6.11. Password Policy

6.11.1. **Difficult-to-Guess Passwords Required**

All user-chosen passwords for computers and networks shall be difficult to guess. Words in a dictionary, derivatives of user-IDs, and common character sequences such as "123456" shall not be accepted as passwords. Likewise, personal details such as spouse's name, license plate, social security number, and birthday shall not be used unless accompanied by additional unrelated characters. User-chosen passwords shall also not be any part of speech. For example, proper names, geographical locations, common acronyms, and slang shall not be employed.

6.11.2. **Display and Printing of Passwords**

The display and printing of passwords shall be masked, suppressed, or otherwise obscured so that unauthorized parties shall not be able to observe or subsequently to recover them.

6.11.3. **Periodic Forced Password Changes**

All users shall be automatically forced to change their passwords at least once every thirty- (30) days.

6.11.4. Assignment of expired passwords

The initial passwords issued by a security administrator shall be valid only for the involved user's first online session. At that time, the user shall be forced to choose another password before any other work can be done.

6.11.5. Account Lockout

A user's account shall be locked out after three unsuccessful logon attempts and only the system administrator can unlock user accounts.

6.11.6. Privileged user accounts – Administrator passwords, operating systems, systems administration.

6.11.6.1. Privileged user accounts may only be given to staff that have attended an approved systems administrator course.

6.11.6.2. Administrators may not use the administrator accounts while performing day-to-day work and may only use them for bona fide systems administration tasks.

6.11.6.3. Administrator user name may not remain as default.

6.11.6.4. Administrator passwords must be kept in a sealed envelope and locked out in a fireproof safe.

6.11.6.5. Administrator passwords must be known to at least 2 trusted people.

6.12. Authentication authorization

6.12.1. Any request for IS resource access shall be accompanied by an authorization letter from immediate management.

6.12.2. Users shall have a unique user name and passwords to identify them on the systems relating to financial transactions and to all systems acquired or upgraded after June 2004. All user names and passwords shall conform to the naming convention of the department and password standards approved.

6.12.3. Authentication to IS resources shall be logged and reviewed at all system levels. The level of security required at that level of access would determine the strength of the authentication method used.

6.12.4. Authentication scheme used or to be used shall be reviewed based on the security requirements of the resources being accessed. The security requirements of the resources access shall dictate the appropriate authentication scheme to be used.

6.13. Operation Security

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

6.13.2. In order to prevent fraud, sabotage, espionage, subversion and actions endangering security, effective configuration management shall be applied to systems in operation. Configuration items of systems shall be uniquely identified and controlled in order to determine and control the influence of a change to a configuration item on the systems and interfaces.

6.13.3. Configuration management shall ensure that any additions, omissions or changes made to systems are authorized and do not compromise the set security measures.

6.13.4. Complete, updated manuals or documentation shall be available to operators, programmers, users and auditors as applicable copies shall be made of all electronic documentation and be stored in a geographically separate location in a safe.

6.13.5. The use of system utility programs (e.g. monitoring/sniffing tools/debugging tools) that might be capable of overriding system and application controls shall be restricted and tightly controlled.

6.13.6. System Owners are to ensure that a backup of the latest two configuration sets is kept, and to ensure that a paper copy of such configurations is kept.

6.13.7. System owners are to ensure that copies of all the software and license agreements approved by the Department are centrally housed in a fire proof safe with the IT section.

6.13.8. System owners are to ensure that accurate records of all users given access to systems are documented.

6.13.9. Access lists of users to systems needs to be verified by Human Resources on a bi-annual basis.

6.13.10. All users' accounts that have been inactive for three months mist be de-activated.

6.14. Document Security Policy

6.14.1. All electronic documents shall be classified in accordance with the MISS classification system. It is the responsibility of the person accessing or using the document to understand the sensitivity of the material contained in it.

6.14.2. Access to highly classified electronic documents shall be strongly controlled. Authorization from appropriate owner shall be obtained. It is the owner's responsibility to ensure that all access requirements to the documentation are satisfied as outlined by the classification requirements and security status of the recipient.

6.14.3. Documents and sensitive data files shall be kept in a safe environment. A backup procedure for all manuals, files and documents critical to the department business shall be put in place to ensure the availability of information in manual file system.

6.14.4. Sensitive documents shall not be printed on network printers accessible to everyone.

6.14.5. Requests for access to highly classified documents shall be scrutinized and logged if granted. All sensitive documents accessed shall be accompanied by a business motivation and authorization.

6.14.6. Systems and network documentation shall be classified as secret. Access to this documentation shall be strictly controlled and only people authorised to view, change or modify the system configurations shall be allowed access to the documentation. Example, administrator passwords, IP addresses, computer name and usernames.

6.14.7. Common directories: No sensitive documents must be stored in public directories, as these directories are made available to all users.

6.14.8. Common directories: Each common directory must have a designated owner who is responsible for the regular cleaning out of redundant data.

6.15. Remote Access & Dial In

6.15.1. Secure remote access shall be strictly controlled. Control shall be enforced via one-time password authentication or public/private keys with strong pass-phrases.

6.15.2. The Department employees and contractors with remote access privileges shall ensure that the Department-owned or personal computer and workstation, which is remotely connected to the Department's network, is not connected to any other network at the same time.

6.15.3. The department's employees and contractors with remote access privileges to the Department's corporate network shall not use Private email accounts (i.e. Hotmail, Yahoo, AOL), or other external resources to conduct official business, thereby ensuring that official business is never confused with personal business.

6.15.4. All hosts that are connected to the Department's internal networks via remote access technologies shall use the most up-to-date anti-virus software and this includes personal computer.

6.15.5. Personal equipment that is used to connect to the Department's networks shall meet the requirements of DCSR – owned equipment for remote access.

6.15.6. Organizations or individuals who wish to implement non-standard remote access solutions to the Department's production network shall obtain prior written approval from the IT Manager.

6.16. Third Party Connections Security

6.16.1. A Third Party Company shall apply in writing to the Head of Department which will be referred to Department of Finance's IT manager for access to Mpumalanga Provincial Government Network.

6.16.2. The Third party organisation shall notify the department promptly in writing upon a change in the user base for the work performed over the network Connection or whatever in Company's opinion a change in the connection and/or functional requirements of the network connection is necessary

6.17. IT Change Management Policy

6.17.1. Change Requests and Approval

6.17.1.1. A formal change management process shall be established including approval of change requests.

6.17.1.2. All changes shall be done in accordance with an approved change management process of the department

6.17.2. Implementation and Testing

6.17.2.1. All approved changes shall be monitored to ensure that they are implemented according to specification.

6.17.2.2. The effects of changes shall be analysed shall be analysed before changes are approved and implemented.

6.17.2.3. It is responsibility of management to ensure that all approved changes to critical IT resources are at a minimal level of risk to the IT infrastructure.

6.17.3. Documentation

6.17.3.1. Documentation reflecting all significant changes to production computer and communications systems in the department shall be prepared within a week from the time that a change took place. This documentation shall reflect the proposed change, management approval, and the way in which the change was performed.

6.17.3.2. Documentation shall be classified as confidential. Only authorized personnel shall have access to the documentation.

6.18. IT Acquisitions

6.18.1. Security and Interoperability standards as laid out in the MISS and Interoperability Standards are to be adhered to.

6.18.2. All new acquisitions to be made in accordance with relevant regulations.

6.18.3. The security manager in consultation with IT Manager in the department of Finance shall be informed of all system acquisition initiatives.

6.18.4. All new IT equipment should be accompanied by specifications approved by the IT Manager to meet the Department network standards.

6.19. Inventory and Assets Management

6.19.1. As it is critical for Disaster Recovery and Business Continuity inventory of all IT resources shall be kept by means of an asset register.

6.19.2. Items in the asset register shall be uniquely identified by means of an asset number/tag number allocated by the asset management section in the Department.

6.19.3. The asset registry shall be updated when new hardware/software is procured or written off. It is the responsibility of the Information Security Officer to ensure that all newly procured items are included in the IT Asset Register.

6.19.4. Removal control shall be executed by means of an approved Gate Release Voucher/Form. The Security Management will be responsible to provide permission or approval of all assets leaving the departmental premises. Security Management will provide permanent, temporary and daily removal permits.

6.19.5. Standards and procedure for the disposal of IT Hardware, Software, Data and all data media devices shall be established to ensure that the department is not compromised in the disposal process.

6.19.6. The IT Manager, Regional Office Managers shall coordinate disposal actions in respect of hardware and software within their own environment according to Provisioning Administration Standards.

6.20. System Development

6.20.1. All systems developed for the Department shall be developed in accordance with a formally defined SDLC.

6.20.2. Security requirements of development shall be determined and the risks identified before a system is developed.

6.20.3. Prior to live deployment of a system, the IT Manager in conjunction with ITB and SITA shall review the security requirements and approve that the required security mechanism have been implemented.

6.20.4. The departmental IT Manager shall be informed of all system development.

6.21. Encryption

6.21.1. All external communication over the DCSR WAN and/or DCSR LAN to LAN communication over the WAN classified confidential, secrete or top secrete shall be encrypted with approved SACSA cryptographic devices before transmission.

6.21.2. When making use of Public Key Infrastructure (PKI), all sessions keys shall be transmitted in encrypted format.

6.21.3. When encryption is not used for the external transmission of classified information, it shall be reported as a breach of security to the IT Security section.

6.21.4. If the department's data is classified secrete or top secret, that need to be transported in computer-readable storage media (such as magnetic tapes, floppy-disks, mobile hard drives, laptops, USB flash drives, SD cards or CD/DVD Discs), they shall be in encrypted form.

6.22. Incident Management (Handling)

6.22.1. An Incident Management Team shall be established with the following tasks and responsibilities:

- Receive notification of incidents
- Investigate incidents and analyse the cause of the incident with a view to formulate corrective measures that such an incident does not reoccur
- Draft a report providing detail of the incident and accompanying evidence.
- Report to the affected Departmental Responsibility Manager.

6.22.2. All incidents affecting information systems and information shall be escalated to the IT Manager.

6.22.3. All incidents affecting physical security shall be escalated to the Security Manager.

6.22.4. The Incident response procedure shall be adhered to. This procedure covers the following types of security incidents:

6.22.5. All users of IS services shall be made aware of the procedure of reporting security incidents and be required to report any observed or suspected action/ security weakness in, or threats to, systems or services. All deliberate or non-deliberated breaches of security shall be investigated and reported.

6.22.6. The incident management team shall draft a report providing the details of the security breach and all accompanying evidence/documentation, and forward this to the Accounting Officer, who is required to submit regular incident reports to the NIA and Auditor-General of South Africa (AGSA) of all instances of non-compliance with the MISS, in which the threat posed by the incident is indicated. If sabotage, espionage or subversion is suspected, the ISO must report all instances of security breaches to the Chief Director: security at National Intelligence Agency (NIA), the South African Police Service (SAPS), the South African National Defence Force (SANDF) and Military Intelligence (MI).

6.23. Firewall

6.23.1. Information Technology Management must tightly control the physical access to the firewalls, allowing only the firewall administrators and network services manager physical access to the servers.

6.23.2. The Firewall Administrator is responsible for Firewall configuration tables to determine what is permitted in or denied.

6.23.3. Rules shall be established as to which incoming and outgoing services shall be denied or allowed for various client/servers (e-mail, ftp, telnet, www, etc.).

6.23.4. Standards must be established to stipulate which service utilized\s specific port numbers. All services and connections through the firewall shall be denied unless specifically permitted by the Network Administrator.

6.23.5. The firewall must log all reports on daily, weekly and monthly basis to allow the analysis of the network activity through the firewall.

6.23.6. Firewall administrators must audit the firewall logs in a timely manner (daily, if possible) to detect any possible attacks from the Internet.

6.23.7. Threat and vulnerability analysis shall be performed continuously (3 months).

7. REFERENCE POLICIES

The policy is to be read in context of the legislation and standards as listed below.

7.1. Minimum Information Security Standards (MISS)

7.2. State Information Technology Agency Act, 1998 (Act no. 88 of 1998)

7.3. SACSA/090/1(4) "Communication Security in the RSA"

7.4. Protection of Information Act, 1982 (Act no. 84 of 1982)

7.5. Mpumalanga ICT Governance Policy Framework (CGICTF of 2013)

7.6. Information Act, 2002 (Act no. 70 of 2002)

7.7. Promotion of Access to Information Act, 2000 (Act no. 2 of 2000)

7.8. Electronic Communication and Transaction Act, 2002 (Act no. 25 of 2002)

7.9. National Intelligent Act, 1994 (Act no. 39 of 1994)

7.10. Copyright Act, 1978 (Act no. 98 of 1978)

7.11. National Strategic Intelligence Act, 1994 (Act no. 39 of 1994)

7.12. National Archives of SA Act, 1996 (Act no. 43 of 1996)

7.13. Public Service Act, 1994 (Act no. 103 of 1994)

7.14. State procurement policy

7.15. State archiving policy and procedure

7.16. DCSR Contingency plan

8. ASSOCIATED DOCUMENTS

8.1. Non-Disclosure Agreement to be signed by third party working for DCSR

8.2. DCSR Information Technology User Declaration Agreement to be signed by all users within DCSR

8.3. Email disclaimer that is required to be placed as signature to all email messages outgoing from the users in the department.

8.4. DCSR Asset Management Policy

8.5. DCSR Business Continuity Plan

9. CONTRAVENTIONS

Any person who contravenes or fails to comply with any provision of this policy may be subjected to disciplinary action through disciplinary processes applicable to the Public Service.

10. APPROVAL

MR SW MNISI
HEAD: CULTURE, SPORT AND RECREATION
DATE: 5/1/2017