Province of the
EASTERN CAPE
RURAL DEVELOPMENT AND
AGRARIAN REFORM

DEPT OF RURAL DEVELOP
AND AGRARIAN REFORM
2018 -06- 07
RECEIVED

Information Communication and Technology Policy

Vibrant, equitable, sustainable rural communities and food security for all

PROVINCIAL GROWTH AND DEVELOPMENT PLAN
PGDP
EASTERN CAPE

Ikamva eliqaqambileyo!

FOREWORD

DRDAR Executive Management is actively supporting Information Communication and Technology within the department through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of Information Communication and Technology responsibilities.

This commitment from the executive management:

i) Provides the necessary direction and support to information security;

ii) Acknowledges that Information Communication and Technology is a business-critical issue to DRDAR ;

iii) Demonstrates the commitment of DRDAR to a security-positive environment; and

iv) Demonstrates to all parties with whom information is exchanged that DRDAR deals with Information Communication and Technology in a professional manner.

MR L. L NGADA

HEAD OF DEPARTMENT: DRDAR

DATE: 27/03/2018

Abbreviations and Definitions

Abbreviations

COBIT	Control Objectives for Information and related Technology
DRDAR	Department of Rural Development and Agrarian Reform
HOD	Head of Department
ICT	Information Communication and Technology
ICTSC	Information Communication Technology Steering Committee
IS	Information Security
IT	Information Technology

Definition and Terms

Access - Two types of access - Physical and Logical.

Physical Access The process of obtaining use of a computer system, - for example by sitting down at a keyboard, - or of being able to enter specific area(s) of the organisation where the main computer systems are located.

Logical Access The process of being able to enter, modify, delete, or inspect, records and data held on a computer system by means of providing an ID and password (if required). The view that restricting physical access relieves the need for logical access restrictions is misleading. Any organisation with communications links to the outside world has a security risk of logical access.

Access Control - refers to the rules and deployment mechanisms which control access to information systems, and physical access to premises. The entire subject of Information Communication and Technology is based upon Access Control, without which Information Communication and Technology cannot, by definition, exist.

Asset - anything that has value to the organisation

Availability - the property of being accessible and usable upon demand by an authorised entity.

Authentication - refers to the verification of the authenticity of either a person or of data, e.g. a message may be authenticated to have been originated by its claimed source. Authentication techniques usually form the basis for all forms of access control to systems and / or data.

Authorisation - the process whereby a person approves a specific event or action. In companies with access rights hierarchies it is important that audit trails identify both the creator and the authoriser of new or amended data. It is an unacceptably high risk situation for an individual to have the power to create new entries and then to authorise those same entries themselves.

Back-up – the process whereby copies of computer files are taken in order to allow recreation of the original, should the need arise. A backup is a spare copy of a file, file system, or other resource for use in the event of failure or loss of the original.

BCP - Business Continuity Plan - This is a plan to ensure that the essential business functions of the organisation are able to continue (or re-start) in the event of unforeseen circumstances; normally a disaster of some sort.

Business Requirement - The needs of the business processes which must be addressed by either a manual or computerised system.

Confidentiality - the property that information is not made available or disclosed to unauthorised individuals, entities, or processes.

Control - means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be of administrative, technical, management, or legal nature.

DMZ - De-Militarised Zone, is a separate part of an organisation's network which is shielded and 'cut off ' from the main departmental network and its systems. The DMZ contains technical equipment to prevent access from external parties (say on the Internet) from gaining access to your main systems.

Employees – Employee means any person other than an independent contractor who Works for DRDAR or the state and who receives, or is entitled to receive any remuneration and in any manner assist in carrying on or conducting the business of an employer.

Encryption - a means of scrambling the data so that is can only be read by the person(s) holding the 'key' - a password of some sort. Without the 'key', the cipher cannot be broken and the data remains secure.

Information Asset - Refers to Information stored on electronic media, printed on paper, transmitted across networks (fax and email) and communicated by all means. Information asset refers to applications, servers, workstations and building facilities

Information Communication and Technology – Is the preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved

Information Communication and Technology event - an identified occurrence of a system, service or network state indicating a possible breach of Information Communication and Technology policy or failure of safeguards, or a previously unknown situation that may be security relevant

Information Communication and Technology incident - a single or a series of unwanted or unexpected Information Communication and Technology events that have a significant probability of compromising business operations and threatening information security

Integrity the property of safeguarding the accuracy and completeness of assets

Intrusion Detection Systems - monitor network activity using various techniques, such as 'intelligent agents'. Current applications will not only detect misuse but also identify a known pattern of attack, or attack scenario. The IDS can then automatically terminate the offending session and send an alert to the Systems Administrator.

Risk analysis- systematic use of information to identify sources and to estimate the risk

Risk assessment - overall process of risk analysis and risk evaluation

Risk management - coordinated activities to direct and control an organisation with regard to risk

Third party - a person or body that is recognised as being independent of the parties involved, as concerns the issue in question.

Threat - a potential cause of an incident that may result in harm to a system or organisation

Vulnerability - a weakness of an asset or group of assets that can be exploited by one or more threats.

User - includes employees, contractors, students, consultants, vendors with management approved access to information and information assets.

CONTENTS

1 Introduction

DRDAR information is an important asset that is protected according to its value and the degree of damage that could result from its misuse, unavailability, destruction, unauthorised disclosure or modification. This implies that information assets are identified, valued, assessed for risk and protected cost effectively from identified threats. Information Communication and Technology is the protection of information from a wide range of threats in order to ensure business continuity, minimise business risk, and maximise return on investments and business opportunities.

Information Communication and Technology Management refers to the implementation and co-ordination of department-wide measures aimed at protecting department information. The purpose of this Information Communication and Technology governing policy is to demonstrate management commitment to supporting the goals and principles of Information Communication and Technology in line with the DRDAR business strategy and objectives towards the protection of DRDAR and client information assets.

2 Policy Objectives

a) To protect the DRDAR information and any client or customer information within its custody or safekeeping by safeguarding its confidentiality, integrity and availability.

b) To safeguard department's information assets from theft, abuse, misuse and any form of damage.

c) To establish responsibility and accountability for Information Communication and Technology in the Department.

d) To encourage management and employees to maintain an appropriate level of awareness, knowledge and skill to allow them to minimise the occurrence and severity of Information Communication and Technology undesirable incidents.

e) To ensure that the Department is able to continue its business activities in the event of significant Information Communication and Technology adverse incidents.

3 Regulatory Frame Work

a) International Standards Operations (ISO) 27001/2
b) Information Communication and Technology Forum Standard
c) Minimum Information Communication and Technology Standard (MISS)
d) Electronic Communications and Transactions Act 25 of 2002
e) Public Service Corporate Governance of Information and Communication Technology Framework
f) Public Finance Management Act (PFMA) Act No 1 of 1999 as amended by Act 29 of 1999

4 Principles Values and Philosophy

To satisfy business objectives, information needs to conform to certain control criteria, which COBIT refers to as business requirements for information:

a) **Efficiency** – information is provided through optimal (most productive and economical) use of resources.

b) **Effectiveness** - information is relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.

c) **Confidentiality** - information is only accessible to those authorised to access it;

d) **Availability,** information is available and accessible by authorised users when required;

e) **Integrity** – to ensure authenticity, reliability and completeness of the information is protected.

f) **Compliance** – ensure compliance with the laws, regulations and contractual arrangements to which the business process is subject, i.e. externally imposed business criteria as well as internal policies.

g) **Reliability** - provision of appropriate information for management to operate the department and exercise its fiduciary and governance responsibilities.

h) **Authentication** - verification of the authenticity of either a person or of data, e.g. a message must be authenticated to have originated by its claimed source.

i) **Authorisation** - approval of a specific event or action must be approved by the relevant authority.

5 Scope of applicability

a) This Information Communication and Technology Policy applies to all DRDAR employees and business areas within DRDAR.

b) This ICT Policy applies to suppliers, clients, third parties, and other stakeholders.

c) This ICT Policy also applies to all information no matter what form it takes or means by which it is shared or stored. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation.

6 Policy Implementation

In alignment with the COBIT 5 framework which serves as a guideline in ICT Policy development; this policy is a combination of various policy areas that must be in place for effective implementation of ICT Governance.

For a broader and clearer interpretation of this policy; implementation procedure guidelines must be read in conjunction with this document.

This policy covers the following policy areas:-

a) Information Classification and Asset Management
b) Human Resource Security
c) Access Control
d) Cryptography
e) Network Security
f) Electronic Communication
g) Acceptable and Non acceptable Use
h) Change and Configuration Management
i) Audit Controls
j) Business Continuity
k) Information systems acquisition, development and maintenance

6.1.1 Information Classification and Asset Management

The classification of information or an information system is determined based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organisational operations, organisational assets, or individuals. DRDAR must ensure that information is classified in terms of its value, legal requirements, sensitivity and criticality to the department in order to protect the information asset.

DRDAR Management must ensure that inventory/inventories of all information assets are drawn up and maintained.

6.1.2 Policy statements

This Information classification and asset management Policy has the following objectives:

a) To achieve and maintain appropriate protection of organisational assets.

b) To ensure that information receives an appropriate level of protection.

c) To protect the DRDAR information and any client information within its custody by safeguarding its confidentiality, integrity and availability.

6.1.3 Inventory and Assets Management

a) As it is critical for Disaster Recovery and Business Continuity, inventory of all IT resources must be kept by means of an ICT asset register.

b) Items in the asset register must be uniquely identified by means of a serial number and the barcode allocated by asset management of the Department.

c) It is the .responsibility of the GITO Directorate to ensure that all newly procured, reallocated and disposed items are included in the ICT asset registry.

d) Computer equipment found to be redundant or obsolete must be reallocated or disposed after a motivation has been supplied to the DRDAR Disposal Committee.

6.1.4 Responsibility for Assets

a) All IT assets must be accounted for and have a nominated official to whom the responsibility of appropriate controls should be assigned. This responsibility should commence on physical receipt of the asset by the official.

6.1.5 Information Classification

a) All information (both electronic and hard copy) must be graded or classified according to its degree of sensitivity, value, criticality to the Department and where relevant, regulatory requirements.

b) The responsibility for the grading and degrading of information (whether electronic or hard copy) rests with DRDAR where the information has its origin. This function rests with the author, information owner or Head of Department or his/her delegate(s).

c) The classification assigned to information must be strictly observed and may not be changed without the consent of the Head of Department or his/her delegate.

6.1.6 User Classification

a) Technical support provided to users will be according to their roles and responsibilities within the department

b) Executive Management may get priority support on the calls logged on their behalf.

c) The MEC, Head of Department and the Deputy Director Generals must form part of the priority users list in the department.

d) Response time to calls will also differ and executive management will always be responded to in the shortest time.

e) Only selected, dedicated and certain level of technical support should provide the necessary support to executive management

6.1.7 Media handling and Labelling

a) Removable media containing or accessing DRDAR information resources must be permitted prior to connecting to DRDAR information systems. This pertains to all devices connecting to the DRDAR network, regardless of ownership.

b) DRDAR supplied removable media should be used primarily for legitimate business purposes in the course of assigned duties. Any personal use should not interfere with these duties or compromise the security or the business of DRDAR, and may only be incidental and occasional in nature.

c) Information on removable computer media must be backed up and updated on a regular basis and should only be used as a temporary data store, for a minimum possible duration and should not replace network storage

d) Personnel must adhere to the departmental disposal procedure and the National Archives and Records Service of South Africa Act (No.43 of 1996 as amended) when disposing of computer equipment and other information processing or storage devices containing sensitive information.

e) Destruction of media should be conducted only by trained and authorised personnel. Safety and special disposition needs should be identified and addressed prior to conducting any media destruction.

f) Users must exercise utmost discretion when sharing information with other people, taking into account the classification of the information and such information must be stored securely. Persons handling classified information must have the necessary security clearance.

6.1.8 Exchange of information

a) Users must ensure that the communication of sensitive information over internal or external networks, or via removable media, satisfy the requirements as stipulated in this policy.

b) The encryption standard should be applied for information transported across the network and devices, based on a risk assessment and information classification performed.

c) All classified documents or files (in hard copy or on storage devices such as CDs, DVDs, USB disks or external hard drives) to be dispatched via courier must be entered in a register indicating the title/description of the document and the date and time of dispatch, and must be handed over against the signature of the courier.

d) Classified documents in the Secret and Top Secret categories that cannot be dispatched by courier may, as an exception, be mailed on provision that it be sent by registered mail and then only with the express permission of the Accounting Officer.

6.1.9 Human Resource Security

a) DRDAR Information Technology Department in conjunction with DRDAR Human Resources must ensure that ICT responsibilities and procedures for employment, or termination or change of employment are clearly defined.

b) An adequate level of awareness, education, and training in ICT security procedures and the correct use of information processing facilities should be provided to all employees with access, contractors and third party users to minimize possible security risks. Handling of security breaches will be dealt with using the departmental disciplinary processes for internal employees and, for external users security breaches will be dealt with by legal department.

c) Guidelines must be in place to ensure an employee's, contractors or third party users exit from the organization is managed, and that the return of all equipment and the removal of all access rights are completed.

d) Change of responsibilities and employments within an organization must be managed as the termination of the respective responsibility in line with ICT, and any new employments should be managed.

6.1.10 Policy statements

a) The employees of the Department accessing information systems and the data processed by the systems must meet the necessary security requirements as determined by the sensitivity of information accessed.

b) Access to the systems and data should be immediately terminated as soon as evidence to non-compliance with the security requirements is detected.

c) All employees who use IT services are required to acknowledge acceptance and intention to comply with the Acceptable Use Policy by signing the Departments Information Technology User Declaration Agreement.

d) Any employee found to have violated this policy must be subjected to disciplinary action.

6.1.11 During employment

a) The Department adopts a zero tolerance stance and therefore failure to comply with this policy or any of the supporting and complimenting policies, standards and processes are viewed as misconduct that could result in a security violation.

b) A formal disciplinary process must be followed for employees who have violated departmental security policies. This process must ensure correct and fair treatment of employees who are suspected of committing serious or persistent security breaches.

c) All public service technical and IT operations staff must receive training in information and IT security threats and safeguards. The extent of the training should reflect staff member's individual responsibility for configuring and maintaining information security.

d) Where IT staff change jobs, information and IT security needs must be re-assessed and new training provided as a priority and all new information system and IT end user staff is to receive mandatory Information Security training as part of induction.

6.1.12 Termination or change of employment

a) In the event that an employee, consultant, or contractor is terminating his or her relationship with the Department, HRM must notify the Information Technology (IT) directorate within one business day.

b) In cases where computer support personnel are involuntarily terminated, they must immediately be relieved of all duties and be caused to immediately surrender all departmental equipment and information, and escorted while they pack up their belongings and leave the DRDAR's facilities.

6.1.13 Access Control

Effective access control mechanisms can reduce the risk of unauthorised access to information and systems of the department. Access control arrangements should be established to restrict access by all types of user to approved system capabilities of the computer installation. A poorly chosen access control mechanism may result in unauthorized access and/or exploitation of Department of Rural Development and Agrarian Reform information and information assets.

6.1.14 Policy statements

The purpose of this policy is to establish a standard for the creation of strong access control, the appropriate use of access control mechanism as well as the management of access control. The policy will address the logical and physical access to information prevents unauthorized access to information systems.

6.1.15 Business requirement for access control

a) Users access to functions and information must be restricted according to individual user roles and based on a "need to know and need to do basis" as specified by information system owners.

6.1.16 User Access Management

a) Access to the DRDAR IT network and IT resources will be provided to all employees, contractors, consultants, temporary workers, in line with their specific work function and will be promptly terminated at the time when an employee, contractor or 3rd party ceases to provide services to DRDAR.

b) IT users of the system must be identified using a unique User ID and authenticated with a password to ensure repudiation and such ID's must conform to the recommended standard naming convention.

c) Users are to access only files and data that are their own, are publicly available, or to which authorised access has been granted. Under government rules and regulations, the illegal access of confidential information must be considered a dismissible offence.

d) DRDAR's systems and technical support staff must support a clear separation of functions (such as system administrators vs. regular users) to prevent unauthorised access and functions being performed.

e) In order to prevent unauthorised access to DRDAR computer systems, a formalised password standard must be in place regarding password length and composition (alphanumeric), frequency of change and re-use of passwords.

f) Passwords must be locked out after 3 invalid attempts

g) Passwords will have a password history of a minimum of 20 passwords

h) A formal test and review of users' access rights must be conducted periodically by GITO and the System Controllers. IT staff must generate relevant reports to facilitate this process.

6.1.17 User responsibilities

a) All personnel are responsible for all activities performed with their personal user IDs as well as special logon IDs. As such, user IDs and other logon IDs may not be utilised by anyone other than the individuals to whom they have been issued and users are forbidden from performing any activity with IDs belonging to other users. Gross negligence or wilful disclosure of this information can result in disciplinary action, including termination.

b) The screensaver of all workstations and mobile computing devices (including desktop PC's, laptops, PDA's, cellular telephones and tablet computers) that are left unattended while connected to the network should be activated, the screen locked or the account logged out. If the workstation or device screen cannot be locked, it should be shut down/switched off.

6.1.18 Network, Operating System and Application Access Control

a) A formal record, identifying users and the specific services to which they have access to must be maintained.

b) Access to DRDAR computer systems and network from DRDAR premises must only be attempted by way of computer equipment made available by DRDAR to users. Use of other computer equipment to access the DRDAR network must be specifically authorised by the GITO.

c) DRDAR network architecture is based on the windows server authentication platform and therefore all unit connecting to the network must be windows based.

d) All access to the network must be authenticated. This must include all network logons requiring a unique user ID and password to ensure that only authorised users gain access to the network and users are required to log out of all systems, including the network, after hours.

e) DRDAR employees and contractors with remote access privileges will ensure that DRDAR-owned or personal computer and workstation, which is remotely connected to the DRDAR network, is not connected to any other network at the same time.

f) DRDAR networks should be segregated into logical and physical segments or network domains based on the value and classification of information or assets that need to be accessed, levels of trust, or lines of business.

g) DRDAR reserves the right to adjust, suspend, or permanently revoke powerful access-rights at any time, without notice, discussion or disclosure at the entire discretion of the information owner.

6.1.19 Physical and Environmental Security

a) Buildings and rooms/ storerooms housing major concentrations of IT equipment, local cabling and non-critical hardware are classified as secure areas.

b) Effective control must be instituted over access to security areas in a building such as cryptographic and computer centres, the registry (where secret and top secret documents and files are kept) and other areas identified as sensitive. An access register must be instituted and kept up to date for all persons/officers not normally working in these areas.

c) Based on the category of the secure area, the GITO directorate must ensure that the physical and environmental controls are implemented to protect the information processing facilities which are consistent with the equipment they contain.

d) Access to secure areas should be reviewed on a periodic basis by the building facilities manager or any other designated IT management representative.

e) Access to delivery and loading areas must be appropriately controlled to avoid unauthorised access to public service information processing facilities.

f) Third party organizations will be given access privileges to the IT resources after DRDAR management has determined that they have legitimate business need. These privileges will be enabled only for the time period required to accomplish approved tasks.

g) A Third Party Company must apply in writing to the departmental GITO for access to the department's Network.

h) No visitors must be allowed access to any of the IT resources of the Department unless approved by the GITO. The hosting party/person is responsible for ensuring that the required approval is obtained before any access is granted.

6.1.20 Cryptography

a) Making a decision as to whether a cryptographic solution is appropriate should be seen as part of the wider process of risk assessment and selection of controls. This assessment can then be used to determine whether a cryptographic control is appropriate, what type of control should be applied and for what purpose and business processes.

b) Key Management Server should be in place to support the use of cryptographic techniques. All cryptographic keys should be protected against modification, loss, and destruction. In addition, secret and private keys need protection against unauthorized disclosure. Equipment used to generate, store and archive keys should be physically protected.

6.1.21 Policy statements

The purpose of this policy is to protect the confidentiality, authenticity and integrity of information by cryptographic means.

A policy on the use of cryptographic controls is necessary to maximize the benefits and minimize the risks of using cryptographic techniques, and to avoid inappropriate or incorrect use. When using digital signatures, consideration is given to relevant legislation, in particular those describing the conditions under which a digital signature is legally binding

6.1.22 Cryptographic Controls

a) To prevent unauthorized disclosure of data when computers are sent out for repairs or when they are stolen, all data stored on hard disks must be encrypted.

b) The system owner and/or data owner and/or information transmitter should determine the need for encryption of data based on its sensitivity.

c) The use of cryptographic keys for encryption of sensitive information should be formally approved by the GITO of DRDAR.

6.1.23 Network Security

The departmental network infrastructure is provided as a central utility for all users of DRDAR Information Resources. It is important that the infrastructure, which includes cabling and the associated equipment such as routers and switches, continues to develop with sufficient flexibility to meet user demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

The level of protection will be assessed by analysing confidentiality, integrity and availability and any other requirements for the information considered.

6.1.24 Policy statements

The purpose of the Network Security Policy is to establish the rules for the maintenance, expansion and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of DRDAR information.

6.1.25 Equipment Security

a) The buildings that house IS and IT equipment must be constructed so that they offer adequate protection against environmental threats and hazards such as fire, water damage and vandalism.

b) Based on the category of the server room, the equipment must be protected from power failures and electrical anomalies by a suitable electrical supply (Uninterrupted Power Supply or UPS).

c) Power and telecommunications cabling carrying data or supporting information services must be protected from interception or damage.

d) Other computer related devices such as smartphones, tablets, scanners etc. are also non-standard DRDAR computer equipment and **must not** be provided unless specifically requested and approved by the Head of Department.

6.1.26 Network Security

a) The SITA GCCN (Openet Security Policy) must apply for the remote connections to the department's environment to ensure the safeguarding of information in networks and the protection of the supporting infrastructure.

b) A Network Specialist is responsible for the design and configuration management of the LAN, maintenance of the existing LAN, and procurement of hardware and software to support the LAN.

6.1.27 Server Security

a) All servers hosting data and applications must be located in a physically secure environment where access is strictly controlled and logical access to servers must be allocated on a need-to-know basis, in accordance with the access control section of this policy.

b) Servers must be backed up in accordance with the departmental backup policy and procedures as outlined by the department's backup & recovery policy.

6.1.28 Workstation Security

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

b) Sensitive data must not be stored on local hard drive of workstations. All sensitive data processed using workstations will be saved on a secure network drive on a server.

c) All workstations must be loaded and protected by the latest approved Anti-Virus software.

d) It is the responsibility of the workstation user to ensure that appropriate security measures and practices are adhered to adequately to protect their workstation from logical threats as well as physical environmental threats.

e) Workstations used to access sensitive information like Finance, HR and investigations data classified to be highly sensitive will be protected by means of password protected screen save.

f) Users **must not** share domain passwords and user accounts with anyone.

6.1.29 Mobile computing and Tele-working

a) The Head of Department must authorise the issue of portable devices. Usage is restricted to business purposes, and users must be aware of, and accept the terms and conditions of use, especially responsibility for the security of information held on such devices.

b) Persons who are issued with portable devices and who intend to travel for business purposes must be made aware of the information security issues relating to portable computing facilities and implement the appropriate safeguards to minimise the risks.

c) Users must not make use of remote control software to control their or any other computer within the department unless they are authorised to do so to perform their function.

d) Off-site computer usage, whether at home or at other locations is restricted to business purposes. The users must be aware of and accept the terms and conditions of use, which must include the adoption of adequate and appropriate information security measures.

e) All wireless access points connected to the departmental networks must be registered and approved by GITO. These Access Points are subject to periodic penetration tests and audits.

f) Users must exercise caution when connecting to wireless access points that appear to be legitimate.

6.1.30 Network Security Management

a) The departmental IT must tightly control the physical access to the firewalls, allowing only the firewall administrators and network services manager physical access to the servers.

b) Privileges to modify the functionality, connectivity and services supported by firewalls must be restricted to a few individuals with a business need for these privileges. These privileges may only be assigned to competent technical staff. There must be at least two staff members who are adequately trained to make changes to each firewall, so as to provide a backup in the event of an emergency.

6.1.31 Malicious Code Protection - Anti-Virus

a) Departmental Information Technology must ensure that all desktops, servers and mobile devices have the latest versions of an approved malicious code protection software implemented, enabled and maintained.

b) All equipment connected to the network must have an approved and up-to-date anti-virus and integrity-checking software installed.

c) No employee may knowingly distribute viruses or bypass any detection systems in place.

d) Users are not allowed to open any e-mail if the source of the e-mail is unknown to the user.

e) Individuals receiving or downloading data media, from any source within or outside the Department, have the responsibility for ensuring that it is checked for viruses before use. Similarly, individuals intending to pass on data media within the department or to external parties must ensure that it is first checked for viruses.

f) Computer virus policies require that the presence of viruses be automatically detected.

g) There must be an automatic, daily, update of the virus definitions for all servers and personal computers.

6.1.32 Electronic Communication

a. DRDAR encourages the use of electronic communications to share information and knowledge in support of DRDAR's mission to public service and to conduct DRDAR's business. To this end, DRDAR supports and provides interactive electronic communications services and facilities for Telecommunications. All electronic communication services such as internet and e-mail services must be securely utilised to prevent misuse and security threats.

6.1.33 Internet Security

a) All Internet connections must be via the approved Internet service provider of DRDAR. Any other connections are prohibited.

b) 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.

c) Staff must be aware that they are prohibited from accessing or transmitting sexual, racist or religious information / images, which may be offensive; making obscene, discriminatory or harassing statements; which may be illegal or downloading illegal material while using DRDAR e-mail system, Internet or Intranet, as this constitutes prohibited material.

d) Users will·not publicly disclose internal DRDAR information via the Internet, which could adversely affect the DRDAR, customer relations or public image.

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

f) Only DRDAR approved versions of Internet browsers are to be used with necessary cumulative updates or the applicable version at the time. Users are prohibited from changing any configuration properties of their web browsers.

g) It is discouraged for employees to browse the Internet for non-business purposes during working hours

h) Posting of personal messages on the Internet showing affiliation with DRDAR is forbidden.

i) The downloading of software onto the organisation's system without the prior written consent of line management is prohibited. Software pertaining to direct business use, will be downloaded, scanned and installed with managerial approval. Downloaded software may only be used under the terms of its license agreement.

6.1.34 Issuing of 3G Data Cards

a) 3G Data Cards are issued to those members of staff who after application have a proven requirement for internet & email mobile connectivity.

b) Under no circumstances must Officials send Short Message Services (SMS), make video calls or voice calls or subscribe for any other functionality of the 3G Data Card that is not for Official purposes.

c) Officials should always ensure that the 3G Data Cards are securely kept to prevent damage, theft or loss.

6.1.35 Instant Messaging

a) To ensure that instant messaging services are available when required, the confidentiality and integrity of messages is protected in transit, and the risk of misuse is minimised.

b) Use of instant messaging should be signed off by an appropriate business representative.

6.1.36 E-mail Security

a) As a productivity enhancement tool, DRDAR 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 DRDAR.

b) E-mail must be used primarily for legitimate business purposes in the course of assigned duties. Incidental and occasional limited personal use of the e-mail system is permitted, providing at all times that such use does not:

   i) Interfere with the user's work or performance;

   ii) Interfere with any other user's work or performance;

   iii) Cause disruptions to the operations or resources of DRDAR information system resources; and

c) Sending of forged e-mail messages is expressly forbidden. Individuals are not to use an e-mail account that has been assigned to another user. All messages must clearly identify the true author.

d) To protect DRDAR network from threats such as mail bombs, automatic forwarding of e-mail from external addresses to DRDAR e-mail systems is prohibited.

e) Business related e-mails should only be sent from DRDAR e-mail addresses and not sent from a private e-mail account e.g. gmail, yahoo, live, Hotmail etc.

6.1.37 Acceptable and Non Acceptable Use

As the Department provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives and it must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets.

This policy requires the users of information assets to comply with departmental policies and protects the department against damaging legal issues.

6.1.38 Ensuring Compliance

a) Personnel must be trained in what is acceptable and prohibited. Any contravention of corporate acceptable use policies should constitute a security violation and transgressing personnel must be held accountable and may be subjected to disciplinary action or criminal prosecution

6.1.39 Complying with Copyright and Licensing

a) All software used on departmental information resources must be procured in accordance with official departmental policies and procedures, and must be licensed, and registered in the name of the Department. All personnel must abide by software copyright laws and must not obtain, install, replicate, or use software except as permitted by the software licensing agreements.

6.1.40 Using personally owned software

a) To protect the integrity of the departmental information resources, personnel must not use personally owned software on departmental information resources. This includes purchased and licensed applications, shareware, freeware and downloads

6.1.41 Protecting Intellectual Property

a) To ensure the integrity of departmental software, all personnel must abide by the intellectual property protection contract provisions of the Department.

6.1.42 Authorized monitoring

a) System administrators and other personnel with unrestricted access to email and similar services must receive management approval prior to decrypting or reading the email traffic of other personnel. If management approval is not immediately available, then system administrators and other personnel that intercept, read, or restrict email accounts must document their actions and provide that documentation to management within twenty-four (24) hours.

6.1.43 Generally Prohibited uses of Information Resources

a) Generally prohibited activities when using departmental information resources include, but are not limited to, the following:

I. Stealing or copying of electronic files without permission.

II. Violating copyright laws.

III. Performing unofficial activities that may degrade the performance of systems, such as the playing of electronic games.

IV. Performing activities intended to circumvent security or access controls of any organization, including the possession or use of hardware or software tools intended to defeat software copy protection, discover passwords, identify security vulnerabilities, decrypt encrypted files, or compromise information security by any other means.

V. Promoting or maintaining a personal or private business, or using departmental information resources for personal gain.

VI. Using someone else's logon ID and password.

VII. Conducting fraudulent or illegal activities, including but not limited to: gambling, trafficking in drugs or weapons, participating in terrorist acts, or attempting unauthorized entry to any departmental or non-departmental computer.

VIII. Conducting fundraising, endorsing any product or service, lobbying, or participating in any partisan political activity.

IX. Disclosing any departmental information that is not otherwise public.

X. Performing any act that may defame, libel, abuse, embarrass, tarnish, present a bad image of, or portray in false light, the Department or any person.

6.1.44 Incident Management

A formal information security event reporting procedure should be established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of an information security event. A point of contact should be established for the reporting of information security events. IT should be ensured that this point of contact is known throughout the organization, is always available and is able to provide adequate and timely response.

Responsibilities and procedures should be in place to handle information security events and weaknesses effectively once they have been reported. A process of continual improvement should be applied to the response to, monitoring, evaluating, and overall management of information security incidents.

Where evidence is required, IT should be contacted to ensure compliance with legal requirements.

6.1.45 Reporting information security events and weaknesses

a) All incidents, security related environmental changes or software malfunctions with the potential to disrupt network traffic or operational systems, or threaten confidentiality, integrity or availability of any component of a DRDAR information system must be reported to the line manager and the Helpdesk who should escalate all high impact incidents to the Information Security Officer / Specialist and GITO as soon as possible so that prompt remedial action can be taken.

b) All DRDAR employees, IT staff, external parties, contractors and temporary staff must be made aware of the security incident reporting procedure and that they are required to report any security incidents and malfunctions as soon as possible.

6.1.46 Management of information security incidents and improvements

a) The first priority in responding to any security incident in the department is to stop the security breach itself and prevent its recurrence. Where the severity of the incident and its likelihood of recurrence justifies it, management can and must take any steps necessary on a temporary basis, such as removing systems from operation, revoking system accesses or removing involved personnel from departmental facilities.

6.1.47 Communication

a) To ensure that communication can still continue with outside companies in the event of incident handling, business unit must document all guidelines and contact details for interactions with other organisations regarding incidents.

b) The Directorate: Communication is solely responsible to liaise with the media

c) On instruction of the Head of Department, Forensic Investigators must be appointed to ensure that incidents of high impact are reported to the South African Police Services to be investigated and that unlawful acts can be convicted.

6.1.48 Incident Management (Handling)

a) All users of Information System services must 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-deliberate breaches of security must be investigated and reported.

6.1.49 Training

a) **Line Management is** responsible to ensure that **Technical Administration staff members** dealing with respective system incidents have obtained specialised knowledge and experience.

6.1.50 Change and Configuration Management

The Change Management regulates all configuration changes to the public service information technology environment, to ensure that it is controlled and coordinated. It ensures that no changes are made unless a full assessment has been done on the impact and risk to the organisation and authorisation has been obtained to perform such a change.

Change: A change is any activity that occurs to any information resource where the status is different from a previously defined condition. This is applicable to all DRDAR IT hardware, communications equipment and software, system software, 'live' applications software and all documentation and procedures that are relevant to the running, support and maintenance of live systems. A change can also be initiated to resolve a critical problem.

Emergency Change: An emergency change is an unexpected or unplanned change that will either minimise service disruption or restore service.

The departmental Management must ensure that a defined change management process is used to ensure that changes are evaluated, prioritised, authorised, planned, tested, implemented, documented, and reviewed in a controlled manner to, among other things, reduce incidents and disruption.

A configuration management system must be used to maintain accurate configuration records, manage changes and releases effectively, and to resolve incidents and problems faster.

Clear and comprehensive release and deployment plans must be adhered to, to ensure that release packages are built, installed, tested and deployed securely, efficiently, successfully and on schedule.

6.1.51 Audit Controls

a) The departmental Information Technology component must ensure that regular audits and activities involving checks on operational systems are carefully planned and conducted at least annually.

b) Audit logs recording user activities, exceptions, and Information Communication and Technology events must be developed and implemented by the departmental Information Technology component.

6.1.52 Business Continuity

The policy recognizes the potential strategic, operational, financial and stakeholder support risks associated with service interruptions and the importance of maintaining viable capability to continue with departmental business processes with minimum impact in the event of an emergency.

This policy provides guidance for the Resumption and Recovery of time sensitive business operations in accordance with pre-established timeframes as well as ensuring that adequate plans are in place for the less time sensitive business operations.

Managed processes, plans and strategies must be maintained for disaster recovery and business continuity throughout the organisation to address the Information Communication and Technology requirements needed for the organisation's business continuity.

6.1.53 Information security aspects of business continuity management

a) A documented and tested Disaster Recovery Plan (DRP) must cover all critical business processes, systems and Information System facilities. The DRP should be addressed as a subset of Business Continuity Plan (BCP) of the department. Business Continuity Plan is the responsibility of the executive management (Security Committee) and it shall include all the areas of security and risk in the Department, as outlined in the DPSA Information and Communication Technology Service Guideline of January 2018.

b) The contingency plan of the department must provide for the destruction, storage and/or moving of classified/sensitive documents in the event of an emergency in order to prevent the risk of being compromised.

6.1.54 Backup

a) Regardless of classification, the availability of all data must be maintained by means of periodic back-ups and recovery mechanisms.

b) Off-site storage of back-up media: Back-ups of sensitive, critical, and valuable information must be stored in an environmentally-protected and access-controlled site, situated in an area where the possibility of the risk occurring at this site is minimal.

c) To prevent data from being revealed to or used by unauthorised parties, all sensitive, valuable, or critical information recorded on back-up media (tapes, floppy disks, CDs, etc.) which is stored outside the departmental offices must be covered adequately in the existing contract/arrangement of the service provider.

d) All public service related files are to be stored on the departmental network file server. No public service related files are to be stored on local hard drives. This is critical as no local drives are backed up. GITO will not be able to recover any lost files that were stored on local drives.

e) Personal files must not be stored on network servers – under no circumstances are personal, non-business related files to be stored on a DRDAR's file servers. In the event of PC theft where confidential data was stored on the local drive, the employee shall be held responsible for the loss of such data.

6.1.55 Information systems acquisition, development and maintenance

a) When a need to acquire or develop a new system arises from the directorate/department within DRDAR, GITO must be consulted prior development or acquiring of the new system.

b) New systems or applications, that are developed or acquired, need to function securely in the public service information environment. For this purpose information security considerations need to be addressed from the beginning.

c) Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. The design and implementation of the information system supporting the business process are crucial for security. Security requirements should be identified and agreed prior to the development and implementation of information systems. This can ensure that later additional costs are not incurred by adding information security to existing systems and applications.

d) All the business requirements should be identified at the requirements gathering phase of a project and justified, agreed, documented and signed-off as part of the overall business case for an information system.

e) Appropriate controls should be designed into applications, including user developed applications to ensure correct processing. These controls should include the validation of input data, internal processing and output data.

f) Access to system files and program source code should be controlled, and IT projects and support activities conducted in a secure manner. Care should be taken to avoid exposure of sensitive data in test environments.

g) The developed/acquired solution must be tested by ICT and the User Acceptance Testing should be done by the business, prior implementation/go live, for quality assurance.

6.1.56 Security Requirements of Information Systems

a) All systems developed for the DRDAR must be developed in accordance with a formally defined System Development Life Cycle.

b) Security requirements of a development should be determined and the risks should be identified before a system is developed.

c) Prior to live implementation of a system, security requirements must be reviewed and confirmed to ensure that required security mechanisms have been implemented.

6.1.57 Security Requirements Analysis and Specification

a) During the implementation of all new systems or changes to systems development, staff should document all aspects of how information security has been considered and implemented. In addition, system developments and changes to existing systems must have accompanying up to date documentation before going live. This is to include appropriate signoff levels by a system chief user, the Responsible Manager Information Systems.

b) Business application systems should go into production when all users and information operations staff have received appropriate documentation and training.

c) Vendor developments or modification must be governed by an approved system development methodology outlined in the service level agreements.

d) Staff members in the Directorate: Systems Development involved in system development or making changes to existing systems must at all times ensure that no third party rights are infringed upon.

e) When a need arises to make alterations to an existing system all parties involved must comply with the Change Control procedure as outlined in this policy for any information application, computer installation, network or system changes. All associated or supporting documentation must be appropriately updated in response to the changes made.

6.1.58 Monitoring

a) Procedures for monitoring use of information processing facilities will be established to ensure that users are only performing authorised activities.

b) DRDAR reserves the right to intercept and / or monitor all communications and / or the use of all IT Systems and services, including e-mail and Internet usage, for security, management and maintenance purposes and any other lawful purpose.

c) Monitoring of Network Traffic: Network traffic, both internal and external facing gateways e.g. firewalls, routers etc. must be monitored for unusual activity (for example, abnormal combinations of connections, deliberate probing or attacks, unusually large amounts of data being transferred cross-border, etc.).

d) Monitoring of Individuals: Intensive, direct monitoring of an individual user (actions on the system, content of user files or electronic communications) may only be done by the GITO or firm-appointed agents in extreme cases where DRDAR has reason to believe that security threat exists.

e) Monitoring of software: Regular reviews should be conducted of software and data content of systems supporting critical business processes. The presence of any unapproved files or unauthorised amendments should be formally investigated.

f) Network monitoring: Monitoring will be performed at appropriate levels to detect malicious actions and determine the availability of network resources. Special attention will be given to detecting rogue devices (personal laptops, pocket PC's, wireless access points, etc.) on the LAN.

g) Computer Clocks: Computer clocks must be synchronized to ensure the accuracy of audit logs for investigations or as evidence in legal or disciplinary cases. Computers and communication devices that have the ability to operate as real-time clocks should be set to an agreed standard.

7 Awareness and Training

The Information Technology Department must ensure that Information Communication and Technology awareness, education and training programmes must be conducted regularly to ensure that users are aware of Information Communication and Technology policies, threats, and concerns.

8 Roles and Responsibilities

8.1.1 Executive Management

a) Assigned overall accountability for information security. Management is also responsible for setting a good example for their employees by following all applicable Information Communication and Technology practices.

b) A Security Committee responsible for enterprise security, including IT security related issues and business continuity must be put in place. This will be composed of representatives from Security Management (Chair), Records Management, GITO, Risk Management and Internal Audit. Representatives from the Business Units can be co-opted as and when required.

c) Executive Management will ensure implementation of and compliance with Information Communication and Technology policies, standards, procedures and guidelines as listed in this policy

d) Executive Management will ensure that all Information Communication and Technology policies are addressed at DRDAR meetings as part of performance management contract.

8.1.2 Security Committee

a) A DRDAR Security Committee is established to ensure a clear direction for security initiatives and visible management support.

b) The Security Committee should consist of a group of individuals in DRDAR who are responsible for Departmental Security, and who can assist those charged with the governance of Information Communication and Technology and those using information systems and technology in carrying out their responsibilities to protect the integrity, availability and confidentiality of public service information assets.

Responsibilities of this function include:

a) Ensuring proper protection of public service information;

b) Establish and assign security roles and responsibilities;

c) Assist management in performing security risk analysis, preparation of action plans and security evaluation of in-house developed and vendor products and solutions;

d) Approval, implementation and maintenance of the Information Communication and Technology policy;

e) Development, implementation and maintenance of Information Communication and Technology standards, procedures and guidelines;

f) Co-ordination of Information Communication and Technology Awareness campaigns;

g) Provision of professional Information Communication and Technology education, training, awareness programs and services to all users of DRDAR information assets;

h) Co-ordinate the implementation of Information technology security across DRDAR;

i) Act as a liaison function on Information Communication and Technology matters among DRDAR business units and are the focal point for all Information Communication and Technology activities throughout DRDAR;

j) Maintain periodic contact with relevant Information Communication and Technology authorities (e.g. law enforcement, fire department, supervisory authorities) in the event of Information Communication and Technology incidents;

k) Maintain periodic contact with relevant regulatory bodies and interest groups related to Information Communication Technology (e.g. Standing Committee on Information System Security (SCISS), Information Communication and Technology Forum (ISF), Information Systems Audit and Control Association (ISACA), International Information Systems Security Certification Consortium, Inc., (ISC)²® etc);

l) Support and advise the line functions in the implementation of Information Communication and Technology policies and standards for both information systems and the data that it processes;

m) Certify the validity of all Information Communication and Technology risk analysis; and

n) Investigate Information Communication and Technology breaches and perform other activities necessary to assure a secure information-handling environment.

8.1.3 Departmental Government Information Technology Officer (DGITO)

Responsible for establishing and operating the Information Security function and also accountable to the Head of Department for any matters having an impact on IS security.

8.1.4 Head of Department(HOD)

a) The HOD must provide an enabling environment for the implementation and enforcement of this policy as well as security operations and management of DRDAR systems.

b) The HOD must ensure that ownership and security responsibilities for all systems are defined.

8.1.5 Internal Audit and Risk Management

a) Internal Audit must ensure compliance of the Information Communication and Technology controls with the approved standards/best practices.

b) Ensure that weaknesses observed by the audit process are made available to and discussed with stakeholders to mitigate identified risks following natural disasters.

8.1.6 Information Communication and Technology Steering Committee (ICTSC)

a) ICTS Committee is responsible for overseeing the Information Communication and Technology Function and its activities and to provide clear direction and visible management support for GITO initiatives.

b) Responsible for the design, implementation, management, coordination and review of the organisation's Information Communication and Technology controls and policies, as well as providing guidance and advice on their implementation.

8.1.7 Network Security Specialist

Network Security Specialist is responsible for the implementation and maintenance of security controls that will improve information technology network security.

8.1.8 Application Security Specialist

a) Application Security Specialist is responsible for the development, maintenance and administration of information systems and applications security.

b) All security personnel should be made aware of their responsibilities and reporting lines in their contract of employment, job description or any other predetermined formal method of communication.

c) Internal audit must periodically review the adequacy of information system controls, as well as compliance with such controls.

8.1.9 ICT Administrators

ICT administrators are responsible for the practical implementation of security policies, standards, procedures and solutions.

8.1.10 Third Parties

a) All third parties such as contractors, consultants, business partners and outsourced staff must sign a confidentiality agreement as part of their initial terms and conditions of employment. The signing of the agreement should take place prior to the employee gaining access to DRDAR systems and information.

b) All the above-mentioned parties should be appointed with sufficient resources and authority to enable them to discharge their duties effectively.

8.1.11 Information owners

Information owners are responsible for determining classification levels of the information, as per Archives and Records Management Policy of the Department, as well as maintaining accuracy and integrity of the information.

8.1.12 System owners

System owners are responsible for ensuring that appropriate information controls are embedded in their information systems.

8.1.13 Users

Any person who uses a DRDAR information system must 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 must provide a means by which individual users can be held individually accountable for their actions.

Employees, contractors, and temporary and part-time employees are responsible for:

a) Ensuring that organisation information assets are used only in proper pursuit of the department's business in accordance with Information Communication and Technology policies, standards and procedures;

b) Ensuring that information is not improperly disclosed, modified, or endangered;

c) Reporting Information Communication and Technology breaches.

9 Policy Compliance

Failure to comply with this policy or any of the supporting and complementing policies, standards, and/or procedures must be construed as misconduct and may result in one or more of the actions mentioned below:

a) The restriction, suspension or termination of the user's access to the network, information, information assets and facilities, including the summary suspension of his or her access or rights pending further investigations;

b) The taking of disciplinary steps against the user, which may lead to suspension or dismissal.

c) The institution of legal proceedings by the Department, including but not limited to criminal prosecution under applicable laws that may prevail in South Africa from time to time.

10 Policy Deviation

Under compelling conditions where a solution or change does not comply with this policy a deviation request must be submitted to the Head of Department for approval.

11 Policy Review

The Information Technology Component is responsible for the development, review and evaluation of the Information Communication and Technology policies.

This policy must be reviewed in five (5) years after approval, or when required because of significant Information Communication and Technology incidents, new vulnerabilities and changes to organisational or technical infrastructure.

12 Recommendations and Approvals

Comments:

27/03/2018

Deputy Director General: Administration
Z.B. MAKINA

Date

Approved/~~Not Approved~~

Comments:

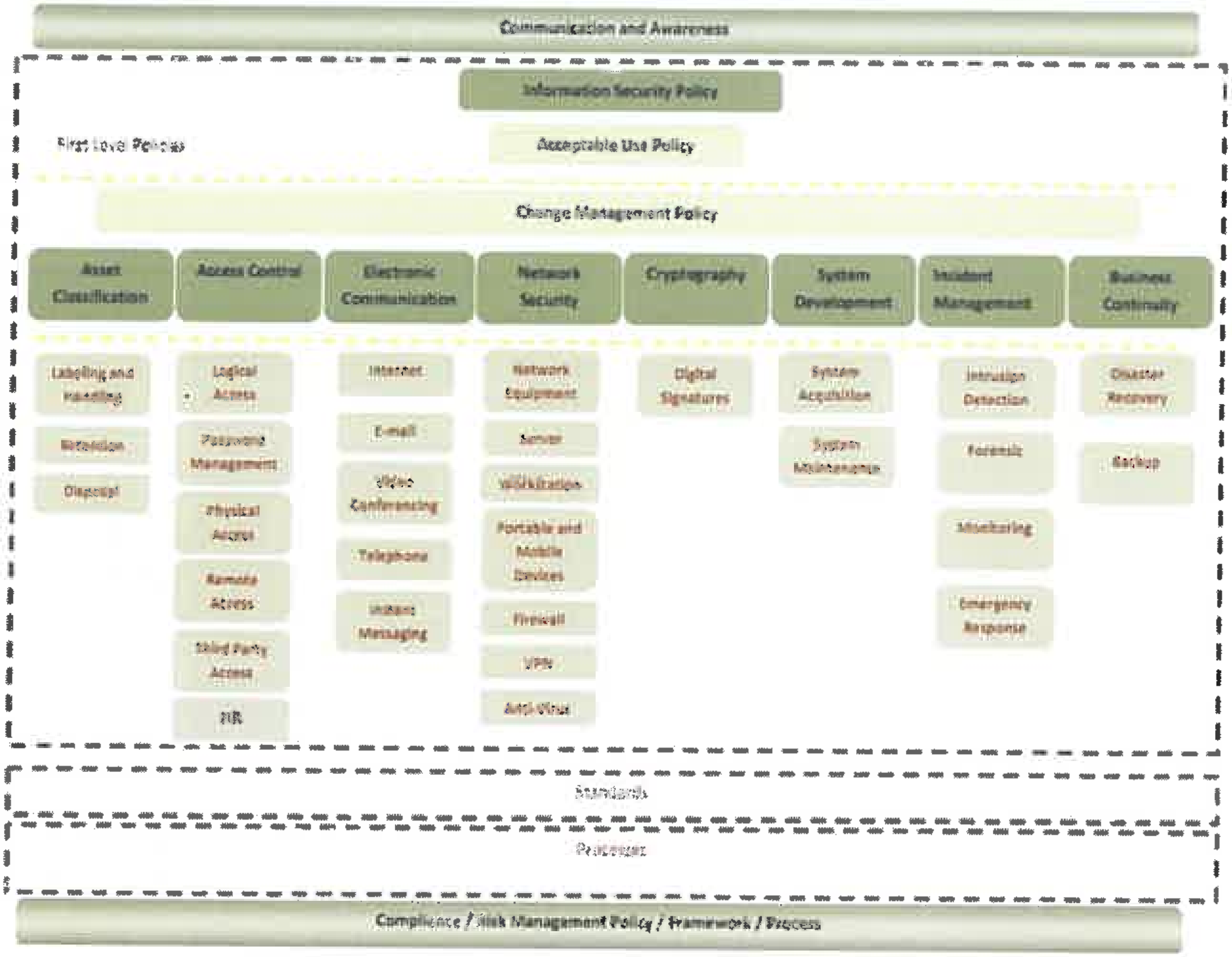
Ngad

27/03/2018

Head of Department
L.L. NGADA

Date

Annex A : Information Communication and Technology Framework



Annex A : Information Communication and Technology Governance Policy RACI Chart

R Responsible- Responsible to make sure that the process works as planned. The R owns the process/problem or project. **A–Accountable**- Delegated the task of completing the Activity. **C–Consult**- Have in depth knowledge of the process in question and all major decisions need signed off by section. **I–Inform**- Section that needs to be informed of activity taken, but not necessarily consulted.	**Daft and Review Policy**	**Communication and Awareness**	**Policy Implementation**
EXCO	I	I	I
ISSC	A	A	A
DGTO / Information Communication and Technology Department	R	R	R
Human Resources	C	I	R
Finance	C	I	R
Support IT	R	R	R
Internal Audit and Risk	C	I	R
Legal Services	C	I	R

Annex B : User declaration

I, ____

(FULL NAME AND EMPLOYEE NUMBER)

Hereby declare that:

a) I will take personal accountability and responsibility to apply Information Communication and Technology principles in my daily work-related activities.

b) I will attend applicable Information Communication and Technology awareness programmes and training, as determined by DRDAR.

c) I will ensure that information assets under my control and in my possession are protected as dictated by their classification level.

d) I undertake to use the information assets and equipment to which I have authorised access in the manner and for the reason intended. I will therefore not share my password with any individual.

e) I will participate in the determination of resilience measures, such as business continuity plans, for my area of responsibilities, where applicable.

f) I will adhere to environmental and physical security regulations.

g) I will immediately report any information security-incident and actively take part in resolving any incidents affecting my activities and outputs.

h) I will respect all protective measures implemented on my work station and will not try to circumvent or disable these in any way.

I understand that the DRDAR reserves the right to monitor the use of information resources to ensure the protection of the network, information and information assets. The monitoring activities will be performed in line with guidelines prepared by Human Resources Department.

I understand that disciplinary action is possible if I deliberately and knowingly contravene the Information Communication and Technology policy or any of the supporting and complementing policies, standards and/or procedures.

______________________________ ________________

SIGNATURE DATE