Building a Caring Society. Together.

Province of the
EASTERN CAPE
SOCIAL DEVELOPMENT

DEPARTMENT OF SOCIAL DEVELOPMENT INFORMATION SECURITY POLICIES AND ICT POLICIES

24 Hour Call Centre
Toll-Free Number : 080-0032-364

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

INFORMATION SECURITY POLICIES AND ICT POLICIES

A. Acceptable User Policy

I. Terms and Definition

Terms	Definition
i) Administration	Administration is the process of managing user identities, the roles and credentials they are assigned, and the resources and services they use.
ii) Department	the Department of Social Development
iii) Executive Management	this constitutes the Top Management of the Department
iv) Electronic Communications	any Communications via email, fax, telephone and internet
v) End user	the person utilising the information
vi) Database	This is a specialised software system that is used for managing highly structured data. Databases range from simple desktop systems to huge, multi-machine implementations.
vii) Host	A physical server that is housing a number of virtual servers within it.
viii)HTTP	Short for Hypertext Transfer Protocol, the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.
ix) Download	Accessing files over networks involves "downloading" them to your computer, disc drive or a part of your network. Web pages and the images or other files they contain are downloaded to your browser over the Internet or intranet, where they can be viewed as temporary files or saved.
x) Diginet Line	A Diginet leased-line connection is a permanent data circuit rented from Telkom that carries data from one fixed point to another.
Private Automatic Branch Exchange (PABX)	Private Automatic Branch Exchange (PABX) - sometimes shortened to PBX refers to private switchboards, providing internal telephony services to an organisation, and the interface with external telephone lines.

xi) Third Party	A third party is a person who is sponsored/contracted by the department and needs access to ECDSD resources.
Acronyms	
i) BYOD	Bring Your Own Device
ii) CIO	Chief Information Officer
iii) ECDSD	Department of Social Development
iv) GITO	Government Information Technology Officer
v) ICT	Information and Communication Technology
vi) IT	Information Technology
vii) ISP	Internet Service Provider
viii)iOS	Internet Operating System
ix) SG	Superintendent General

II. Legislative Framework

i) The Promotion of Access to Information Act, 2000 (Act no. 2 of 2000)
ii) The Protection of Information Act, 1982 (Act no. 84 of 1982)
iii) The State Information Technology Act, 1998 (Act no. 88 of 1998)
iv) SABS/ISO 17799 (2005)
v) Minimum Information Security Standards (MISS 1996)
vi) Guidelines for the Handling of Classified Information (SP/2/8/1) 1988
vii) Electronic Communications and Transaction Act, 2002 (Act no. 25 of 2002)

1 Preamble

The policy has been in use since 2012 but was due for review and with the change in technology and the inundated request from users to receive emails through their smart phones there was a need to address issues of bring your own device policy. This was pertinent due the technology evolution but it needs to be deployed within the acceptable controls. The other gap was the risk of fax to email solution that is not supported by the department. This posed a challenge on securing the information that traverse using this internet solution. The intention to publish the Acceptable Use Policy is not to impose restrictions that are contrary to the ECDSD established culture, openness, trust and integrity. The department is committed to protecting employees, partners, and the government of South Africa as a whole from illegal or damaging actions by individuals, accidentally or intentionally.

Every institution, to which the Minimum Information Security Standards and/or the Guidelines for the Handling of Classified Information (SP/2/8/1) apply, has the duty to secure computer networks containing classified data. This applies to all Government institutions who act as custodians of Government information and data. Government institutions are bound to uphold the right to privacy as entrenched in the constitution insofar as this relates to Government information and data.

Users shall be aware of the security limitations of the electronic communication channels, and shall not abuse their privileges. They shall promptly report all information security alerts, warnings, suspected vulnerabilities and suspected policy violations to the Information Security Manager. The ECDSD reserves the right to monitor all activity on ECDSD electronic communication channels. All policy violations shall be investigated by the Information Security Manager.

Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of any information user to know these guidelines and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of any information and information system within the Department of Social Development.

3. Objectives

The objective of this policy is to outline the acceptable use of any information and information system within the ECDSD. The overall objectives of this policy are to:

a) mitigate against legal liability by setting boundaries for appropriate employee conduct when using electronic communications facilities;

b) safeguard our Electronic Communications facilities from abuse, damage or disruption;

c) ensure that employees understand that the electronic communications facilities provided to them are primarily for business use; and

d) comply with all relevant regulatory and legislative requirements such as the Regulation of Interception of Communications Act (2002) and the provisions of the Electronic Communications and Transactions Act, 2002 (Act no. 25 of 2002)

4. Scope of Applicability

This is a standard departmental policy that applies to all users of the department's information and technology systems.

5. Principles and Values

Information security is more than just computer security. It also includes a wide range of physical security measures such as protecting your information assets against natural disasters or theft, and social engineering attacks such as someone tricking you giving out sensitive information. There are three basic principles of information security

a) **Confidentiality:** means making sure that information is only seen by people who have the right to see it.

b) **Integrity:** means making sure that information remains intact and unaltered.

c) **Availability:** implies having access to your information when you need it.

6. Policy statements

a. Privacy

a) The ECDSD reserves the right to intercept and quarantine networking traffic and computing resources, such as internet mail and other internet services, which may pose a threat to the ECDSD.

b) Any duly appointed Departmental accounting officer may, in writing, authorize access to any directory/sub directory, including directories/sub directories which purport to be personal to a user

c) All reports of alleged violations of this policy shall be investigated on a case-by-case basis by the Information Security Manager. During the course of the investigation, access privileges may be suspended. Violations of this policy may result in disciplinary action including, but not limited to the permanent loss of internet access privileges.

d) The ECDSD managers are responsible for ensuring that all employees, contractors, consultants, temporary staff and other users have read and comply with the substance of this policy.

e) Employees shall not post any information (software, internal memos, policies, etc.) on any publicly-accessible internet computer, unless the posting of these materials has first been approved by Executive Management. Likewise, the ECDSD's electronic mail system shall not be used to send or receive copyrighted materials,

f) trade secrets, proprietary financial information, client or employee information, or similar materials without prior authorisation.

b. Security

a) The ECDSD shall utilize proxy or other internet gateway solutions. The proxy or gateway shall be capable of implementing as many of the following controls as possible:

i) monitoring and filtering content accessed via web browsing and any other internet services for appropriate use;

ii) detecting malicious content;

iii) detecting unauthorised disclosure of ECDSD information;

iv) allowing only authorised, authenticated users access to web resources;

v) logging access and Audit Usage;

vi) caching; and

vii) detecting and blocking unapproved applications and protocols tunnelling through open, permitted ports.

b) All internet browsing shall traverse the ECDSD-controlled content filtering and inspection solution, whether locally installed at the endpoint, or via the network internet gateway.

c) Users shall promptly report all information security alerts, warnings, suspected vulnerabilities and suspected policy violations to the Information Security Manager.

d) Users are prohibited from utilizing ECDSD systems to forward such information to other users, whether the other users are internal or external to the ECDSD.

e) No media advertisement, internet home page, electronic bulletin board posting, electronic mail message, voice mail message, or any other public representation about the ECDSD shall be issued unless it has first been approved by the Communications Directorate or relevant authority.

f) All non-text files (databases, software object code, spreadsheets, formatted word processing package files, etc.) downloaded from non-ECDSD sources via an electronic communication channel shall be screened with virus detection software prior to being used. Whenever an external provider of the software is not trusted, downloaded software should be tested on a stand-alone non-production machine that has been recently backed-up. Downloaded files shall be decrypted and decompressed before being screened for viruses.

g) If an electronic mail message contains information relevant to the completion of a business transaction, contains potentially important reference information, or has value as evidence of a management decision, it shall be retained for future reference. Users are responsible for archiving these messages on designate servers or other approved storage. Electronic mail systems are not intended for an archival storage solution.

c. Electronic Mail Acceptable Behaviour

a) Before employees release any internal ECDSD information, enter into any contracts, or order any products via public networks, the identity of the individuals and organisations contacted shall be confirmed. Identity confirmation is ideally performed via digital signatures or digital certificates.

b) All official ECDSD electronic mail messages, including those containing a formal management approval, authorization, delegation, or handing over of responsibility, or similar transaction, shall be filed in an acceptable manner within the appropriate department.

c) Misrepresenting, obscuring, suppressing, or replacing a user's identity on the internet or any ECDSD electronic communications system is forbidden. The user name, electronic mail address, organisational affiliation, and related information included with messages or postings shall reflect the actual originator of the messages or postings. Falsifying mail addresses, headers, or routing information so as to obscure the origins or route a message may have taken is in direct violation of the ECDSD's security policies.

d) The ECDSD’s electronic communication system shall not be used to create any offensive or disruptive messages. Disruptions include, but are not limited to: distribution of unsolicited advertising or information, chain letters, charitable solicitations or propagation of malicious software. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, sexual orientation, religious or political believes, national origin, or disability. Users shall not use profanity, obscenities, or derogatory remarks in any form of electronic communication. To avoid libel, defamation of character, and other legal problems, whenever any affiliation with ECDSD is included with an internet message or posting, 'flaming' or similar written attacks are strictly prohibited. Likewise, employees shall not make threats against another user or organisation over the internet. All internet messages intended to harass, annoy, or alarm another person are similarly prohibited.

e) The ECDSD's electronic mail system shall not be used to send or receive copyrighted materials, trade secrets, proprietary financial information, client or employee information, or similar materials without prior authorisation. Users are required to respect and comply with local and international legal protection provided by trade secrets, patents, copyrights, and trademarks to any information viewed or obtained via the internet. Copying of software in a manner that is not consistent with the vendor's license is strictly forbidden. Similarly, the reproduction, forwarding, or in any other way republishing or redistributing words, graphics, or other materials shall be done only with the permission of the author/owner. Employees should assume that all materials on the internet are copyrighted unless specific notice states otherwise. Under no condition may staff participate in pirate software bulletin boards and similar activities via ECDSD-owned infrastructure. All contracts shall be formed by paper documents prior to purchasing or selling via electronic systems. ECDSD, electronic mail, and similar binding business messages shall therefore be releases against blanket orders, such as a blanket purchase order.

f) All electronic commerce systems shall be approved by the CIO and Legal representatives prior to usage. All contracts formed through electronic offer and

acceptance messages (fax, EDI, electronic mail, etc.) shall be formalised and confirmed via paper documents, or other legally binding mechanism, within two weeks of acceptance. Employees shall not employ scanned versions of hand rendered signatures to give the impression that an electronic mail message or other electronic communications were signed by the sender. Taking into account all applicable local legislation, the ECDSD shall implement disclaimer text for all outbound e-mail communication.

g) Sensitive information shall not be sent via unencrypted e-mail.

h) All electronic and paper documents shall be sent via approved ECDSD communication system services and no third party systems such commercial Fax to email systems will be utilised.

i) Employees may not employ internet service provider (ISP) accounts and outside connections, for example dial-up lines, to access the internet with ECDSD computers. Instead, all internet activity shall pass through ECDSD firewalls so that access controls and related security mechanisms can be applied.

j) The confidentiality of any e-mail message should not be assumed. Even when an e-mail message is erased, it may still be possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality. Where permitted by law, the ECDSD reserves and intends to exercise its right to review, audit, intercept, access and disclose all messages created, received or sent over the electronic messaging system for any purpose. The content of electronic messages properly obtained for legitimate business purposes may be disclosed within the ECDSD and to law enforcement agencies without the permission of the employee. Notwithstanding the ECDSD's right to retrieve and read any electronic mail messages, such messages shall be treated as confidential by other employees and accessed only by the intended recipient. Other than authorised systems administrators, employees are not permitted to retrieve or read any email messages for which they are not the intended recipient. Any exception to this shall be received in writing prior to disclosure of the electronic mail's contents.

k) The ECDSD reserves the right to delete outdated electronic messages stored on exchange systems to reserve space and simplify records management.

l) Use of anonymous log-ins for electronic communication channels is not permitted.

d. Internet Acceptable Behaviour

a) The decision to allow the personal use of Internet and e-mail is at the discretion of line management. Where allowed, any personal use of Internet, e-mail and other non-business activities shall be performed on personal, not department time, and is subject to the stipulations in the information security policy document. Access to private e-mail boxes via ECDSD computing resources is forbidden.

b) The department will give automatic internet access to all personnel classified as Assistant Manager and above. This policy also applies to secretaries and personal assistants of those classified as Director and upwards.

c) Browsing or distribution of distasteful material such as erotica, discriminatory sites that advocate racial supremacy, material that is forbidden by the laws of the country and sites that are not in alignment with the ideals or image of the department are prohibited. Employees using ECDSD computers who discover that they have connected with a web site that contains sexually explicit, racist, violent, or other potentially offensive material shall immediately disconnect from that site. The ability to connect with a specific web site does not in itself imply that users of ECDSD systems are permitted to visit that site.

d) Employees may not establish new internet web pages dealing with ECDSD business, or make modifications to existing web pages dealing with ECDSD business, unless they have first obtained the approval of the executive management. Modifications include the addition of hot-links to other sites, updating the information displayed, and altering the graphic layout of a page. Management shall ensure that all posted material is protected by adequate security measures approved by the ICT.

e) In keeping with the confidentiality agreements signed by all employees, ECDSD software, documentation, and all other types of internal information shall not be disclosed to any non-ECDSD party for any purposes other than business purposes expressly authorised by management. Exchanges of software and/or data between the ECDSD and any third party may not proceed unless a written agreement has first been signed. Such an agreement shall specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected.

f) Employees shall not probe security mechanisms at either ECDSD or other internet sites unless they have first obtained permission from CIO. Likewise, the possession of tools for cracking information security systems is prohibited without the advance permission of CIO. Likewise, using ECDSD networking and computing resources to make or attempt unauthorized entry to any network or computer accessible via the internet, is strictly prohibited.

e. Bring Your Own Device (BYOD)

a) Employees shall not to use their own personal notebook and laptop for work, the department prohibits such use of equipment in the ECDSD network.

b) Employees may be allowed to bring their own smartphones running the following operating system versions are allowed: iPhone 4 or older, Android 4.3 or older, Blackberry 7 or older and Windows Phone 8.0 or older.

c) BYO tablets including iPad and Android running minimum operating versions noted above are allowed.

d) Do not download or store any kind of confidential ECDSD information to your device or any personal, external storage device unless the data can be encrypted on the device. If you are uncertain whether it is permissible to download certain information, please review the Information System Security Policy and contact the legal section for advice.

e) Devices must be password protected with a strong password according to the Department’s password Policy.

f) Rooted (Android) or jailbroken (iOS) smartphones or tablets are strictly forbidden from accessing the ECDSD network.

g) Your personal data on your BYO device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of the department’s data and technology infrastructure.

7. Approving Authority

The member of the Executive Council and the Superintendent General has the responsibility to approve the departmental acceptable user behaviour Policy

8. Exceptions/ Exemption

Exceptions will be made for the new employees who have not received the ICT resources to bring their own Laptop/ Notebook for work purpose.

9. Accountabilities and Responsibilities

a. The Superintendent General

The SG in conjunction with the CIO shall implement, enforce and monitor the controls in accordance with the requirements outlined by management, and must advise users on the correct ways to access information and systems.

b. All employees

All employees are responsible for complying with this and other corporate policies at all times. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of acceptable behaviour) to comply with this policy and other information security policies.

c. Information Security Manager

Information Security Manager is responsible for maintaining this policy and advising generally on information security controls. Working in conjunction with other corporate functions, it is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy.

d. Internal Audit

Internal Audit is authorised by management to assess compliance with all corporate policies at any time.

10. Effective date of the Policy

The Acceptable User Behaviour is effective from the date the member of the Executive Council has approved it.

11. Monitoring Mechanisms

Such mechanisms as mentioned below shall be used to monitor this policy:

a) ICT Operational Committee
b) ICT Steering Committee
c) ICT Managers Meeting

The CIO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.

12. Review of the Policy

The policy will be reviewed every three years and whenever there are new developments to maintain relevance

13. Enforcement

a) The CIO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.

b) Failure to comply with this policy shall result in disciplinary action.

c) Any conduct that interferes with the normal and proper operation of the departments IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved acceptable user behaviour policy.

d) The ECDSD executive management reserves the right to revoke the privileges of any user at any time.

14 Policy Recommendation and Approval

The signatories hereof, being duly authorised thereto, by their signatures hereto authorise the execution of the work detailed herein, or confirm their acceptance of the contents hereof and authorise the implementation/adoption thereof, as the case may be, for and on behalf of the parties represented by them.

ECDSD Approval

ECDSD: Member of Executive Council: N Sihlwayi

31/March 2016.
Date

ECDSD Recommended

ECDSD: Superintendent General: S Khanyile

30/03/2016-
Date

B. Access Control Policy

I. Definition and Terms

Terms	Definition
i) Executive Management	this constitutes the Top Management of the Department
ii) Department	the Department of Social Development
iii) Access	a way of being able to use or gain entry in the system
iv) End user	the person utilising the information
v) Users	Users are the people who use the system
vi) Resources	Resources are objects in the system that needs to be protected
vii) Relationship	Relationships are optional conditions that exist between users and resources
viii)Actions	Actions are the activities that users can perform on the resources
ix) Remote sources	Any source externally that poses threat to the internal environment
x) Firewall	A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices that is configured to permit or deny network transmissions based upon a set of rules and other criteria.
xi) Router	A device used to connect, accept and transfer data packets from one Wide Area Network to the Local Area Network.
xii) Databases	This is a specialised software system that is used for managing highly structured data. Databases range from simple desktop systems to huge, multi-machine implementations.
xiii)Generic Accounts	are computing accounts set up for a specific purpose that can be accessed by multiple people. (Administrator, Guest Accounts)
Acronyms	
i) COBIT	Control Objectives for Information and Related Technology

ii) CIO	Chief Information Officer
iii) DSD	Department of Social Development
iv) GITO	Government Information Technology Officer
v) ICT	Information and Communication Technology
vi) IT	Information Technology
vii) ID	Identification
viii)DRP	Disaster Recovery Plan
ix) ITIL	Information Technology Information Library
x) SG	Superintendent General
xi) ISF	Information Security Forum
xii) MISS	Minimum Information Security Standard
xiii)SLA	Service Level Agreement
xiv) AG	Auditor General
xv) PC	Personal Computer
xvi) PDA	Personal Digital Assistant

II. Legislative Framework

i) Minimum Information Security Standard (MISS 1996)
ii) Public Finance Management Act (PFMA)
iii) Public Service Regulation (PSR 2008)
iv) Public Service Act (Act No. 103 of 1994)
v) Labour Relations Act (Act No.12 of 2002)
vi) ISO 27001:(2005)
vii) Electronic and Communication and Transaction Act (Act No. 25 of 2002)
viii) Regulation of Interception of Communication Act (Act No. 70 of 2002)
ix) Protection of Information Act (Act No. 84 of 1982)
x) Protection of Personal Information Act (Act no: 2013)
xi) CIO Governance Charter (May 2013)

1. Preamble

The policy has been in use since 2012 but was due for review and upon review it has been observed that the controls objectives are still relevant. These controls when tested by auditors were found to be found to be sound. The information of the Department of Social Development Eastern Cape is considered one of the most important assets.

The rapid development and progress in the area of computer technology add to the escalating threat in respect of information systems security, which calls for the establishment of security policies, standards and control measures to protect the information systems configurations and information of the ECDSD against security risks. This policy is based on international standards, best practices, South African government law, regulation and acts and is subject to the policies and standards as issued by National Intelligence regarding minimum information security standards

Executive management acknowledges the importance of the computing resources of the ECDSD and supports information systems security throughout the department.

2. Purpose

The purpose of this document is to authorise a group of users to perform a set of actions on a set of resources. Unless authorised through this policy, users have no access to any functions of the system

3. Objective

The objective of this access control policy is to minimize the risks to the ECDSD's assets that might arise from unauthorised access, from local as well as from remote sources.

4. Scope of Applicability

The policy applies to all business units, employees, contractors and any other resources requiring access to the ECDSD computing environment.

Computing environment includes:

a) physical and environmental; and

b) hardware, software, system and applications.

5. Principles and Values

Information security is more than just computer security. It also includes a wide range of physical security measures such as protecting your information assets against natural disasters or theft, and social engineering attacks such as someone tricking you giving out sensitive information. There are three basic principles of information security.

a) **Confidentiality:** means making sure that information is only seen by people who have the right to see it.
b) **Integrity:** means making sure that information remains intact and unaltered.
c) **Availability:** implies having access to your information when you need it.

6. Policy statements

6.1 Privileged access rights

a) The number of people having elevated rights shall be kept to a minimum;

b) A record shall be kept of the people having elevated rights;

c) Access to operating system commands shall be restricted to IT staff members, who are authorised to perform systems administration functions.

6.2 Review and monitoring of access

a) Access to IT resources shall be logged and monitored on a continuous basis;

b) Logs of access to critical business systems, network and application shall be kept, these logs should be:

   i. reviewed regularly to help identify suspicious or unauthorised activity by the password administrator;

   ii. retained for at least a three month period to be able to investigate past activities;

   iii. protected against unauthorised change.

c) A formal record of all registered users in the department shall be maintained and updated quarterly, clearly indicating appropriate access rights and/or privileges recorded in an access control register.

6.3 User registration and termination

a) Granting of access to generic accounts (service accounts) shall be strictly controlled;

b) Formal and documented user registration and termination procedures for granting and terminating access to all multi-user information systems and services shall exist. The user registration and termination procedures shall include as many of the following components as possible:

   i) It must be clearly stated who has the responsibility for the correct registration of a user's access rights;

   ii) Each user shall be assigned a unique user ID. Generic (i.e. non-personal) accounts shall be avoided wherever possible; all exceptions shall be authorised by the CIO;

   iii) A formal check that user has authorisation from the system owner for the use of the information system or service shall be performed;

   iv) A check that the level of access granted is appropriate to the business purpose and is consistent with the security policy and the security standards and does not violate segregation of duties;

v) Ensure that service providers are not provided access until authorisation procedures have been completed;

vi) Maintain a formal record of all persons registered to use the service;

vii) Promptly removing or re-evaluating access rights of users who have changed jobs or left the organisation;

viii) Periodically checking for, and disabling, redundant user IDs and accounts;

ix) Email accounts not accessed or inactive for 60 days will be disabled unless they are special accounts (for example staff on maternity leave);

x) Ensuring that redundant user IDs are not issued to other users;

xi) accounts for consultants, contractors and temporary employees shall be included in all new hire and termination processes that a department puts in place.

c) All ECDSD information systems privileges shall be promptly terminated at the time when an employee ceases to provide services to the department;

d) Access to the application and associated information shall be restricted to authorised individuals in order to ensure that only authorised individuals are granted access to the application, and that individual accountability is assured;

e) Users of application, systems or data should be:

i) authorised by the application/system/data owner;

ii) identified by a unique user ID;

iii) authenticated by a password;

iv) provided with the minimum functionality required to perform their role; and

v) revoked promptly when an individual user is no longer entitled to them such as when a user is transferred to another department/ directorate, terminates his/her services, the department terminates his/her services or is suspended by the department.

f) Any user who has access to departmental classified information and/or data record(s) or database(s) in any format, shall be subject to appropriate security clearance and duly complete the confidential agreement form and the application for user creation form to be kept safe by the business unit manager and another copy in his/her personnel file;

g) No employee or any user of the Department shall be given access to any other official(s), employee’s files, information, data or records stored and/or processed on his/her desktop/laptop and/or server without his/her consent. Access shall be deemed to be authorised only when it has been reduced to writing and has been signed and approved by the CIO or District Manager;

h) No IT staff member or any employee may remotely take over a user's computer without his/her permission;

i) When issuing new or changing passwords it shall be ensured that password policy is adhered to.

6.4 User access management

The allocation of access rights to users shall be strictly controlled through user registration and administration procedures, including special restrictions over the allocation of privileges and passwords, and regular access rights reviews.

6.5 User responsibilities

Users shall be made aware of their responsibilities towards choosing strong passwords and keeping them confidential. Systems shall be locked when left unattended (e.g. using password protected screensavers or key locks).

6.6 Network access control

a) Access to network services shall be controlled, both within the department and between departments. Enforced paths and network segregation may be appropriate (e.g. using fixed/predefined network routes, firewalls and proxy servers);

b) Remote users of the network and network nodes shall be suitably authenticated;

c) Remote diagnostic ports shall be securely controlled. Security attributes of all network services should be clearly described.

6.7 Operating system access control

Operating system security facilities and utilities shall be used appropriately.

6.8 Application access management

Application systems shall incorporate security controls to restrict unauthorized access. Sensitive systems may require dedicated/isolated platforms and special handling.

6.9 Monitoring system access and use

a) Systems shall be monitored for access policy violations and other security events such as use of privileges and alarms/exception conditions;

b) Logs and alarms shall be reviewed at a frequency relating to the level of risk. System clocks shall be synchronized.

6.10 Mobile computing and teleworking

There shall be formal policies covering the secure use of portable PCs, PDAs, cell phones etc., and secure teleworking ("working from home" and other forms of mobile working).

7. Approving Authority

The member of the Executive Council and the Superintendent General has the responsibility to approve the departmental Access Control Policy

8. Accountabilities and Responsibilities

8.1 The Superintendent General

The SG working in conjunction with the CIO shall be responsible for ensuring the effective implementation and compliance of the ECDSD policies, standards and procedures.

8.2 Asset/information/application owner

a) The designated owner of the information asset shall take responsibility for all access granted.

b) The owner of the information resource shall ensure that all access to the resource granted is appropriate and justified.

8.3 Information Security Manager

The Information Security Manager is also responsible for maintaining this policy.

8.4 Internal Audit

a) The Internal Audit department is authorised by management to assess compliance with all departmental policies at any time.

b) The Internal Audit department may assist with audits of outsourcing contracts including security compliance audits, and advise management on the risks and controls relating to access to ECDSD environment.

9. Effective date of the Policy

The Access Control Policy is effective upon the date the member of the Executive Council has approved it.

10. Monitoring Mechanisms

a) ICT Operational Committee

b) ICT Steering Committee

c) ICT Managers Meeting

The CIO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy. Such mechanisms as mentioned above shall be used to monitor this policy

11. Review of the Policy

The policy will be reviewed every three years and whenever there are new developments to maintain relevance.

12. Enforcement

a) Failure to comply with this policy shall result in disciplinary action.

b) Any conduct that interferes with the normal and proper operation of the departments IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved Access Control Policy.

c) The ECDSD executive management reserves the right to revoke the privileges of any user at any time until such time it is deemed fit to reinstate the rights.

13. Policy Recommendation and Approval

The signatories hereof, being duly authorised thereto, by their signatures hereto authorise the execution of the work detailed herein, or confirm their acceptance of the contents hereof and authorise the implementation/adoption thereof, as the case may be, for and on behalf of the parties represented by them.

ECDSD Approval

ECDSD: Member of Executive Council: N Sihlwayi

31/March 2016.
Date

ECDSD Recommended

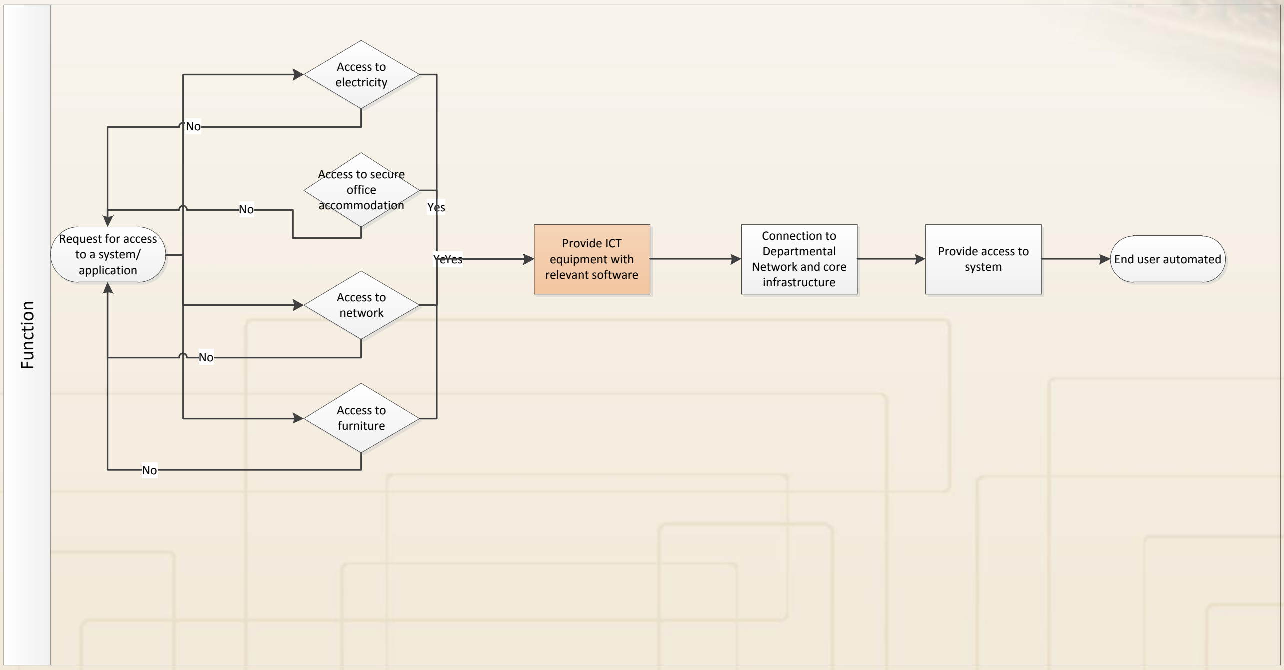
ECDSD: Superintendent General: S Khanyile

30/03/2016-
Date

Annexure A

Process flow diagram

This is to be developed and maintained on an annual basis.


Function
Request for access to a system/ application
Access to electricity
Access to secure office accommodation
Access to network
Access to furniture
No
No
No
No
Yes
YeYes
Provide ICT equipment with relevant software
Connection to Departmental Network and core infrastructure
Provide access to system
End user automated

C. Backup Policy

I. Definition and Terms

Terms	Definition
i) Archive	the process of **moving** inactive files from online disk storage to tape, i.e. deleting the files from disk after copying them, in order to release online storage for re-use
ii) Backup	the process of **copying** active files from online disk storage to tape so that files may be restored to disk in the event of damage to or loss of data
iii) Backup administrator	a person designated to perform the administration functions and maintenance of the backup solution
iv) Backup tape	the tape storage media where the information is to be stored for offline and/or offsite storage
v) File server	A device which controls access to separately stored files, as part of a multi-user system
vi) Firewall	A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices that is configured to permit or deny network transmissions based upon a set of rules and other criteria.
vii) Mail server	An application that receives incoming email from local users and forwards outgoing email for delivery
viii) Active Directory controllers	Server running a version of windows server operating system and has the service of active directory installed.
ix) Department	the Department of Social Development
x) End user	the person utilising the information
xi) Grandfather- Father- Son (GFS)	a tape rotation strategy. GFS simplifies tape handling by organizing rotation into daily, weekly, and monthly backup tapes. You can also create Custom backup jobs that use the GFS strategy
xii) Server	A computer or device on a network that manages network resources or provides services and resources to users.
Acronyms	
i) LAN	Local Area Network
ii) WAN	Wide Area Network
iii) CFO	Chief Financial Officer

iv) SG	Superintendent General
v) ECDSD	Social Development Eastern Cape
vi) IT	Information Technology
vii) ISO	International Standard of Operation

II. Legislative Framework

i) Minimum Information Security Standard (MISS)
ii) Public Finance Management Act (PFMA)
iii) Public Service Regulation (PSR 2008)
iv) Public Service Act (Act No. 103 of 1994)
v) Labour Relations Act (Act No.12 of 2002)
vi) ISO 27001: (2005)
vii) Electronic and Communication and Transaction Act (Act No. 25 of 2002)
viii) Regulation of Interception of Communication Act (Act No. 70 of 2002)
ix) Protection of Information Act (Act No. 84 of 1982)
x) Protection of Personal Information (Act No 4 of 2013)
xi) Disaster Recovery Policy (2016)
xii) Disaster Recovery Plan (2016)
xiii) CIO Charter (2013)

1. Preamble

The policy has been in use since 2012 but was due for review as it was in its third year of implementation. This document provides a standard guideline to ensure that Department of Social Development data can be fully recovered in case of accidental, intentional corruption or deletion. The most fundamental aspect of storage management is therefore the access, backup and recovery process. Managing huge quantities of diverse data, widely distributed across the enterprise is a daunting task. Technology, when integrated into a comprehensive data and business recovery strategy, can reduce the risk of data loss and reduce the cost of data recovery and downtime.

The rapid development and progress in the area of computer technology add to the escalating threat in respect of information systems security, which calls for the establishment of security policies, standards and control measures to protect the information systems configurations and information of the ECDSD against security risks. This policy is based on international standards, best practices, South African government law, regulation and acts and is subject to the policies and standards as issued by National Intelligence regarding minimum information security standards

Executive management acknowledges the importance of the computing resources of the ECDSD and supports information systems security throughout the department. This policy should be read in conjunction with the Disaster Recovery Plan and Policy.

2. Purpose

This document is to define and provide a framework for managing data storage and focusing on efficient and dependable archival, preservation and retrieval of information leveraged by applications and employees of the Department of Social Development.

3. Objective

a) This document provides a standard guideline to ensure that Department of Social Development data can be fully recovered in case of accidental, intentional corruption or deletion.

b) Provide proper controls and management systems that will ensure effective, efficient and economical use of the ECDSD's information.

4. Scope of Applicability

This policy applies to the backup administrator who administer any ECDSD-owned internal network domain servers or otherwise.

5. Principles and Values

Information security is more than just computer security. It also includes a wide range of physical security measures such as protecting departmental information assets against natural disasters or theft, and social engineering attacks such as someone tricking you giving out sensitive information. There are three basic principles of information security

a) **Confidentiality:** means making sure that information is only seen by people who have the right to see it.
b) **Integrity:** means making sure that information remains intact and unaltered.
c) **Availability:** implies having access to your information when you need it.

6. Policy Provisions

The policy seeks to provide the following provision:

a) Controls shall be established that must ensure proper management of risks associated with ownership and safeguarding of information which includes:

   i) implement and enforce storage of department approved information on enterprise computers and servers. This ensures that data such as music files, and picture files, do not take space on enterprise storage facilities;

   ii) enforce centralised storage of documents on LAN servers (preferably with offline folder synchronisation for mobile laptops) to facilitate centralised data backup; and

   iii) implement a well-documented tape rotation system to safeguard against accidental overwriting of tapes.

b) Advanced scheduling, automated unattended operation, centralised reporting, and enterprise-wide media management shall be performed;

c) high-performance backup and restore features that reduce the backup window shall be implemented to improved availability of data;

d) Ensure that backup procedures adhere to international standards and procedures;

e) Ensure that in the event of a disaster, backup files can be recovered:

   i) implement scheduled unattended but auditable backup systems that allow operation when network traffic on the enterprise network is at a minimum; and

   ii) implement a backup solution that minimises the recovery time for information by allowing selective restoration.

g) Ensure data integrity at all times by monthly testing the backed up information;

h) Ensure offsite storage is maintained at all times to enable recovery of information should a disaster occur (onsite) due to fire, floods or other causes;

i) Ensure that backup tapes/cassettes are labelled according to the prescribed procedures:

   i) implement a regularly scheduled data restoration exercise to ensure back media is recoverable; and

   ii) keep backups on storage tape offsite to avoid being destroyed should a disaster occur onsite.

j) Ensure all changes to strategy, policy and procedures are properly authorised and documented:

   i) maintain a change control register to record all changes to the policy and procedures; and

   ii) ensure the correct authorisation is obtained prior to effecting any changes.

6.1 Tape Storage

a) There shall be a separate or set of tapes for each backup day including Monday, Tuesday, Wednesday, and Thursday;

b) Backups performed Monday through Thursday shall be kept for one week and used again the following appropriate day of the week;

c) There shall be a separate or set of tapes for each Friday of the month such as Friday1, Friday2, etc.

d) Backups performed on Friday or weekends shall be kept for one month and used again the next month on the applicable Friday.

e) Every month a monthly backup tape shall be made using the oldest backup tape or tape set from the tape sets or archived as the monthly backups and for each Fridays a new set of tapes used.

6.2 Tape Drive Cleaning

a) Tape drives shall be cleaned weekly and the cleaning tape shall be changed according to manufacture specification.

6.3 Age of tapes

a) The date each tape was put into service shall be recorded on the tape. Tapes that have been used longer than six months shall be discarded and replaced with new tapes.

6.4 Data to be Backed Up

Data to be backed up include the following information:

   a) Official User data residing on official laptops and desktops.

Systems to be backed up include but are not limited to:

   a) File server;

   b) Mail server;

   c) Production database server;

   d) Active Directory controllers;

6.5 Constraints and special considerations

a) Tape devices will be required at remote servers to cater for remote servers for local remote server backup;

b) Offline folder synchronisation for desktops and laptops is required to facilitate local remote data centralisation for remote sites;

c) **Firewall:** care must be taken to ensure the backup traffic is allowed through.

7 Approving Authority

The member of the Executive Council and the Superintendent General has the responsibility to approve the departmental Backup Policy

8 Accountabilities and Responsibilities

8.1 The Superintendent General

The SG working in conjunction with the CIO shall be responsible for ensuring the effective implementation and compliance of the ECDSD policies, standards and procedures.

8.2 Asset/information/application owner

c) The designated owner of the information asset shall take responsibility for all access granted.

d) The owner of the information resource shall ensure that all access to the resource granted is appropriate and justified.

8.3 Data Warehouse Manager

The Data Warehouse Manager is also responsible for maintaining this policy.

8.4 Internal Audit

c) The Internal Audit department is authorised by management to assess compliance with all departmental policies at any time.

d) The Internal Audit department may assist with audits of outsourcing contracts including security compliance audits, and advise management on the risks and controls relating to access to ECDSD environment.

8.5 Backup admin

The backup administrators' responsibilities are to:

a) swap the tapes;

b) transfer tapes to offsite storage as per the tape rotation policy;

c) check backup job status;

d) complete the Backup Log daily;

e) ensure that backup and storage logs are maintained;

f) escalate backup issues;

g) ensure that all tapes are write-enabled before inserting into the tape drive;

h) ensure that all tapes are marked properly, i.e. with the name of the type of backup, as well as the date when the tape is used for backup and the save set name is written into the backup logbook next to the appropriate tape;

i) on completion of a backup, the operator must enter the backup date and tape numbers onto the Backup Logbook as well as the backup on the label supplied in tape's case; and

j) store backup tapes in a safe before they are collected to be stored off site.

Failure to execute the above responsibilities must be viewed as negligence and can result in severe data loss.

9 Effective date of the Policy

The Backup Policy is effective upon the date the member of the Executive Council has approved it.

10 Monitoring Mechanisms

a) ICT Operational Committee

b) ICT Steering Committee

c) VEEAM Backup System

The CIO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy. Such mechanisms as mentioned above shall be used to monitor this policy:

11 Review of the Policy

The policy will be reviewed every three years and whenever there are new developments to maintain relevance.

12 Enforcement

a) Failure to comply with this policy shall result in disciplinary action.

b) Any conduct that interferes with the normal and proper operation of the departments IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved Access Control Policy.

c) The ECDSD executive management reserves the right to revoke the privileges of any user at any time until such time it is deemed fit to reinstate the rights.

d) ensure that backup and storage logs are maintained;

e) escalate backup issues;

f) ensure that all tapes are write-enabled before inserting into the tape drive;

g) ensure that all tapes are marked properly, i.e. with the name of the type of backup, as well as the date when the tape is used for backup and the save set name is written into the backup logbook next to the appropriate tape;

h) on completion of a backup, the operator must enter the backup date and tape numbers onto the Backup Logbook as well as the backup on the label supplied tape's case; and

i) store backup tapes in a safe before they are collected to be stored off site.

Failure to execute the above responsibilities must be viewed as negligence and can result in severe data loss.

13 Policy Recommendation and Approval

The signatories hereof, being duly authorised thereto, by their signatures hereto authorise the execution of the work detailed herein, or confirm their acceptance of the contents hereof and authorise the implementation/adoption

ECDSD Approval

_______________________________ 31/March 2016.
ECDSD: Member of Executive Council: N Sihlwayi Date

ECDSD Recommended

_______________________________ 30/03/2016.
ECDSD: Superintendent General: S Khanyile Date

Annex A : Procedures for backup

A.1 Backup schedule and tape rotation

The ECDSD's backup solution uses a four-daily, four-weekly and one-monthly Grandfather-Father-Son data retention cycle. A **Grandfather-Father-Son** rotation scheme must be operated; incremental daily backups *(Son)* must run overnight from Monday to Thursday and must be rotated on a three or four week basis. A full weekly backup (the **Fathers**) must run on Fridays of each week and one full backup per month (the **Grandfather**) must run and be kept for 12 months.

The following data retention cycle must be used when performing backups:

1. Daily GFS data retention cycle:
   - i) ***Server/application/database*-MON-DATE**
   - ii) ***Server/application/database* -TUE-DATE**
   - iii) ***Server/application/database* -WED-DATE**
   - iv) ***Server/application/database* -THU-DATE**

b) Weekly GFS data retention cycle:
   - i) **Week1 – *Server/application/database* -FRI-DATE**
   - ii) **Week2 – *Server/application/database* -FRI-DATE**
   - iii) **Week3 – *Server/application/database* -FRI-DATE**
   - iv) **Week4 – *Server/application/database* -FRI-DATE**
   - v) **Week4 – *Server/application/database* -FRI-DATE**
   - vi) **Week5 – *Server/application/database* -FRI-DATE**

c) 12-monthly GFS data retention cycle:
   - i) **January09 - *Server/application/database* -JAN-DATE**
   - ii) **February09 - *Server/application/database* -FEB-DATE**
   - iii) **March 09 till - *Server/application/database* -MAR-DATE**
   - iv) **December09 - *Server/application/database* -DEC-DATE**

During week one, the Week1 set is used and during week two, Week2 set is used and so on.

<u>The following schedule is used for daily and weekly tape rotation</u>:

Monday (or first business day of the week):

Deliver the previous week's **weekly tape** to the offsite storage facility and collect the oldest set of weekly tapes, e.g. (if you were using Week1 last week you need to send the tapes to the offsite storage and bring the Week2 tapes to the offices).

Make sure that you run a device inventory once the tape has been inserted into the Tape library.

Place the old weekly set in the fire-proof safe and insert new weekly's tape in the tape library. Your tape is now ready for the backup in the evening of that day.

Also note that all daily tapes and 2 spare tapes must be kept in the tape library and these can be changed over a longer period of time. Weekly tapes must be changed

every Monday of the week and monthly Tapes must be changed every first Monday of the Month at 10h00 am.

It is therefore preferable to do this in the morning so that it becomes a routine. Backups only run at 19:00 so that all data for the day is captured on the tapes.

<u>The following schedule is used for monthly tape rotation</u>:

The tapes in this must be labelled:

January

February

March

April

May

June

July

August

September

October

November

December

On the last business day of the month, the daily or weekly backup tape must not be used. Instead use the monthly tape corresponding with the month that you are in. This tape must be taken to the offsite storage as soon as possible. **Note: These tapes should never be kept onsite; they can only be used for emergency recovery.**

A.2 Checking backup job and completion of backup log

As part of the daily backup job the tape will be ejected from the Tape drive into the Tape library after the backup has completed. If the tape has not ejected by 08:00 in the morning there could be an issue with the backups; notify the backup administrators.

Backup job status will be e-mailed to the backup administrators immediately after the job completion. This e-mail is to be used to complete the backup log as it will have information on whether the backup job completed successfully or failed. A detailed log file will also be attached to the e-mail.

The technicians are not allowed to modify any jobs; it is the responsibility of the backup administrators to modify backup scripts. The log file can be forwarded to the backup administrator who will be able to identify the cause of the failed/incomplete backup.

Backup administrators must make sure that each backup tape is labelled stating the specific backup name and serial number. Both the tape and case must be labelled and it is the responsibility of the backup administrator to replace broken or faulty tapes. He/she must also make sure that all backup logs are analysed and resolved if there are any backup issues that are reported.

There are four types of backups logs that the ECDSD will be utilising, viz.

Backup log: This log must be created and maintained by the backup software and stored on the backup tape and on the hard drive. The Backup Log is used to monitor the swapping of tapes and the status of the backups. This needs to be completed every morning when the tapes are swapped. The log file must also be printed and kept in a file in the fire-proof safe. A page will exist for every month and the backups are logged against the sheet.

Error log: This log must be created and maintained by the backup software and stored on the backup tape and on the hard drive.

Backup Restore Log: This log will be created and maintained by the backup software and stored on the backup tape and on the hard drive.

Backup Storage Log: A logbook will be kept at the on-site and off-site storage location. The following backup schedule must be adhered to.

Monday	Tuesday	Wednesday	Thursday	Friday
Daily backups	Daily backups	Daily backups	Daily backups	Full weekly backup
Daily backups	Daily backups	Daily backups	Daily backups	Full weekly backup
Daily backups	Daily backups	Daily backups	Daily backups	Full weekly backup
Daily backups	Daily backups	Daily backups	Daily backups	Full weekly backup

The following is an example of the backup log.

ECDSD Backup Log				Month/Year:		
DATE	TAPE NAME	Tape Serial#	JOB STATUS	ON FAILED/INCOMPLETE STATUS; WHAT ACTION WAS TAKEN	BACKUP ADMIN	SIGNATURE

This log must be completed and signed by the relevant Backup Admin as a log to the completion of the backups. The updates to this log are just as critical as the tapes being swapped and are used when recovery of data is required.

A.3 Backup admin responsibilities and delegation

The backup administrators' responsibilities are to:

a) swap the tapes;

b) transfer tapes to offsite storage as per the tape rotation policy;

c) check backup job status;

d) complete the Backup Log daily;

D. Change Management Policy

I. Definition and Terms

Terms	Definition
i) Executive Management	this constitutes the Top Management of the Department
ii) Department	the Department of Social Development
iii) Change	any transition or substitution within the environment
iv) ICT Change Management Board	Committee appointed by Superintendent General to deal with all the change request in the ICT environment from system owners
v) Change Management Log	A category and detail list of all the requested changes in the ICT environment.
vi) End user	the person utilising the information
Acronyms	
i) COBIT	Control Objectives for Information and Related Technology
ii) CIO	Chief Information Officer
iii) ECDSD	Department of Social Development
iv) GITO	Government Information Technology Officer
v) ICT	Information and Communication Technology
vi) IT	Information Technology
vii) DRP	Disaster Recovery Plan
viii) ITIL	Information Technology Information Library
ix) SG	Superintendent General
x) ISF	Information Security Forum
xi) MISS	Minimum Information Security Standard
xii) SLA	Service Level Agreement
xiii) AG	Auditor General

II. Legislative Framework

i) Labour Relations Act (Act No.12 of 2002)
ii) Control of Access to Public Premises Act (Act No. 53 of 1985)
iii) Minimum Information Security Standard (1996)
iv) Public Finance Management Act (Act No. 105 of 1999)
v) Occupational Health and Safety Act (Act No. 85 of 1993)
vi) Promotion of Access to Information Act (Act No. 2 of 2000)
vii) State Information Technology Act (Act No. 88 of 1998)
viii) CIO Charter (2013)

1. Preamble

The policy has been in use since 2012 but was due for review and upon review it has been observed by policy implementers that the controls objectives are still relevant. Change Management is the process of planning, coordinating, implementing and monitoring changes affecting any production platform within Information Technology's control. The information of the Department of Social Development Eastern Cape is considered one of the most important assets.

The rapid development and progress in the area of computer technology add to the escalating threat in respect of information systems security, which calls for the establishment of security policies, standards and control measures to protect the information systems configurations and information of the ECDSD EC against security risks. This policy is based on international standards, best practices, South African government law, regulation and acts and is subject to the policies and standards as issued by National Intelligence regarding minimum information security standards.

Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the end user community and to increase the value of Information Resources. This document is applicable to the Department of Social Development Eastern Cape and defines management intent in managing changes to the ICT environment to ensure that all change to this environment are authorised and do not comprise the availability, confidentiality and integrity of the department information and systems.

2. Purpose

The purpose of the Change Management Policy is to manage changes in a standardise and predictable manner so that staff and clients can plan accordingly.

3. Objectives

The objectives of the Change Management process are to:

a) ensure that changes are made with minimum disruption to the services IT has committed to its end users,

b) support the efficient and prompt handling of all changes,

c) provide accurate and timely information about all changes,

d) ensure all changes are consistent with business and technical plans and strategies,

e) ensure that a consistent approach is used,

f) provide additional functionality and performance enhancements to systems while maintaining an acceptable level of end user services,

g) reduce the ratio of changes that need to be backed out of the system due to, inadequate preparation,

h) ensure that the required level of technical and management accountability is, maintained for every change,
i) monitor the number, reason, type, and associated risk of the changes.

4. Scope of Applicably

ECDSD Change Management Policy applies to all individuals that install, operate or maintain Information Resources within the department.

It includes the management of any installation or alteration to hardware, network, system or application software, procedure or environmental facilities which adds to, deletes from or modifies the service delivery environment.

5. Principles and Values

Information security is more than just computer security. It also includes a wide range of physical security measures such as protecting your information assets against natural disasters or theft, and social engineering attacks such as someone tricking you giving out sensitive information. There are three basic principles of information security

d) **Confidentiality:** means making sure that information is only seen by people who have the right to see it.
e) **Integrity:** means making sure that information remains intact and unaltered.
f) **Availability:** implies having access to your information when you need it.

6. Policy statements

The department shall adhere to the following provisions:

a) every change to ECDSD Information Resources resource such as: operating systems, computing hardware, networks, and applications is subject to the Change Management Policy and shall be performed according to the Change Management Procedures,

b) the change management procedure shall ensure that proposed changes are reviewed for relevancy and impact (business, technical and financial),

c) the change management procedure will be formally defined, documented and adhered to,

d) all changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) need to be reported to or coordinated with the leader of the change management process,

e) an ICT Change Management Board, appointed by CIO, shall meet as stipulated in the CIO Charter to review change requests and to ensure that change reviews and communications are being satisfactorily performed,

f) a formal written change request shall be submitted for all changes, both scheduled and unscheduled,

g) all scheduled change requests shall be submitted in accordance with change management procedures so that the ICT Change Management Board has time to review the request, determine and review potential failures, and make the decision to allow or delay the request,

h) each scheduled change request must receive formal Change Management Board approval before proceeding with the change,

i) the appointed leader of the Change Management Board may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning,

j) inadequate backup plans, the timing of the change will negatively impact a key business process such as year-end accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events.

k) Changes are to be fully tested in an isolated, controlled and representative environment, and approved before being implemented,

l) Any software change and/or update will be controlled with version control,

m) Using live data for testing new system or system changes may only be permitted where adequate controls for the security of the data are in place,

n) Data is to be protected against unauthorised or accidental changes,

o) Fallback procedures for aborting and recovering from unsuccessful changes will be documented and tested,

p) Emergency changes will be authorized and recorded,

q) Disaster recovery plans will be updated with relevant changes and managed through the change control process,

r) Information resources documentation will be updated when each change is complete and old documentation will be archived or disposed of according to the documentation and data retention policies,

s) Customer notification must be completed for each scheduled or unscheduled change following the steps contained in the Change Management Procedures,

t) A Change Review must be completed for each change, whether scheduled or unscheduled, and whether successful or not,

u) all ECDSD information systems must comply with an Information Resources change management process that meets the standards outlined above,

v) the integrity of general use software, utilities, operating systems, networks, and respective data files are the responsibility of the custodian department. Data for test and research purposes must be de-personalized prior to release to testers unless each individual involved in the testing has authorized access to the data,

w) all changes or modifications to MIS systems, networks, programs or data must be approved by the system owners who are responsible for their integrity.

7. Approving Authority

The member of the Executive Council and the Superintendent General has the responsibility to approve the departmental Change Management Policy

8. Accountabilities and Responsibilities

8.1 The Superintendent General

The SG in conjunction with CIO shall implement, enforce and monitor the controls in accordance with the requirements outlined by management, and must advise end users on the correct ways to access information and systems.

8.2 All employees

All employees are responsible for complying with this and other change management policy at all times. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of acceptable behaviour) to comply with our information security policies.

8.3 Information systems owners

Responsible for analysing and form part of the committee approving all changes that affect the system they are responsible for.

8.4 Information security manager

The information security officer is responsible for maintaining this policy and generally advising on information security controls. Working in conjunction with other department functions, is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy.

8.5 Internal Audit

The Internal Audit department is authorised by management to assess compliance with all department policies at any time as per the audit plan.

9 Effective date of the Policy

The Change Management Policy is effective from the date the member of the Executive Council has approved this policy

10 Monitoring Mechanisms

e) ICT Operational Committee

f) ICT Steering Committee

g) ICT Managers Meeting

The CIO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy. Such mechanisms as mentioned above and in line with the CIO charter shall be used to monitor this policy.

11 Review of the Policy

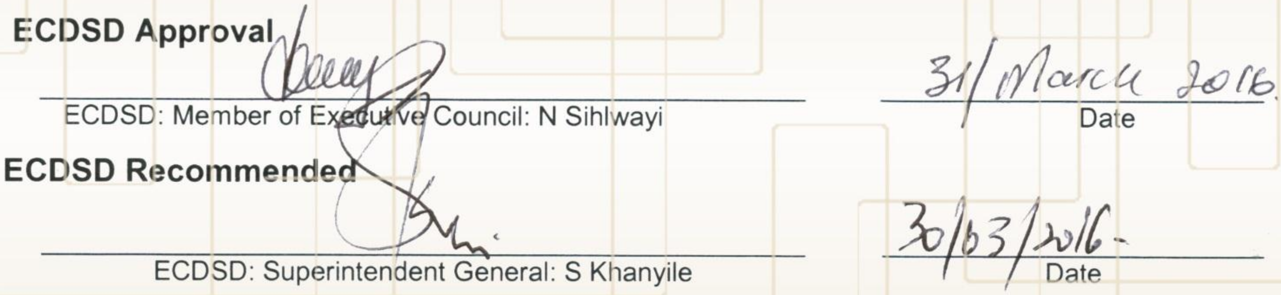
The policy will be reviewed every three years and whenever there are new developments to maintain relevance.

12 Enforcement

a) Failure to comply with this policy shall result in disciplinary action.
b) Any conduct that interferes with the normal and proper operation of the departments IT systems, which adversely affects the ability of other users to use those IT systems,
c) or which is harmful or offensive to other end users, shall constitute violation of this approved Policy.
d) The ECDSD executive management reserves the right to revoke the privileges of any user at any time until such time it is deemed fit to reinstate the rights.

13 Policy Recommendation and Approval

The signatories hereof, being duly authorised thereto, by their signatures hereto authorise the execution of the work detailed herein, or confirm their acceptance of the contents hereof and authorise the implementation/adoption thereof, as the case may be, for and on behalf of the parties represented by them



ECDSD Approval

ECDSD: Member of Executive Council: N Sihlwayi

31/March 2016.
Date

ECDSD Recommended

ECDSD: Superintendent General: S Khanyile

30/03/2016-
Date

E. E-mail Policy

I. Definition and Terms

Terms	Definition
i) Executive Management	this constitutes the Top Management of the Department
ii) Department	the Department of Social Development
iii) Electronic Communications	Any Communications via email, fax, telephone and internet
iv) End user	the person utilising the information
v) Encryption	Turning of sensitive information into unintelligible data
vi) Outbound-email	email sent outside the department
vii) Inbound-email	email coming in the department
viii)Third party e-mail	Any email system that is not sanctioned by the department as the official communication tool.
Acronyms	
i) E-mail	Electronic Mail
ii) CIO	Chief Information Officer
iii) ECDSD	Department of Social Development
iv) GITO	Government Information Technology Officer
v) ICT	Information and Communication Technology
vi) IT	Information Technology
vii) ISP	Internet Service Provider
viii)iOS	Internet Operating System
ix) SG	Superintendent General

II. Legislative Framework

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

ii) The Protection of Information Act, 1982 (Act no. 84 of 1982)

iii) The State Information Technology Act, 1998 (Act no. 88 of 1998)

iv) SABS/ISO 17799 (2005)

v) Minimum Information Security Standards (MISS 1996)

vi) Guidelines for the Handling of Classified Information (SP/2/8/1)

vii) Electronic Communications and Transaction Act, 2002 (Act no. 25 of 2002)

1. Preamble

The policy has been in use since 2012 but was due for review and upon review it was identified that there were gaps on the issue of the access and maintenance of email accounts. E-mail is perhaps the most important means of communication throughout the business world. Messages can be transferred quickly and conveniently across our internal network and globally via the public Internet. However, there are risks associated with conducting business via e-mail. E-mail is not inherently secure, particularly outside the department's own internal network. Messages can be intercepted, stored, read, modified and forwarded to anyone, and do sometimes go missing. Casual comments may be misinterpreted and lead to contractual or other legal issues. The purpose of this document is to define and distinguish acceptable/appropriate from unacceptable/inappropriate use of e-mail within the Department of Social Development – Eastern Cape.

2. Purpose

This policy defines and distinguishes acceptable/appropriate from unacceptable/inappropriate use of electronic mail (e-mail).

3. Objective

a) The objective of this policy is to ensure the proper use of Social Development's email system and make officials aware of what Social Development deems as acceptable and unacceptable use of its email system. Social Development reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

4. Scope of Applicability

This is a standard corporate policy that applies throughout the organisation as part of the corporate governance framework. It applies to all users of the corporate e-mail systems.

5. Principles and Values

Information security is more than just computer security. It also includes a wide range of physical security measures such as protecting your information assets against natural disasters or theft, and social engineering attacks such as someone tricking you giving out sensitive information. There are three basic principles of information security

a) **Confidentiality:** means making sure that information is only seen by people who have the right to see it.
b) **Integrity:** means making sure that information remains intact and unaltered.
c) **Availability:** implies having access to your information when you need it.

6. Policy statements

6.1 Do not use e-mail:

i) to send confidential/sensitive information, particularly over the Internet, unless it is first encrypted by an encryption system approved by Information Security;

ii) no one is allowed to send to everyone group or to any distribution groups using his or her personal email.

iii) to create, send, forward or store e-mails with messages or attachments that might be illegal or considered offensive by an ordinary member of the public i.e. sexually explicit, racist, defamatory, abusive, obscene, derogatory, discriminatory, threatening, harassing or otherwise offensive;

iv) to commit the department to a third party for example through purchase or sales contracts, job offers or price quotations, unless you are explicitly authorised by management to do so (principally staff within Procurement and HR). Do not interfere with or remove the standard corporate e-mail disclaimer automatically appended to outbound e-mails;

v) for private or charity work unconnected with the department's legitimate business;

vi) in ways that could be interpreted as representing or being official public statements on behalf of the department, unless you are a spokesperson explicitly authorised by management to make such statements;

vii) to send a message from anyone else's account or in their name (including the use of false 'From:' addresses); if authorised by the manager, a secretary may send e-mail on the manager's behalf but should sign the e-mail in his/her own name per pro ('for and on behalf of') the manager;

viii) Do not forward e-mail without acquiring permission from the sender;

ix) to send any disruptive, offensive, unethical, illegal or otherwise inappropriate matter, including offensive comments about race, gender, colour, disability, age, sexual orientation, pornography, terrorism, religious beliefs and practice, political beliefs or national origin, hyperlinks or other references to indecent or patently offensive websites and similar materials, jokes, chain letters, virus warnings and hoaxes, charity requests, viruses or other malicious software; and

x) for any other illegal, unethical or unauthorised purpose.

6.2Employees are to:

1) Send all their correspondences for everyone to communic@ececdsd.gov.za,
2) Use the official email system for their official correspondences;
3) Send emails with signatures as approved by communications directorate
4) Always send emails with a relevant subject

5) Send emails clearly stating what action is expected from the recipient after receiving the email;
6) Send email Messages including attachment/s which not exceed 5MB in size;

7) Only mark emails as important if they really are important;
8) Answered all emails within at least 8 working hours, but users shall answer priority emails immediately.
9) Understand that Departmental e-mail services are provided to serve operational and administrative purposes in connection with the business. All e-mails processed by the department's IT systems and networks are considered to be the organisation's property.

6.3Employees shall take heed that:

a) ECDSD electronic communications systems generally shall be used only for business activities. Employees are reminded that the use of corporate resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.

b) 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.

c) Apply your professional discretion when using e-mail, for example abiding by the generally accepted rules of e-mail etiquette. Review e-mails carefully before sending them, especially formal communications sent to external parties.

d) Employees shall not unnecessarily disclose potentially sensitive information in "out of office" messages.

e) E-mails on the department IT systems are automatically scanned for malicious software, spam and unencrypted proprietary or personal information. Unfortunately, the scanning process is not 100% effective (e.g. compressed and encrypted attachments may not be fully scanned), therefore undesirable/unsavoury e-mails are sometimes delivered to users. Delete such e-mails or report them as security incidents to IT Help/Service Desk in the normal way.

f) Except when specifically authorised by management or where necessary for IT system administration purposes, employees shall not intercept, divert, modify, delete, save or disclose e-mails.

g) Limited personal use of the department e-mail systems is permitted at the discretion of local management provided always that it is incidental and occasional, and does not interfere with business. Employees should have no expectations of privacy, all e-mails traversing the department systems and networks are subject to automated scanning and may be quarantined and/or reviewed by authorised employees.

h) Employees shall not use Gmail, Hotmail, Yahoo or similar external/third-party e-mail services (commonly known as "Webmail") for business purposes. Do not forward or auto-forward corporate e-mail to external/third party e-mail systems. You may access your own Webmail via corporate IT facilities at local management discretion provided that such personal use is strictly limited and is not considered private

i) Be reasonable about the number and size of e-mails you send and save. Periodically clear out your mailbox, deleting old emails that are no longer required and filing messages that need to be kept under appropriate e-mail folders.

j) It is the user's responsibility to make sure that he/she frequently backs-up and or archives his/her emails.

k) User's email addresses will be created using their names and surname as they appear in their identity documents or their commonly known-by names and a surname as it appears in their identity documents.

l) Email accounts not accessed within 60 days will be disabled

m) Email accounts will be disabled within 30 days of termination of employment.

7. Approving Authority

The member of the Executive Council and the Superintendent General has the responsibility to approve the departmental E-mail Policy

8. Accountabilities and Responsibilities

8.1The Superintended General

a) The SG in conjunction with the CIO shall implement, enforce and monitor the controls in accordance with the requirements outlined by management, and must advise users on the correct ways to access information and systems.

b) Responsible for building, configuring, operating and maintaining the corporate e-mail facilities (including anti-spam, antimalware and other e-mail security controls) in accordance with this policy.

c) Responsible for assisting users with secure use of e-mail facilities, and acts as a focal point for reporting e-mail security incidents.

8.2 All employees

All employees are responsible for complying with this and other corporate policies at all times. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of acceptable behaviour) to comply with our information security policies.

8.3 Information security manager

The information security manager is responsible for maintaining this policy and generally advising on information security controls. Working in conjunction with other corporate functions, it is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy.

8.4 Internal Audit

The Internal Audit department is authorised by management to assess compliance with all corporate policies at any time.

9. Effective date of the Policy

The Email Policy is effective from the date the member of the Executive Council has approved this policy

10. Monitoring Mechanisms

a) ICT Operational Committee

b) ICT Steering Committee

c) System Centre Configuration Manager

The CIO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy. Such mechanisms as mentioned above shall be used to monitor this policy.

11. Review of the Policy

a) The policy document shall be reviewed in every three years to ensure relevance. Where the policy is materially revised, this shall be published before the end of the third quarter of the financial year to ensure proper planning is in place to address any misalignment in the activities.

12. Enforcement

a) Failure to comply with this policy shall result in disciplinary action.

b) Any conduct that interferes with the normal and proper operation of the departments IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved Access Control Policy.

c) The ECDSD executive management reserves the right to revoke the privileges of any user at any time until such time it is deemed fit to reinstate the rights.

13. Policy Recommendation and Approval

The signatories hereof, being duly authorised thereto, by their signatures hereto authorise the execution of the work detailed herein, or confirm their acceptance of the contents hereof and authorise the implementation/adoption thereof, as the case may be, for and on behalf of the parties represented by them.

ECDSD Approval

ECDSD: Member of Executive Council: N Sihlwayi

31/ March 2016.
Date

ECDSD Recommended

ECDSD: Superintendent General: S Khanyile

30/03/2016-
Date

F. ICT Equipment Policy

I. Definition and Terms

Terms	Definition
i) Executive Management	this constitutes the Top Management of the Department
ii) Department	the Department of Social Development
iii) Electronic Communications	Any Communications via email, fax, telephone and internet
iv) End user	the person utilising the information
Acronyms	
i) CCTV	Closed-Circuit Television
ii) CIO	Chief Information Officer
iii) DSD	Department of Social Development

iv) GITO	Government Information Technology Officer
v) ICT	Information and Communication Technology
vi) IT	Information Technology
vii) ISP	Internet Service Provider
viii)iOS	Internet Operating System
ix) SG	Superintendent General

II. Legislative Framework

i) The Promotion of Access to Information Act, 2000 (Act no. 2 of 2000)
ii) The Protection of Information Act, 1982 (Act no. 84 of 1982)
iii) The State Information Technology Act, 1998 (Act no. 88 of 1998)
iv) SABS/ISO 17799 (2005)
v) Minimum Information Security Standards (MISS 1996)
vi) Guidelines for the Handling of Classified Information (SP/2/8/1)
vii) Electronic Communications and Transaction Act, 2002 (Act no. 25 of 2002)

1. Preamble

The policy has been in use since 2012 but was due for review and upon review the existing controls objectives were still relevant. The department has opted not to outsource the repairs of out of warranty ICT user equipment in the future. This is due to cost cutting measures that the department has embarked on and upskill the internal staff. In light of this decision, secure ICT workshops must be established throughout the province to ensure timely repairs to ICT user equipment. Breakdown of working ICT Equipment can have a negative effect on IT and affect the delivery of services in an adverse manner. It is therefore imperative that there are contingency plans in place to circumvent the risk of unplanned downtime. The long-term purpose of the policy is to provide controls for management and monitoring of these workshops

2. Purpose

The purpose of this document is to define and distinguish policies and procedures of how ICT workshop should established, controlled and managed properly within the ECDSD.

3. Objective

a) The objective of the ICT workshop policy is to ensure the establishment of functional and secure ICT workshops throughout the province.

4. Scope of Applicability

The policy applies to all ICT engineering employees and contracted technicians that require access the ICT workshops.

5. Principles and Values

Information security is more than just computer security. It also includes a wide range of physical security measures such as protecting your information assets against natural disasters or theft, and social engineering attacks such as someone tricking you giving out sensitive information. There are three basic principles of information security

a) **Confidentiality:** means making sure that information is only seen by people who have the right to see it.
b) **Integrity:** means making sure that information remains intact and unaltered.
c) **Availability:** implies having access to your information when you need it.

6. Policy Provision

6.1 Establishment of workshops

1) At least one ICT workshop must be established in each of the districts and at head office.
2) Minimum requirements for an ICT workshops:
   a) A secure lockable room that will be used exclusively as an ICT workshop.
   b) Lockable cabinets or cages must be available for the storage of replacement components.
   c) Adequate tools and testers must be available for the disassembly/assembly of ICT equipment and the test there of.
   d) Network connectivity must be provided for testing of equipment and software.
3) Trained technicians must attend to the repairs of ICT user equipment.

6.2 Access to and security in ICT workshops

A great risk of theft is associated the ICT workshops therefore great care must be taken to restrict access to the workshops and cabinets where components are stored. The following security measures must be implemented in all of the ICT workshops:

1) The entrances to the ICT workshop must be locked at all times.
2) Lockable gates must be installed in all entrances and burglar proofing in all windows.
3) Mechanisms must be put in place to identify individuals before entering the workshop.
4) CCTV must be installed inside and outside all ICT workshops.
5) Registers must be kept of all equipment and components booked into and out of the workshop, these registers and stock level must be verified at least once per week.
6) All cabinets where components are stored must be locked and only the ICT manager may issue replacement components. All components issued must be recorded in a register before it's installed.
7) Only individuals that are approved by the ICT Steering may access the ICT workshops.

6.3 Replacement components

To ensure that the hardware workshops can perform repairs in timely fashion some replacement components must be kept in stock.

There are risks associated with keeping ICT components in stock to minimise these risks the follow measures should be implemented:

1) Maximum stock levels of 5 units per component may be kept per workshop.
2) Components must be kept in lockable cabinets or safes.
3) Only replacement components for desktop computer will be kept as store items.
4) Stock levels of components must be verified on a weekly basis.

7 Approving Authority

The member of the Executive Council and the Superintendent General has the responsibility to approve the departmental Hardware workshop Policy

8 Accountabilities and Responsibilities

8.1 The Superintendent General

The SG working in conjunction with the CIO shall be responsible for ensuring the effective implementation and compliance of the ECDSD policies, standards and procedures.

8.2 ICT Operation Manager

The ICT Operations Manager is responsible for maintaining and review of this policy.

9 Effective date of the Policy

The Hardware Policy is effective upon the date the member of the Executive Council has approved it.

10 Monitoring Mechanisms

a) ICT Operational Committee

b) ICT Steering Committee

c) ICT Managers Meeting

The CIO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy. Such mechanisms as mentioned above and in line with the CIO charter shall be used to monitor this policy.

11 Review of the Policy

The policy will be reviewed every three years and whenever there are new developments to maintain relevance.

12 Enforcement

a) Failure to comply with this policy shall result in disciplinary action.

b) Any conduct that interferes with the normal and proper operation of the departments IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved Access Control Policy.

c) The ECDSD executive management reserves the right to revoke the privileges of any user at any time until such time it is deemed fit to reinstate the rights.

13. Policy Recommendation and Approval

The signatories hereof, being duly authorised thereto, by their signatures hereto authorise the execution of the work detailed herein, or confirm their acceptance of the contents hereof and authorise the implementation/adoption thereof, as the case may be, for and on behalf of the parties represented by them.

ECDSD Approval

____________________________________ 31/March 2016.
ECDSD: Member of Executive Council: N Sihlwayi Date

ECDSD Recommended

____________________________________ 30/03/2016-
ECDSD: Superintendent General: S Khanyile Date

G. Laptop Policy

I.Definition and Terms

Terms	Definition
i) Executive Management	this constitutes the Top Management of the Department
ii) Department	the Department of Social Development
iii) Electronic Communications	any Communications via email, fax, telephone and internet
iv) End user	The person utilising the information.
v) “Your”	Determiner which denotes the departmental equipment.
vi) freeware	Any proprietary software that is available for free

vii) public domain software	Software that is placed in the public domain, with no copyright or trademark
Acronyms	
i) GB	Gigabyte
ii) CIO	Chief Information Officer
iii) ECDSD	Department of Social Development
iv) GITO	Government Information Technology Officer
v) ICT	Information and Communication Technology
vi) IT	Information Technology
vii) ID	Identification
viii)PC	Personal Computer
ix) PDA	Personal Digital Assistant
x) SG	Superintendent General
xi) USB	Universal Serial Bus
xii) CD	Compact Disc
xiii)DVD	Digital Video Disc
xiv) CD-ROM	Compact Disc Read Only Memory

II.Legislative Framework

i) The Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)
ii) The Protection of Information Act, 1982 (Act No. 84 of 1982)
iii) The State Information Technology Act, 1998 (Act No. 88 of 1998)
iv) SABS/ISO 17799
v) Minimum Information Security Standards (MISS) 1996
vi) Guidelines for the Handling of Classified Information (SP/2/8/1) 1988
vii) Electronic Communications and Transaction Act, 2002 (Act no. 25 of 2002)

1. Preamble

The policy has been in use since 2012 but was due for review and upon review the existing controls objectives were still relevant. All departments' computer systems face information security risks. Laptop computers are an essential business tool but their very portability makes them particularly vulnerable to physical damage or theft. Furthermore, the fact that they are often used outside the department's premises increases the threats from people who do not work for the department and may not have its interests at heart.

Portable computers are especially vulnerable to physical damage or loss, and theft, either for resale (opportunistic thieves) or for the information they contain (industrial spies).

The impacts of such breaches include not just the replacement value of the hardware, but also the value of any department's data on them, or accessible through them. Information is a vital asset to the department. The department's computer users depend heavily on computer systems to provide complete and accurate business information when and where they need it. The impacts of unauthorised access to or modification of, important and/or sensitive department's data can far outweigh the cost of the equipment itself.

This policy refers to certain other/general information security policies, but the specific information given here is directly relevant to laptops and, in case of conflict, takes precedence over other policies.

2. Purpose

The purpose of this policy is to ensure proper use and protection of laptop computers and information stored within them.

3. Objective

The purpose of this document is to ensure proper usage and protection of laptops computers and information stored within them. This policy describes the controls necessary to minimise information security risks affecting the ECDSD laptops. This policy describes the controls necessary to minimise information security risks affecting the ECDSD laptops.

4. Scope

This policy applies to all users within the ECDSD who have access to or use laptops within and outside the department's premises.

5. Principles and Values

Information security is more than just computer security. It also includes a wide range of physical security measures such as protecting your information assets against natural disasters or theft, and social engineering attacks such as someone tricking you giving out sensitive information. There are three basic principles of information security:

a) **Confidentiality:** means making sure that information is only seen by people who have the right to see it.
b) **Integrity:** means making sure that information remains intact and unaltered.
c) **Availability:** implies having access to your information when you need it.

6. Policy Provisions

6.1 Physical security controls for laptops

a) The physical security of 'your' laptop is your personal responsibility, therefore take all reasonable precautions. Be sensible and stay alert to the risks.

b) Keep your laptop in your possession and within sight whenever possible, just as if it were your wallet, handbag or mobile phone. Be extra careful in public places such as airports, railway stations and restaurants. It takes thieves just a fraction of a second to steal an unattended laptop.

c) If you have to leave the laptop temporarily unattended in the office, meeting room or hotel room, even for a short while, use a laptop security cable or similar device to attach it firmly to a desk or similar heavy furniture. These locks are not very secure but they do deter casual thieves.

d) Lock the laptop away out of sight when you are not using it, preferably in a strong cupboard, filing cabinet or safe. This applies at home, in the office or in a hotel. Never leave a laptop visibly unattended in a vehicle. If absolutely necessary, lock it out of sight in the trunk or glove compartment but it is generally much safer to take it with you.

e) Carry and store the laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage. Do not drop it or knock it about. Bubble-wrap packaging may be useful. An ordinary-looking briefcase is also less likely to attract thieves than an obvious laptop bag.

f) In an event a laptop is lost, stolen, drop or knock (Incur substantial damage) and an element of negligence has been established you will be liable for the cost of repair or total cost of replacement.

g) Keep a note of the make, model, serial number and the department asset label of your laptop but do not keep this information with the laptop. If it is lost or stolen, notify the police immediately and inform the relevant ICT Assistant Manager, Supply Chain and Risk Management Unit as soon as practicable (within 24 hours).

6.2 Virus protection of laptops

a) Viruses are a major threat to the department and laptops are particularly vulnerable if their anti-virus software is not kept up-to-date. The anti-virus software **shall** be updated at least monthly. The easiest way of doing this is simply to log on to the department's network for the automatic update process to run. If you cannot log on for some reason, contact the IT Help/Service Desk for advice on obtaining and installing anti-virus updates.

b) E-mail attachments are the number one source of computer viruses. Avoid opening any e-mail attachment unless you were expecting to receive it from that person.

c) Always virus-scan any files downloaded to your computer from any source (CD/DVD, USB hard disks and memory sticks, network files, e-mail attachments or files from the Internet). Virus scans normally happen automatically but the IT Help/Service Desk can tell you how to initiate manual scans if you wish to be certain.

d) Report any security incidents (such as virus infections) promptly to the IT Help/Service Desk in order to minimise the damage.

e) Respond immediately to any virus warning message on your computer, or if you suspect a virus (e.g. by unusual file activity) by contacting the IT Help/Service Desk.

f) Do not forward any files or upload data onto the network if you suspect your PC might be infected.

g) Be especially careful to virus-scan your system before you send any files outside the Department. This includes **e-mail** attachments and CD-ROMs that you create.

6.3 Controls against unauthorised access to laptop data

a) The user must use approved encryption software on all corporate laptops, choose a long, strong encryption password/phrase and keep it secure. Contact the IT Help/Service Desk for further information on laptop encryption. If your laptop is lost or stolen, encryption provides extremely strong protection against unauthorised access to the data.

b) The user is personally accountable for all network and systems access under your user ID, so keep your password absolutely secret. Never share it with anyone, not even members of your family, friends or IT staff.

c) Corporate laptops are provided to employees for official use. Do not loan your laptop or allow it to be used by others such as family and friends.

d) Avoid leaving your laptop unattended and logged-on. Always shut down, log off or activate a password-protected screensaver before walking away from the machine.

6.4 Unauthorised software

Do not download, install or use unauthorised software programs. Unauthorised software could introduce serious security vulnerabilities into the department networks as well as affecting the functioning of your laptop. Software packages that permit the computer to be ‘remote controlled’ (e.g. PC anywhere) and ‘hacking tools’ (e.g. network sniffers and password crackers) are explicitly forbidden on the department’s equipment unless they have been explicitly preauthorised by management for legitimate business purposes.

6.5 Unlicensed software

Be careful about software licences. Most software, unless it is specifically identified as “freeware” or “public domain software”, may only be installed and/or used if the appropriate licence fee has been paid. Shareware or trial packages must be deleted or licenced by the end of the permitted free trial period. Some software is limited to free use by private individuals whereas commercial use requires a licence payment. Individuals and companies are being prosecuted for infringing software copyright: do not risk bringing yourself and the department into disrepute by breaking the law.

6.6 Backups

The users shall make their own backups of data on their laptop. The simplest way to do this is to logon and upload a data from the laptop to the network on a regular basis – ideally daily, but weekly at least. If you are unable to access the network, it is your responsibility to take regular off-line backups to CD/DVD, USB memory sticks etc. Make sure that off-line backups are encrypted and physically secured. Remember, if the laptop is stolen, lost or damaged, or if it simply malfunctions, it may be impossible to retrieve any of the data from the laptop. Off-line backups will save you a lot of heartache and extra work.

6.7 Laws, regulations and policies

You must comply with relevant laws, regulations and policies applying to the use of computers and information. Software licensing has already been mentioned and privacy laws are another example. Various corporate security policies apply to laptops, the data they contain, and network access (including use of the Internet). Visit Information Security's intranet website for further information.

6.8 Inappropriate materials

Be sensible. The department will not tolerate inappropriate materials such as pornographic, racist, defamatory or harassing files, pictures, videos or e-mail messages that might cause offence or embarrassment. Never store, use, copy or circulate such material on the laptop and steer clear of dubious websites. IT staff routinely monitor the network and systems for such materials and track use of the Internet: they will report serious/repeated offenders and any illegal materials directly to management, and disciplinary processes will be initiated. If you receive inappropriate material by e-mail or other means, delete it immediately. If you accidentally browse to an offensive website, click 'back' or close the window straight away. If you routinely receive a lot of spam, call IT Help/Service Desk to check your spam settings.

6.9 Health and safety aspects of using laptops

Laptops normally have smaller keyboards, displays and pointing devices that are less comfortable to use than desktop systems, increasing the chance of repetitive strain injury. Balancing the laptop on your knees hardly helps the situation. Limit the amount of time you spend using your laptop. Wherever possible, place the laptop on a conventional desk or table and sit comfortably in an appropriate chair to use it. If you tend to use the laptop in an office most of the time, you are advised to use a 'docking station' with a full-sized keyboard, a normal mouse and a display permanently mounted at the correct height if available. Stop using the portable and consult Health and Safety/employee wellness for assistance if you experience symptoms such as wrist pain, eye strain or headaches that you think may be caused by the way you are using the portable.

7 Approving Authority

The member of the Executive Council and the Superintendent General has the responsibility to approve the departmental Laptop Policy

8 Accountabilities and Responsibilities

8.2 The Superintendent General

The SG working in conjunction with the CFO shall be responsible for ensuring the effective implementation and compliance of the ECDSD EC policies, standards and procedures.

8.3 ICT Operations Manager

The ICT operations manager is responsible for maintaining this policy.

8.4 Internal audit

a) The Internal Audit Unit is authorised by management to assess compliance with all corporate policies at any time.

b) The Internal Audit department may assist with audits of outsourcing contracts including security compliance audits, and advise management on the risks and controls relating to outsourcing.

9 Effective date of the Policy

The Laptop Policy is effective upon the date the member of the Executive Council has approved it.

10 Monitoring Mechanisms

a) ICT Operational Committee

b) ICT Steering Committee

c) ICT Managers Meeting

The CIO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy. Such mechanisms as mentioned above shall be used to monitor this policy

11 Review of the Policy

The policy will be reviewed every three years and whenever there are new developments to maintain relevance.

12 Enforcement

m) Failure to comply with this policy shall result in disciplinary action.

n) Any conduct that interferes with the normal and proper operation of the departments IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of this approved Policy.

o) The ECDSD executive management reserves the right to revoke the privileges of any user at any time until such time it is deemed fit to reinstate the rights.

13 Policy Recommendation and Approval

The signatories hereof, being duly authorised thereto, by their signatures hereto authorise the execution of the work detailed herein, or confirm their acceptance of the contents hereof and authorise the implementation/adoption thereof, as the case may be, for and on behalf of the parties represented by them.

H. Malicious Codes Policy

I. Definition and Terms

Terms	Definition
i) Executive Management	this constitutes the Top Management of the Department
ii) Department	the Department of Social Development
iii) Electronic Communications	Any Communications via email, fax, telephone and internet
iv) Administrator	Administration is the process of managing user identities, the roles and credentials they are assigned, and the resources and services they use.
v) End user	the person utilising the information
vi) Malicious Code	A new breed of Internet threat which is intended to cause security breach or damage the system
Acronyms	
i) GB	Gigabyte
ii) CIO	Chief Information Officer
iii) ECDSD	Department of Social Development
iv) GITO	Government Information Technology Officer
v) ICT	Information and Communication Technology
vi) IT	Information Technology
vii) PC	Personal Computer
viii)PDA	Personal Digital Assistant
ix) SG	Superintendent General

II. Legislative Framework

i) The Promotion of Access to Information Act, 2000 (Act no. 2 of 2000)
ii) The Protection of Information Act, 1982 (Act no. 84 of 1982)
iii) The State Information Technology Act, 1998 (Act no. 88 of 1998)
iv) SABS/ISO 17799 (2005)
v) Minimum Information Security Standards (MISS 1996)
vi) Guidelines for the Handling of Classified Information (SP/2/8/1)
vii) Electronic Communications and Transaction Act, 2002 (Act no. 25 of 2002)

1. Preamble

The policy has been in use since 2012 but was due for review and upon review it has been observed by policy implementers that the controls objective were still relevant. This policy establishes malicious code prevention requirements for ECDSD information resources. Malicious code is a new breed of Internet threat that cannot be efficiently controlled by conventional antivirus software alone. In contrast to viruses that require a user to execute a program in order to cause damage, malicious codes are auto-executable applications. Malicious-code program typically includes computer viruses, worms, Trojan horses, spyware, adware and malicious mobile code (executable code in the form of Java applets, MS ActiveX, JavaScript or VBScript, that has been written deliberately to perform unauthorised functions). All individuals who have access to information and systems of the Department of Social Development should be aware of the risks from malware, and the actions required minimising those risks.

Every institution, to which the Minimum Information Security Standards (MISS) and/or the Guidelines for the Handling of Classified Information (SP/2/8/1) apply, has the duty to secure computer networks containing classified data. This applies to all Government institutions who act as custodians of Government information and data. Government institutions are bound to uphold the right to privacy as entrenched in the constitution insofar as this relates to Government information and data.

2. Purpose

The purpose of this policy is to protect the departmental IT systems and resources from malicious codes.

3. Objective

The policy objective is to ensure that:

a) Malicious code prevention requirements for ECDSD information resources are properly established.

b) An antivirus and malicious-code program shall be deployed and managed to ensure effective management of the risks relating to viruses and malicious code. Damage caused by malicious software shall be prevented, using preventive, corrective and detective controls.

4. Scope of Applicability

It applies to all users of the departments ICT systems and all devices capable of propagating malicious code and attached or requires access to the department network.

5. Principles and Values

Information security is more than just computer security. It also includes a wide range of physical security measures such as protecting your information assets against natural disasters or theft, and social engineering attacks such as someone tricking you giving out sensitive information. There are three basic principles of information security

a) **Confidentiality:** means making sure that information is only seen by people who have the right to see it.
b) **Integrity:** means making sure that information remains intact and unaltered.
c) **Availability:** implies having access to your information when you need it.

6. Policy provisions

a) The ECDSD shall ensure that there are adequate resources and skills for:
   i) installing virus protection software;
   ii) updating software;
   iii) updating virus definition files;
   iv) cleaning infected computers;
   v) distributing information to users;
   vi) identifying unprotected computers and implementing remedial measures; and
   vii) where the ECDSD does not have these resources in-house, it shall make a contract with an external provider. The ECDSD shall have access to either internal or third party resources for the:
      1) evaluation of virus protection software for PCs and workstations;
      2) evaluation of virus protection software for servers, mail-servers and firewalls;
      3) evaluation of the vendors of the software packages;
      4) evaluation of the risk in a new virus;
      5) deciding if distributed warning signals are true or false; and
      6) continuous evaluation of the efficiency of software installed.

b) The ECDSD shall have effective procedures in place:
   i) for logging, reporting and escalation of potential virus incidents;
   ii) for cleaning virus-infected computers and the cleaning shall be performed at the ECDSD premises. If this is not possible and the infected computer has to be transported to an external party, the policies for removing equipment from the ECDSD premises shall apply.

c) Any user who suspect infection by a virus shall immediately shut down the specific computer, calls the IT Administrator, and makes no attempt to remove the virus, unless they are instructed by IT administration or server administrator.

d) Users shall forward any security warnings information received, for example via e-mail, to the ICT, who will then determine what action is appropriate. Users shall not personally redistribute system-vulnerability information, nor forward the warnings to any other party.

e) Users must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any ECDSD computer or network.

f) ECDSD approved anti-virus software shall be installed and enabled on all ECDSD servers (including but not limited to application servers, exchange servers, file servers, network servers, desktop, laptop computers) and other end user computing devices.

g) These machines shall also have the latest virus screening pattern file. The installation and configuration/setup of the virus screening software shall be as per the standards prescribed by the ICT. Any deviation from these standards shall first be approved by ICT.

h) Exceptions will be made for operating systems and platforms where no known vulnerabilities exist, and for which no anti-virus software exists. All ECDSD computers except for end-user devices shall run software that checks for unauthorized files or changes.

i) ICT shall implement network scanning tools to assess internal vulnerabilities and virus readiness across the network. ICT shall implement real time alerting utilities to centrally monitor the network for virus outbreaks and threats. Computer systems joining the network shall be scanned to ensure that the required software patches and anti-virus software is up to date, and that no viruses are present. This scan shall be carried out periodically while the computer system remains attached to the network. Computer systems failing this scan shall be disconnected or quarantined from the network until steps have been taken to ensure compliance.

j) Every ECDSD employee who examines, processes, or stores ECDSD information using a computer that he or she owns shall install and regularly run the most current version of a virus detection software package approved by ICT.

k) Externally-supplied removable computer readable media may not be used on any ECDSD personal computer or server unless they have been checked for viruses.

l) All outbound software and executable files containing software or executable statements shall be certified as virus free prior to being sent to any third party.

m) All externally-supplied computer-readable files shall be decrypted prior to being subjected to an approved virus checking process;

n) Only application software and systems software formally approved by ICT management are to be installed. No executable software, regardless of the source may knowingly be installed on a device connected to the department network. This is applicable to all platforms. The following rules shall be observed when planning to download and/or install any software.

  i) Where authorization has been obtained, software may only be downloaded from a known and trusted source. Software verification tools, such as digital signatures shall be employed where possible, for example code-signing certificates, MD5 checksums;

  ii) Downloaded software shall be scanned for malicious code prior to being installed.

iii) Software or files received from an external entity, and intended to be installed on ECDSD production machine shall be tested for unauthorized software on a standalone non-production machine before being deployed.

o) Before any files are restored to a production ECDSD computer system from backup storage media, all backup files shall have been scanned with the latest version of virus screening software.

p) To ensure that viruses are neither received at nor sent from ECDSD, all communications transmitted shall be checked by virus protection and protocol filtering software installed on mail server and/or firewall.

q) Anti-Virus software shall be configured to update itself on a regular basis and be capable of receiving pushed updates as and when required.

r) Virus protection software shall trigger an alarm when a virus has been detected. If the computer is connected to a network, that alarm shall be sent to either a virus protection console that aggregates alarms for the facility or to the person responsible for the cleaning of virus infected computers at the facility.

s) The virus protection software shall be able to quarantine or delete infected files, programs and documents.

t) Only devices approved by ICT manager may be connected to the department network.

7. Approving Authority

The member of the Executive Council and the Superintendent General has the responsibility to approve the departmental Malicious Code Policy

8. Accountabilities and Responsibilities

8.1 The Superintendent General

a) The SG in conjunction with the CIO shall implement, enforce and monitor the controls in accordance with the requirements outlined by management, and shall advise users on the correct ways to access information and systems.

b) Responsible for building, configuring, operating and maintaining the departments ICT facilities (including anti-spam, anti-malware and other email security controls) in accordance with this policy.

c) Responsible for assisting users with secure use of ICT facilities, and acts as a focal point for reporting ICT security incidents.

d) Responsible for ensuring that all devices have approved malicious code version and release installed and mechanism is in place to ensure malicious code patterns are updated and current.

8.2 All employees

All employees are responsible for complying with this and other corporate policies at all times. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of acceptable behaviour) to comply with the departments information security policies.

8.3 Information Security Manager

Information Security Manager is responsible for maintaining this policy and advising generally on information security controls. Working in conjunction with other corporate functions, it is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy.

8.4 Internal Audit

Internal Audit is authorized by management to assess compliance with all corporate policies at any time.

9 Effective date of the Policy

The Malicious Code Policy is effective upon the date the member of the Executive Council has approved it.

10 Monitoring Mechanisms

a) ICT Operational Committee

b) ICT Steering Committee

c) ICT Managers Meeting

The CIO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy. Such mechanisms as mentioned above shall be used to monitor this policy.

11 Review of the Policy

The policy will be reviewed every three years and whenever there are new developments to maintain relevance as and when a need is identified by the person responsible as specified above.

12 Enforcement

a) Failure to comply with this policy shall result in disciplinary action.

b) Any conduct that interferes with the normal and proper operation of the departments IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved Malicious Code Policy.

c) The ECDSD executive management reserves the right to revoke the privileges of any user at any time until such time it is deemed fit to reinstate the rights.

13 Policy Recommendation and Approval

The signatories hereof, being duly authorised thereto, by their signatures hereto authorise the execution of the work detailed herein, or confirm their acceptance of the contents hereof and authorise the implementation/adoption thereof, as the case may be, for and on behalf of the parties represented by them.

ECDSD Approval

ECDSD: Member of Executive Council: N Sihlwayi

31/March 2016.
Date

ECDSD Recommended

ECDSD: Superintendent General: S Khanyile

30/03/2016-
Date

I. Network Policy

I. Definition and Terms

Terms	Definition
i) Executive Management	this constitutes the Top Management of the Department
ii) Department	the Department of Social Development
iii) Database	This is a specialised software system that is used for managing highly structured data. Databases range from simple desktop systems to huge, multi-machine implementations.
iv) Firewall	A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices that is configured to permit or deny network transmissions based upon a set of rules and other criteria.
v) Demilitarized zone	A physical or logical sub network that exposes an organisation's external–facing service to a larger and untrusted network usually the internet.
vi) Router	A device used to connect, accept and transfer data packets from one Wide Area Network to the Local Area Network.
vii) Physical Access control	Is a term which refers to the ability of people to physically gain access to a computer
viii)Trusted connections	Trusted networks are more secured and confidential because of strong firewall settings
ix) Untrusted connections	Untrusted networks are configured machines separate from the secured network which are more prone to attacks
x) Logical Access control	Tools and protocols used for identification, authentication, authorisation
xi) Electronic Communications	Any Communications via email, fax, telephone and internet
xii) End user	the person utilising the information
Acronyms	
i) GB	Gigabyte
ii) CIO	Chief Information Officer
iii) ECDSD	Department of Social Development
iv) GITO	Government Information Technology Officer
v) ICT	Information and Communication Technology

vi) IT	Information Technology
vii) PC	Personal Computer
viii)PDA	Personal Digital Assistant
ix) SG	Superintendent General
x) ISS/RM	Information System Security/ Risk Management
xi) SSL	Secure Socket Layer
xii) HTTP	Hyper Text Transfer Protocol
xiii) VPN	Virtual Private Network
xiv) EDI	Electronic Data Interchange
xv) FTP	File Transfer Protocol

II. Legislative Framework

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

ii) The Protection of Information Act, 1982 (Act no. 84 of 1982)

iii) The State Information Technology Act, 1998 (Act no. 88 of 1998)

iv) SABS/ISO 17799 (2005)

v) Minimum Information Security Standards (MISS 1996)

vi) Guidelines for the Handling of Classified Information (SP/2/8/1) (1988)

vii) Electronic Communications and Transaction Act, 2002 (Act no. 25 of 2002)

viii) Departmental Health and Safety Policy

1. Preamble

The policy has been in use since 2012 but was due for review and upon review it has been observed that the controls objectives are still relevant. The network refers to fibre optic and copper cabling, data stream circuits, desktop and office network access points, drop-in facilities, dial-up services, and the routers, switches, patch panels and other equipment used to connect networking components.

The network is a shared resource intended to support computing activities related to the official and administrative functions of the ECDSD. Policies are developed to provide officials and staff of the ECDSD open access to the network and to the email, Internet or Intranet, subject to ECDSD and other regulations and the Law.

Network equipment, such as wiring closets, switches and firewalls, shall be regarded as sensitive, and shall be protected with physical and logical access control. The activities on managed network equipment shall be logged in centralized syslog facilities. The network may be internally divided into different segments, depending on evaluated risks. This segmentation may be implemented by means of secure network nodes. The ICT shall be notified immediately of each security event, system implementation or additional network connectivity that may have a security implication for the rest of the ECDSD.

Every institution, to which the Minimum Information Security Standards (MISS) and/or the Guidelines for the Handling of Classified Information (SP/2/8/1) apply, has the duty to secure computer networks containing classified data. This applies to all Government institutions who act as custodians of Government information and data. Government institutions are bound to uphold the right to privacy as entrenched in the constitution insofar as this relates to Government information and data

2. Purpose

The purpose of this document is to define and distinguish policies and procedures of how Network should be controlled and managed properly within the ECDSD to ensure security and proper usage.

3. Objective

The objective of this policy is to ensure the network, both for internal trusted connections, as well as for untrusted external connections is secured.

4. Scope

This is a standard departmental policy that applies to all users of the department’s Information and technology systems. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound to comply with our information security policies.

5. Principles and Values

Information security is more than just computer security. It also includes a wide range of physical security measures such as protecting your information assets against natural disasters or theft, and social engineering attacks such as someone tricking you giving out sensitive information. There are three basic principles of information security

a) **Confidentiality:** means making sure that information is only seen by people who have the right to see it.
b) **Integrity:** means making sure that information remains intact and unaltered.
c) **Availability:** implies having access to your information when you need it.

6. Policy statements

a. Network security

The department shall adhere to these provisions:

a) Only authorised people shall have access to wiring closets, especially in buildings where other companies other than ECDSD reside;

b) For the IT service provider to the ECDSD, the communication between the service provider's network and the ECDSD network shall be controlled by secure, documented interfaces approved by the ECDSD;

c) In case an interruption in communications or similar event should take place, the ECDSD shall have procedures in place to make sure that all data affected by an interrupted transaction is restored;

d) Where supported by the device firmware or operating system, managed network devices such as print servers, routers, hubs and switches shall be protected with user name and password credentials, changed from their default values and capable of identifying unique individual users;

e) The log information of managed network equipment shall be included in centralized syslog facilities;

f) All data communication between systems and applications shall be controlled, to ensure that:

   i) all data is transmitted in its entirety; and

   ii) transmission cannot be intercepted or manipulated.

g) The following principles apply to untrusted connections:

   i) all untrusted connections shall be registered with, and authorized by the IT top management;

   ii) the ICT shall maintain a current inventory of all connections to external networks including telephone networks, extranets and the internet;

   iii) all untrusted connections shall make use of a secure network node;

   iv) all untrusted connections, shall be secured and will not allow unauthorised access to any sensitive data or systems of ECDSD; and

   v) all untrusted connections shall be authorised at IT executive level.

h) Systems or users who make use of untrusted connections shall not be provided with any unnecessary functionality which may impact the security (system or data) of ECDSD.

i) All untrusted connectivity (HTTP or SSL) shall be terminated on the secure part of the ECDSD Network;

j) Application-gateway firewalls (layer 7 firewalls) are required to protect the traffic at the message level;

k) ECDSD computer systems containing secret information shall not be connected to any untrusted network or computer;

l) All web servers accessible via the Internet shall be protected by a router and firewall approved by the ISS/RM Committee. All internet commerce servers including payment servers, database servers, and web servers shall be protected by firewalls in a demilitarized zone. Public Internet servers shall be placed on subnets separate from internal ECDSD networks;

m) Routers and firewalls shall be employed to restrict traffic from the public servers to internal networks. Any user and/or systems requiring access to the ECDSD Internal Network via an untrusted network shall be authenticated on the ECDSD Network. Strong authentication via an access control and/or authentication server is required to authenticate this type of users and/or systems via the network perimeter firewall;

n) The access control server will be used to authenticate users and/or systems and provide a role based profile which will restrict the user and/or system to the various systems and/or servers. All information security measures which are used in securing an untrusted connection, for example the installation of a secure network node, shall be in compliance with the information security standards set by ISS/RM Committee endorsed by IMST Board. Where standards have not yet been set, ISS/RM Committee shall be approached to ratify the situation;

o) All inbound dial-up lines, or other in-bound real-time external connections to ECDSD internal networks and/or multi-user computer systems shall pass through an additional access control point including an approved firewall, and access server before users can reach a log-in banner;

p) All firewalls used to protect ECDSD's internal network shall run on separate dedicated computers. These computers may not serve other purposes such as act as web servers;

q) Firewall configuration rules and permissible service rules have been reached after an extended evaluation of costs and benefits. These rules shall not be changed unless the permission of the ISS/RM Committee has first been obtained, and appropriate change control procedures have been followed;

r) All connections between ECDSD internal networks and the internet (or any other publicly accessible computer network) shall include an approved firewall and related access controls;

s) The establishment of Internet or any other external network connections (including 3G), is prohibited unless this connection has first been approved by IMST Board, and after the IMST has determined that the combined system will be in compliance with ECDSD security requirements.

i) These connections include the establishment of multi-computer file systems, internet home pages, internet FTP servers, and the like;

ii) All tunnels are to be registered and secured via methods acceptable to ISS/RM Committee and will terminate on a dedicated tunnelling device such as a VPN concentrator;

iii) Users and vendors shall not make arrangements for, or actually complete the installation of data lines with any carrier, if they have not first obtained approval from the IMST Board;

iv) The management of nodes (routers etc.) which reside on untrusted networks may not reduce the level of security, which is required between trusted and untrusted networks;

v) Unless the executive management have all approved in advance, employees are prohibited from using new or existing internet connections to establish new business channels. These channels include EDI arrangements, electronic malls with on-line shopping and on-line database service.

t) Users shall not establish intranet servers, electronic bulletin boards, local area networks, modem connections to existing internal networks, or other multi-user systems for communicating information without the specific approval of ISS/RM Committee. This policy helps ensure that all ECDSD-networked systems have the controls needed to prevent unauthorised access;

u) Real-time connections between two or more in-house computer systems shall not be established unless ISS/RM Committee has first determined that such connections will not jeopardize information security of the department;

v) As a condition of gaining access to ECDSD's computer network, every third party shall secure its own connected systems in a manner consistent with ECDSD requirements;

w) ECDSD reserve the right to audit the security measures in effect on these connected systems without prior warning. ECDSD also reserve the right to immediately terminate network connections with all third party systems not meeting such requirements;

x) Where third party suppliers provide support for an environment and telnet or FTP applications are required, strong authentication i.e. two factor authentication will be imposed on the Firewall when connecting to the device;

y) Unless ISS/RM Committee approval has been obtained, all ECDSD computers that are internet connected or directly reachable through the internet are prohibited from using shared directory systems, sometimes called shared file systems. These systems allow a user to obtain access to more than one computer's file system with only a single log-in process;

z) Exceptions are made for internet commerce and other systems where multiple machine architecture involves automatically passing users with severely restricted privileges from one computer to another;

aa) All large networks crossing national or organisational boundaries shall have separately defined logical domains, each protected with suitable security perimeters and access control mechanisms;

bb) The internal system addresses, configurations, and related system design information for ECDSD networked computer systems shall be restricted such that both systems and users outside ECDSD's internal network cannot access this information;

cc) All secure network nodes, will be classified as having a high security risk to the systems and data of ECDSD. The security measures which are implemented to address the security exposures shall be capable of enforcing the level of security (as defined by its classification) which is required within that environment. The integrity of these nodes will be monitored on a daily basis. All changes made to secure network nodes shall be verified by change control, that the correct change control procedures were followed;

dd) Except as otherwise specifically provided, employees shall not intercept or disclose, or assist in intercepting or disclosing, electronic communications;

b. Health and Safety

a) Users are responsible for ensuring that they are sufficiently familiar with the operation of any equipment they use, for making their own use of it safe and effective and for avoiding interference with the use of it by others. Equipment must also be used within Departmental Health and Safety policies.

c. Infrastructure New and Changes

The policy seeks to provide the following provisions for any request on new or changes to existing infrastructure:

a) The requestor has a lease agreement which will run for at least the following three years. If the remaining lease period is less than three years then the request for network cabling cannot be processed.

b) All cabling will be done to departmental cabling standards. (See ICT Standards document)

c) The building where the cabling is required has reliable electrical power.

d) The chances of the building being burgled are non-existent or very low.

e) There is no renovations which will be undertaken within the next eighteen months.

f) Users who require changes to the network infrastructure, including the activation of desktop network access points, the installation of new desktop or office network access points, the provision of cabling shall, in the first place, request these changes from the IT department;

g) Officials have no authority to change any network access points or modify network equipment in any way, except where this authority has been explicitly granted in exceptional circumstances by the IT Department. The granting of such authority on one occasion shall not be interpreted as license to make similar changes at other times.

d. Connecting computing equipment to the network

a) Computers and workstations may be connected to the network subject to the following conditions:

i) In offices and public access areas, a network access point already allocated to a configured computer shall not be used by another personal computer;

ii) Users who wish to directly connect personal computers to the network are required to obtain a network address for their computer from their IT where the technicians will help them configure their computers;

iii) Users of portable (laptop) computers who wish to directly connect to the Department network are also required to register their computer with IT where the technicians will help them configure their laptops;

iv) No modem, fax or any other data communications device may be directly connected to a network access point without the prior approval of the Network Manager or a person acting on his/her behalf;

v) Requests for such connections shall first go to the ISS/RM Committee department for assessment and approval;

vi) No departmental computing device shall be directly connected to the Department network and at the same time be connected to another private computing network whether through another Internet Service Provider (ISP), direct cabling, modem, satellite, radio or any other technology;

vii) Requests for approval of such connections shall be made directly to the IT Department giving full details of the proposed connection, reasons thereof, duration of the proposed connection and the details of the private network intended to use. The user must bear in mind that this connection may be declined by the IT department;

viii) Any computing device that is connected to the Department network should be properly protected against hacking, viruses and similar security threats through appropriate use of security technology, including anti-virus software;

ix) There is a risk if any computer which is not properly secured is used directly in the network;

x) No private devices are allowed to be connected to the departmental network.

i. Use of the network

a) Users shall not run network applications in such a way as to deny network access to other users;

b) IT Department reserves the right to prohibit any activity which may deny network access to other users or which poses a threat to the availability, integrity and privacy of any computing services connected to the network;

c) Users who wish to run new network applications shall consult with the IT Department;

d) If a member of staff requires access to a new service or one that has been previously made unavailable, their first request shall be to their relevant ICT manager naming the actual service required, and it would be helpful if the applicant provided reasons for the need of the service and overall goal with regards to the required service;

e) Officials shall pass their requests to their ICT managers who should pass these requests Provincial IT;

f) If a staff member requests for a services considered being too dangerous for security reasons the Department network can decline such a request at that point, or the request would be passed on to the ISS/RM Committee, who would make the necessary decisions based on the security threat of the request. When request is declined, the ISS/RM Committee will provide reasons and where possible advice on any alternative methods of carrying out the desired objective;

g) Where new information indicates the presence of a significant threat associated with an existing operational service, ISS reserves the right to discontinue access to the service until the threat is no longer a significant risk. Where possible those affected by such a change will be informed in advance of access being curtailed;

h) The Network Security Officer shall maintain a record of what services have been permitted and blocked and to whom and shall act as a reference point for this information;

i) Electronic mail between computers connected to the Department network and the Internet must be relayed via the Department e-mail gateway, either directly or through a local departmental mail server. The Department does not accept mail to external addresses sent from an address, which is itself external to the Department or sent from a computer, which has not been properly registered with an authorised network address;

j) In order to use external Web resources, local users shall use a web browser configured to use the Department web cache;

k) As new services are added to the network or become available on the Internet it may become necessary for similar proxy or cache systems to be used for these services in order to provide an acceptable level of security or performance.

ii. Removal of equipment

a) No equipment or other electronic communication facility may be borrowed, removed or moved from a designated location or Departmental premises, without the explicit permission of the IT department;

b) For permission to be granted the necessary forms detailing the purpose of the removal of the equipment and the equipment details must be filled by the applicant and countersigned by the appropriate manager.

7. Approving Authority

The member of the Executive Council and the Superintendent General has the responsibility to approve the departmental Network Policy

8. Roles and responsibilities

e. The Superintendent General

The SG working in conjunction with the CFO shall be responsible for ensuring the effective implementation and compliance of the ECDSD policies, standards and procedures.

f. The CIO

IT shall implement, enforce and monitor the controls in accordance with the requirements outlined by management, and must advise users on the correct ways to access information and systems.

g. Information Security Manager

Information Security Officer is responsible for maintaining this policy and advising generally on information security controls. Working in conjunction with other corporate functions, it is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy.

h. Internal Audit department

The Internal Audit department is authorised by management to assess compliance with all corporate policies at any time.

9. Effective date of the Policy

The Network Policy is effective upon the date the member of the Executive Council has approved it.

10. Monitoring Mechanisms:

a) ICT Operational Committee

b) ICT Steering Committee

c) ICT Managers Meeting

The CIO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy. Such mechanisms as mentioned above shall be used to monitor this policy

11. Review of the Policy

The policy will be reviewed every three years and whenever there are new developments to maintain relevance.

12. Enforcement

a) Failure to comply with this policy shall result in disciplinary action.

b) Any conduct that interferes with the normal and proper operation of the departments IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved Network Policy.

c) The ECDSD executive management reserves the right to revoke the privileges of any user at any time.

13. Policy Recommendation and Approval

The signatories hereof, being duly authorised thereto, by their signatures hereto authorise the execution of the work detailed herein, or confirm their acceptance of the contents hereof and authorise the implementation/adoption thereof, as the case may be, for and on behalf of the parties represented by them.

ECDSD Approval

ECDSD: Member of Executive Council: N Sihlwayi

31/March 2016.
Date

ECDSD Recommended

ECDSD: Superintendent General: S Khanyile

30/03/2016-
Date

J. Password Policy

I. Definition and Terms

Terms	Definition
i) Executive Management	this constitutes the Top Management of the Department
ii) Department	the Department of Social Development
iii) Electronic Communications	Any Communications via email, fax, telephone and internet
iv) End user	the person utilising the information
v) Password	A string of characters that allows access to a computer, interface or system
vi) Legacy Systems	Old method, technology, computer systems or application program.
Acronyms	
i) GB	Gigabyte
ii) CIO	Chief Information Officer
iii) ECDSD	Department of Social Development
iv) GITO	Government Information Technology Officer
v) ICT	Information and Communication Technology
vi) IT	Information Technology
vii) ID	Identification
viii)ISS/RM	Information System Security/ Risk Management
ix) PIN	Personal Identification Number
x) PC	Personal Computer
xi) PDA	Personal Digital Assistant
xii) SG	Superintendent General

II. Legislative Framework

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

ii) The Protection of Information Act, 1982 (Act no. 84 of 1982)

iii) The State Information Technology Act, 1998 (Act no. 88 of 1998)

iv) SABS/ISO 17799 (2005)

v) Minimum Information Security Standards (MISS 1996)

vi) Guidelines for the Handling of Classified Information (SP/2/8/1) 1988

vii) Electronic Communications and Transaction Act, 2002 (Act no. 25 of 2002)

1. Preamble

The policy has been in use since 2012 but was due for review and upon review it has been observed that the controls were not addressing all the systems. The gap was identified on the control of password complexity and the duration of the password. Policies are required to govern the passwords used when connecting to the ECDSD's network from any host and/or when accessing any operating system or application requesting a password. These policies are designed to minimize the potential exposure to the ECDSD from damages that may result from unauthorized use of resources. Damages include the loss of sensitive or department-confidential data, intellectual property, damage to public image and damage to critical department’s internal systems.

The policy aims to restrict access to information or systems within the Department of Social Development Eastern Cape computer environment to authorised users as well as to prevent unauthorised use or viewing of information and IT resources.

2. Purpose

The purpose of this policy is to ensure that only authorised users gain access to the ECDSD information, applications and computer installations.

3. Objectives

a) The policy aims to restrict access to information or systems within the Department of Social Development’s computer environment to authorised users as well as to prevent unauthorised use or viewing of information and IT resources.

b) This policy focuses on password and user ID requirements, access to the department’s computer systems and networks, and segregation of duties related to IT to ensure that IT users are aware of their responsibility towards usage of information systems in order to minimise possible information security risks. In addition, it covers remote, administrator and third party access.

4. Scope of Applicability

The policy applies to all business units, employees, suppliers, vendor’s contractors and any other resources requiring access to the ECDSD computing environment.

Computing environment includes:

a) physical and environmental; and

b) hardware, software, system and applications.

This policy applies to any and all personnel who have any form of computer account requiring a password on the departmental network including e-mail accounts.

5. Principles and Values

Information security is more than just computer security. It also includes a wide range of physical security measures such as protecting your information assets against natural disasters or theft, and social engineering attacks such as someone tricking you giving out sensitive information. There are three basic principles of information security

a) **Confidentiality:** means making sure that information is only seen by people who have the right to see it.
b) **Integrity:** means making sure that information remains intact and unaltered.
c) **Availability:** implies having access to your information when you need it.

6.Policy provisions

6.1 Issuing a new or changing a password

When issuing new or changed passwords it shall be ensured that:

a) the initial password is transferred to the individual telephonically or by email and is forced to change the password on first use;

b) disclosure of passwords is minimised when they are communicated to the user (e.g. using encrypted e-mails or forcing the user to change passwords when they first use them);

c) the display and printing of passwords must be masked, suppressed, or otherwise obscured so that unauthorised parties are not be able to observe or subsequently recover them. Where passwords are displayed to authorized third parties, for example to a security administrator, the following conditions shall be met:

   i) the users shall be forced to change the password at first logon; and

   ii) the functions and information that can be accessed through using the password have been classified as low sensitivity by the ECDSD.

d) it involves the target user directly (i.e. the person to whom the password uniquely applies);

e) the identity of the target user is verified (e.g. via a special code or through independent confirmation); and

f) when a password is initially assigned to a user the password shall be a temporary one and the user shall be forced to change it immediately;

g) a procedure of providing users who have forgotten their password with a new password shall be in place; and

h) the procedure shall include the following components:

   i) a temporary password is to be supplied to the user after a positive identification;

   ii) the temporary password shall be given to the users telephonically or by email;

   iii) the user shall be forced to change the temporary password immediately; and

iv) a procedure for users who believe that their password has been compromised must be in place.

i) passwords shall be changed at least every 42 days;

j) users that have system-level privileges granted through group membership shall have unique passwords held by the user of that account.

6.2 Minimum password length

The length of the password shall always be checked automatically at the time that users construct or select them. All passwords shall have at least eight alpha-numeric characters.

6.3 Difficult-to-guess passwords required

All user-chosen passwords for computers, web accounts, email accounts, servers and networks shall be difficult to guess. Words in a dictionary, derivatives of user-IDs, and common character sequences such as "123456", “qwerty”, “aaabbb”, “zyxwvuts” shall not be employed. Likewise, personal details such as spouse's name, license plate, and birth date shall not be used unless accompanied by additional unrelated characters;

Backward spelling of any name or recognizable words shall not be used;

Avoid using days or months of the year;

Passwords shall contain at least three of the following: uppercase, lower case, digits and any special characters.

6.4 Display and printing of passwords

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

6.5 Periodic forced password changes:

All users shall be automatically forced to change their passwords at least once every 42 days.

Users shall be informed of the password expiry 5 days before the expiry date.

6.6 Assignment of expired passwords:

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

6.7 Account lockout:

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

6.8 Disclosure

a) A password shall never be disclosed to any third party.

b) A password shall not be written down.

c) The last six passwords should not be reusable, and a period of 15 days between password changes should be set to ensure that users do not change their passwords several times in a row to return to their known old password.

d) In order to prevent unauthorised access to other user's computers, information and/or data, requests to reset passwords shall be strictly and constantly monitored. System administrators shall not reset a password unless the user has logged the call with IT Helpdesk and has duly completed the password reset request form.

6.9 Password storage

a) Passwords may only be stored in encrypted form using a strong one-way encryption algorithm.

b) Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, or in other locations where unauthorized persons might discover or use them, except with the formal permission of the ISM.

6.10 Legacy system/Applications

Some legacy systems constrain the length of passwords, or the characters that may be used, to the extent that the passwords cannot conform to the definition of secure passwords. These systems may continue to operate with the less secure passwords with the approval of the Information System Security/ Risk Management Committee, if one of the following conditions hold true:

a) the system is in the process of being decommissioned, or steps are being taken to correct the situation;

b) the functions and information exposed to the users have been classified as low sensitivity by the ISS/RM Committee;

c) steps have been taken to mitigate the risk, for example by isolating the system on the network and protecting access through an additional authentication layer;

d) the risk has been formally documented, and accepted or transferred by the business/system/information owner;

e) shall support authentication of individual users not groups;

f) passwords shall not be transported or communicated in clear text or in any easily reversible form.

6.11 Password management system

a) Any systems that generate and/or store passwords shall do so securely. Where feasible, applications shall rely on operating system controls for authentication an authorization;

b) Systems shall mask or obscure passwords while being entered. IDs and passwords shall never be conveyed to users in the same communication;

c) Where enabled by operating systems and applications, the ECDSD shall implement a password management system that has the following characteristics: It only accepts individual user IDs and passwords, as opposed to shared accounts. The users shall be allowed to select and change their own passwords and the procedure shall include a confirmation procedure to allow for input errors:

i) the user shall be instructed to change passwords whenever there is any indication of possible system or password compromise;

ii) enforce the selection of secure passwords; and

iii) have controls in place to protect against frequent password changes over a short period of time.

d) All sensitive information, including passwords, shall be encrypted with a ECDSD-approved algorithm using at least 128 bit encryption prior to transmission over a network;

e) System-generated passwords shall be generated using a frequently-changing unpredictable source. System-generated passwords (including PINs) shall always be issued immediately after generation. Regardless of the form they take, unissued passwords and PINs shall never be stored;

f) All computer storage media and computer memory areas used in the construction, assignment, distribution, or encryption of passwords or personal identification numbers, shall be erased using a ECDSD-approved algorithm or equipment immediately after use;

g) Application systems developers shall not develop authentication and access control systems where the controls provided by an operating system or an access control package that enhances the operating system, can be used. Designs featuring custom authentication and access control systems shall be authorised by ISS/RM Committee;

h) All workstations used for ECDSD business activity, no matter where they are located, shall use an access control system approved by the ISS/RM Committee. This system shall lock access to the workstation after a period of inactivity;

i) Every log-in process for multi-user computers shall include a special ECDSD Information Security notice;

j) Following installation of hardware or software, all default vendor passwords shall be altered;

k) If sent by regular mail or similar physical distribution systems, passwords shall be sent separately from user-IDs. These mailings shall have no markings indicating the nature of the enclosure. Passwords shall also be concealed inside an opaque envelope that will readily reveal tampering;

l) All passwords shall be promptly changed if they are suspected of being disclosed, or known to have been disclosed to unauthorised parties;

m) Whenever a system has been compromised, or suspected to have been compromised, a trusted version of the operating system and all security-related software shall also be reloaded. In addition, all recent changes to user and system privileges shall be reviewed for unauthorised modifications. All users shall be instructed to change their passwords on the compromised machine, as well as on any other machines where they used the same passwords;

n) Security administrators shall only disclose passwords if a new user-ID is being assigned, if the involved user has forgotten or misplaced a password, or if the involved user is otherwise locked out of his or her user-ID;

o) Security administrators shall not reveal a password unless the involved user has first provided definitive evidence substantiating his or her identity;

p) All users shall keep their passwords confidential;

q) A user shall never keep a written copy of any ECDSD passwords;

r) Users shall not share passwords;

s) A user will be held responsible for any actions secured with his or her password;

t) Access control to files, databases, computers, and other system resources via shared passwords is prohibited;

u) Procedures or security awareness training shall be in place to ensure that users of electronic equipment, including desktops PCs, server consoles, mobile equipment and others, are instructed to:

   i) terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, for example a password protected screen saver;

   ii) log-off mainframe computers and servers when the session is finished (i.e. not just switch off the PC or terminal);

   iii) secure PCs, laptops or terminals from unauthorized use by using a key lock or an equivalent control, for example password access, when not in use. When a computer is distributed to a user, a password protected screensaver must be activated automatically after 15 minutes; and

   iv) pay special attention to any type of small electronic devices that might easily be removed from the office and that could contain sensitive or classified data.

6.12 Remote access

a) Access to the ECDSD network via remote access shall be controlled using either one time password authentication or public/private key system with strong pass phrase;

b) Pass phrase shall not be the same as user's passwords.

7 Approving Authority

The member of the Executive Council and the Superintendent General has the responsibility to approve the departmental Password Policy

8 Accountabilities and Responsibilities

8.1 The Superintendent General

The SG working in conjunction with the CFO shall be responsible for ensuring the effective implementation and compliance of the ECDSD EC policies, standards and procedures.

8.2 The CIO

The CIO must implement, enforce and monitor the controls in accordance with the requirements outlined by management, and must advise users on the correct ways to access information and systems.

8.3 The ICT Steering Committee

Management helps achieving this objective by making sure that access to information and business processes is controlled on the basis of security requirements that are in-line with business requirements.

8.4 Internal Audit

The Internal Audit department is authorised by management to assess compliance with all corporate policies at any time.

8.5 All employees, contractors and service providers

Users must keep their access information like usernames and passwords secure, ensure that they access systems only for those purposes they were authorised to. The CIO to give access rights to external service providers when a need arises

9.Effective date of the Policy

The Password Policy is effective from the date the member of the Executive Council has approved it.

10. Monitoring Mechanisms

g) ICT Operational Committee

h) ICT Steering Committee

i) ICT Managers Meeting

The CIO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy. Such mechanisms as mentioned above shall be used to monitor this policy:

11. Review of the Policy

The policy will be reviewed every three years and whenever there are new developments to maintain relevance as and when a need is identified by the person responsible as specified above.

12. Enforcement

a) Failure to comply with this policy shall result in disciplinary action.

b) Any conduct that interferes with the normal and proper operation of the departments IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved Malicious Code Policy.

c) The ECDSD executive management reserves the right to revoke the privileges of any user at any time until such time it is deemed fit to reinstate the rights.

13. Policy Recommendation and Approval

The signatories hereof, being duly authorised thereto, by their signatures hereto authorise the execution of the work detailed herein, or confirm their acceptance of the contents hereof and authorise the implementation/adoption thereof, as the case may be, for and on behalf of the parties represented by them.

ECDSD Approval

ECDSD: Member of Executive Council: N Sihlwayi

31/March 2016.

Date

ECDSD Recommended

ECDSD: Superintendent General: S Khanyile

30/03/2016.

Date

Building a Caring Society. Together.

24 Hour Call Centre
Toll-Free Number : 080-0032-364