



social development

Department:
Social Development
NORTHERN CAPE

Information Technology Policy

*Version 7
December 2017*



social development

Department:
Social Development
NORTHERN CAPE

TABLE OF CONTENTS

Preamble.....	1
Policy Impact.....	1
Scope.....	1
Role and Responsibilities.....	1
Definitions.....	2
Legislative Framework.....	3
IT Framework	4
Departmental IT Steering Committee.....	4
Accountability of damaged or stolen IT hard- and software.....	6
Copyright.....	7
Security.....	7
Information about people.....	8
Electronic monitoring.....	8
Internet Usage.....	9
Email Usage.....	10
Passwords.....	14
Hardware and software.....	16
Managing of viruses and destructive programs.....	18
Backup procedures.....	19
Disaster Prevention.....	20
WAN Security.....	21
Disposal of Media.....	21
Notes.....	22
Disciplinary Actions.....	22
Version Control.....	23



social development

Department:
Social Development
NORTHERN CAPE

1. Preamble

The purpose of this policy is to outline the acceptable use of computer equipment in the Department. These rules are in place to protect the employee and the Department.

Inappropriate use of computer equipment exposes the Department to risks including virus attacks, compromise of network systems and services, and might have legal ramifications.

All Information Technology facilities and information resources remain the property of the Department of Social Development and not of individual employees or Programmes.

2. Policy Impact

By following the principles of this policy it will assist in ensuring that IT facilities are used:

- legally;
- securely;
- without undermining the Department;
- effectively;
- in a spirit of co-operation, trust and consideration for others;
- so they remain available.

3. Scope

This policy applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties working with and within the premises of the Department of Social Development. This policy applies to all equipment that are owned or leased by the Department.

4. Roles and Responsibilities

- | | | |
|----------|---|--|
| Users | - | should use IT hard- and software, systems, email facilities, intra- and internet appropriately and in accordance with this policy and any other legislation and policy that controls the Departments information resources. |
| Managers | - | should provide a copy of the policy to users. The subordinates should sign receipt of the policy that will serve as proof of acceptance and that they are aware of the content of the policy.
- should ensure that users comply with this policy by means of monthly inspections on internet and email usage, illegal software etc. |
| ICT Unit | - | should conduct ICT Policy compliance audits to ensure compliance |



social development

Department:
Social Development
NORTHERN CAPE

5. Definition of terms

Attachment	An electronic file that is included with an e-mail message. Attachments can be of any allowed file type. Since e-mail is limited to simple text, attachments are used to send complex data such as documents, plans or spreadsheets.
Trojan Horse	Destructive programs usually viruses or worms that are hidden in an attractive or innocent looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by e-mail or on a removable media, often from another unknowing victim, or may be urged to download a file from a web site or bulletin board.
Chain letter	A message sent to a number of people, asking each recipient to send a copy with the same request to a number of other officials. The message may be sent as part of a get-rich-quick scheme or to propagate a joke, an appeal or a protest. Chain letters can seriously degrade network performance and consume substantial storage space.
Computer virus	A computer program that interferes with, or damages, the normal operation of the computer or software. Virus programs are designed to infect computers by hiding within e-mails or executable programs.
Electronic mail/e-mail	Messages transmitted and received by computers through a network. An electronic mail, or E-mail, system allows computer users on a network to send text, graphics, and sometimes sounds and animated images to other users.
Junk mail	E-mail sent to unsolicited recipients. E-mail that is unwanted and does not relate to Departmental business.
Mail bomb	A huge number of e-mail messages sent to one destination or an e-mail with an extremely large attached file. Mail bombs are sent to antagonise recipients and to cause problems by filling up disks and overloading the e-mail system.
Mailing list	The collective name for a group of e-mail addresses to which an e-mail message may be sent simply by referring to the name assigned to the group.
Personal e-mail	E-mail sent or received that does not support official Departmental business, or activities sponsored by the Department.
Post office	The central place where mail is stored and from which it is routed to its destination.
Prescripts	Regulations, instructions and directions.
Spam/ Mass mailing	Copies of the same message sent to large numbers of newsgroups or users on the Internet. People spam the Internet to advertise products as well as to broadcast some political or social commentary.
Removable media	Removable media refers to memory sticks writable CD's and portable hard disks on which data may be stored. For the purpose of this policy the term includes any removable storage device fitted to a PC.
User	All officials utilising IT equipment in the Department of Social Development.



social development

Department:
Social Development
NORTHERN CAPE

Worm	A program that makes copies or worms—that are hidden in an attractive or innocent-looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by e-mail or on a diskette, often from another unknowing victim, or may be urged to download a file from a Web site or bulletin board.
Information Security	Includes, but is not limited to <ul style="list-style-type: none"> • Documents security; • Physical security measures for the protection of information; • Information and communication technology security; • Personnel security; • Business continuity planning; • Contingency planning; • Security screening; • Technical surveillance counter-measures; • Dealing with information security breaches; • Security investigations; • Administration and organisation of the security function in the organisation.
Information Assets	A piece of information stored in any manner which is recognised as 'valuable' to the organisation. This includes, but is not limited to, internal reports, strategic documents, data and databases, personal and sensitive information, memos, agreements, contracts and any third party information.
Risk	The likelihood of a threat materialising by exploitation of vulnerability.
Vulnerability	A deficiency related to security that could permit a threat to materialise.

6. Legislative Framework

Legal support for this policy includes:

- 6.1. Code of Conduct for Public Service which is part of the Public Service Regulations 1999 and issued in terms of the Public Service Act, 1994.
- 6.2 National Treasury Regulations, Chapter 12: Management of Losses and Claims.
- 6.3 Disciplinary Code and Procedures (Public Service Co-ordinating Bargaining Council Resolution No. 2 of 1999).
- 6.4 Copyright Act 98 of 1978.
- 6.5. Copyright Amendment Act 125 of 1992 of Interception of Communication Related Information Act
- 6.6 Electronic Communication and Transaction Act 36 of 2006
- 6.7 SITA Act 38 of 2002
- 6.8 Information Security Policy
- 6.9 Network Access Policy and User account procedures
- 6.10 National Treasury Public Sector Risk Management Framework April 2010
- 6.11 Departmental Risk Management Policy
- 6.12 Regulation of Interception of Communications and Provisioning of Communication Related Information Amended Act (RICA) 2009



social development

Department:
Social Development
NORTHERN CAPE

- 6.13 Occupational Health and Safety Act 85 of 1993
- 6.14 MISS approved by Cabinet on 4 December 1996.
- 6.15 Films and Publications Amendment Act 2009
- 6.16 Protection of Personal Information Bill, November 2013

7. IT Framework

The IT Governance Framework was approved by the Director-General on 17 January 2013. The purpose of the framework is to institutionalize the Corporate Governance and Governance of ICT as an integral part of corporate governance within NCPG Institutions.

The framework was recommended by DITC on 24 May 2013 and was adopted by the Head of Department on 7 October 2013. An implementation plan was developed in order to reach the deliverables of phase 1 as indicated in the Framework by 31 March 2014.

The Department standardize on certain elements of the following frameworks:

- COBIT – COBIT focuses on the definition, implementation, auditing, measurement and improvement of controls for specific processes that span the entire IT implementation life cycle. The objective of COBIT is to improve the quality and measurability of IT governance across the entire network application implementation life cycle or implementing a control system for improved regulatory compliance.
- Departmental Project Management Framework for ICT projects was approved by the Head of Department on 7 October 2013. This framework will be used as a structured project management framework to ensure that the classification, initiating, planning, executing, controlling and closing project stages are covered.

8. Departmental IT Steering Committee.

As indicated in the DPSA outline for CGICT Charter the ICT Strategic Committee is not necessarily a separate committee from the Executive Management Committee. Functions of the ICT Strategic Committee will be integrated in the Executive Committee.

The DPSA outline for CGICT Charter further indicates that the ICT Steering Committee is not necessarily a separate committee and the functions can be incorporated in existing structures. The functions of the ICT Steering Committee and ICT Operational Committee will be incorporated into the Departmental Information Technology Committee (DITC).

The Departmental Information Technology Committee (DITC) is in place to

- a) Inform the Head of the Department (HOD) of Social Development on issues regarding Information and Telecommunications Technology, as stipulated by the



social development

Department:
Social Development
NORTHERN CAPE

Constitution of the Republic of SA, 1996 Section 217 (1); Public Financial Management Act (PFMA) 1 of 1999 Section 38.

- b) Discuss, formulate and implement IT Strategies and Policies and inform the Users of IT accordingly.
- c) Evaluate and approve IT requisition for hard- and software

The DITC provides insight and advice to Management on topics such as:

- The alignment of IT with the business direction
- The availability of suitable IT resources, skills and infrastructure to meet the strategic objectives
- Optimisation of IT costs, including the role and value delivery of external IT sourcing
- Progress on major IT projects
- Exposure to IT risks, including compliance risks
- Containment of IT risks
- Provides direction to management relative to IT strategy
- IT governance practices
- Ensures projects continuously meet business requirements, including-evaluation of the business case
- Communicates strategic goals to project teams

The DITC considers applications on the following ICT and related matters:

- Acquisition of computers, printers, scanners, etc.
- Acquisition of ICT related equipment, e.g. data projectors.
- Software packages for computers.
- Network devices for new or extension of existing systems.
- Acquisition of Servers and storage devices.
- Upgrading of ICT Resources
- Acquisition of Local Area Networks – Structured cabling and peripherals.
- Acquisition of Network operating systems e.g. Windows 2003, 2008.
- Utilisation of electronic mail and the Internet.
- Development of software application systems.
- Acquisition of Wide Area Network links via SITA.
- Acquisition of Database management systems.
- Acquisition of ICT security systems.

Applications dealt with by the DITC must be on the prescribed application form, and should be signed by the Head of Component and forwarded to the relevant Programme Manager who must ensure that applications are sufficiently motivated and that funds are available.



social development

Department:
Social Development
NORTHERN CAPE

A user can only be issued with either a Laptop or Desktop depending on the job function. If both a Laptop and Desktop is required it should be properly motivated for consideration by the DITC.

Details of the application should be verified by means of the relevant contract, which is available on the Intranet. Quotations will be obtained from approved suppliers and in accordance to the different SITA contracts as available on <http://www.sita.co.za/>.

All applications are submitted to the Secretary of the DITC. This official should be a person from the IT component who is familiar with the procurement processes of the IT environment.

The IT section scrutinizes all applications before it is placed on the Agenda for the DITC meeting. Applications must reach the secretary at least one week prior to the meeting.

Meetings will take place on a monthly basis, usually every second Monday of each month or as determined by the Chairperson. At least 9 meetings should be held during a financial year.

The DITC follows standard meeting procedure, considers and approve normal applications for network peripherals, hard- and software and make recommendations on strategic ICT issues to the HOD.

The secretary informs the applicant of the outcome of the application in writing. The IT Unit then forwards the approved documents to Supply Chain Management who will activate the prescribed procurement procedure.

9. Accountability for damaged or stolen IT hard- and software

All users are responsible for proper utilization and safekeeping of IT hard- and software allocated to them to perform their official duties. If hard- and/or software is damaged it should be immediately reported to the ICT Unit. If IT hard- and software are stolen it should be reported within 24 hours to the SAPS, Security Management, Asset Management and ICT Unit.

The Departmental lost report should be completed and submitted to the Security Management Unit and a copy to Asset Management.

The information will then be forwarded to Labour Relations who will investigate. If it is found that the damaged or the theft was as a result of negligence by the user, he or she will be held responsible for the replacement value according to the same specification of the hard- and software provided by the Departmental ICT Unit.

It should be noted that according to Microsoft Software License agreement, the software lives and dies with the hardware and therefor it cannot be installed on another machine or transferred to another user.



social development

Department:
Social Development
NORTHERN CAPE

10. Copyright

Employees are urged to take care in using software legally in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges against the perpetrator.

11. Security

The Information Security Policy was approved by the HOD on 7 October 2013. The Information Security Policy was reviewed during July 2016 and submitted during September 2016 to the HOD for approval. The revised Information Security Policy was approved by the MEC on 7 November 2016. The objective of the policy is to provide the NCPG with an information system and information communication security policy and standards.

- 11.1 It is prohibited to attempt to gain unauthorised access to information or facilities, and any unauthorized access to information shall be dealt with accordingly.
- 11.2 Employees are advised to make use of the IT Support personnel's assistance should they need to access any information or facility that might otherwise be prohibited as stated above.
- 11.3 It is prohibited to disclose, without authorization, personal system passwords or other security details like logins and so forth to other employees, volunteers or unauthorized external third parties, as this compromises the security of the Department.
- 11.4 Only IT staff may access IT sensitive areas (server- network rooms). Proper access control and key management should be applied by means of access control registers. These registers should be verified on a weekly basis by the relevant Managers.
- 11.5 Each server or network room should have a formal maintenance register for the air conditioner. The registers should be verified on a monthly basis and the air-conditioners should be serviced on a quarterly basis.
- 11.6 No eating, drinking or smoking is allowed in IT sensitive areas or near any IT equipment.
- 11.7 In the event that an unauthorized third party gets to know an employee's password, the said employee must ensure that it is changed as soon as it is practically possible. Any losses or damage suffered by the Department or by a third party as a result of an employee's failure to have the password changed shall be the sole burden of the said employee.



social development

Department:
Social Development
NORTHERN CAPE

- 11.8 Employees are urged not to leave their unattended computers without logging off as any unauthorized use of the said computer, and consequences thereof, shall be the sole responsibility of the said employee.
- 11.9 In order to protect the Department from a computer virus contamination that can destroy information resources employees are urged to always scan removable media for viruses, even if it is believed they are clean (A procedural manual is available from the IT Unit).
- 11.10 Usage of laptop computers by employees is restricted to business purposes only, and users shall be aware of, and accept the terms and conditions of use, especially the responsibility for the security of information held on such devices.
- 11.11 All employees that remove a laptop from the premises should complete an asset removal form obtainable from Security Management and it must be approved by the relevant Manager. If an employee cannot present this document when exiting the premises, the equipment may not leave the premises.

12. Information about people:

- 12.1 Any employee who is recording or obtaining information about individuals must ensure that by doing so she/he is not violating any law. In the event of any violations ignorance of the law shall be no excuse.
- 12.2 The Department shall not be held liable in the event of an employee illegally recording, obtaining and disseminating of any information, whether true or false, about any other person. The individual employee shall be solely liable.

13. Electronic monitoring:

- 13.1 The Department respects the right to privacy of its employees, however, the individual's right to privacy does not extend to his /her work-related conduct and the use of the Department's resources. Such resources are supplied by the Department for the furtherance of its business interests and to enable employees to complete their allocated daily tasks, and as such private usage thereof is strictly restricted, with the Department reserving the right to totally prohibit it.
- 13.2 The electronic mail system (e-mail) has been installed by the Department to facilitate business communications, and remains the property of the Department, and as such the content of each and every e-mail communication remains accessible at all times to the Department as the Department has a right to protect its interests.



social development

Department:
Social Development
NORTHERN CAPE

- 13.3 The members of management designated for the purpose will at all times monitor the usage of the e-mail facility by employees and will, from time to time, read e-mail communications sent and received over the departmental network.
- 13.4 The Department reserves the right to monitor access to the internet and intercept and read e-mails at any time without notice.
- 13.5 The Department reserves the right to retrieve e-mail if it is required for evidence, whether in Court or in any enquiry of whatever nature.
- 13.6 All Officials have to be aware that merely deleting information may not necessarily remove it from the system and deleted material may still be retrieved and viewed by the Department and/or disclosed to third parties where a need arises.
- 13.7 The Department has the right to make information gathered in terms of this policy, particularly under sub-paragraph 13.5 above available internally and externally, including, where relevant, to such authorities as the police, provided that the information so obtained shall not be disseminated, published or prejudice any person, except to the extent that it is evidence in disciplinary matters.

14. Internet Usage

- 14.1 Access to the Internet will be granted to employees that have a legitimate need for such access, the user needs to apply for access formally through the respective line manager and the Programme Manager must approve the request.
- 14.2 All Internet connections shall be via the approved Internet service provider of SITA, Departmental 3G modems, ADSL and VSAT. Any other connections are prohibited.
- 14.3 Use of Internet is a privilege, which constitutes the acceptance of responsibilities, and obligations that are subject to government policies and laws. Acceptable use must be legal, ethical, and respectful of intellectual property, ownership of data, systems security mechanism and individual rights to privacy from intimidation, harassment and annoyance.
- 14.4 Users will not publicly disclose internal Departmental information via the Internet, which could adversely affect the Department, customer relations and the Department's public image and that of its employees.
- 14.5 Employees are strictly prohibited to access any websites that contain sexually explicit, profane and pornographic, socially perverse and other potentially offensive material.



social development

Department:
Social Development
NORTHERN CAPE

- 14.6 Users shall be subject to limitations on their use of the Internet as determined by the appropriate supervising authority.
- 14.7 At any time and without prior notice, management reserves the right to examine Web browser cache files, Web browser bookmarks and other information that is stored on or passing through the computers of the Department. Such management access assures compliance with internal policies, assists with internal investigations and assists with the management of the Department.
- 14.8 Any downloading, copying, printing, posting and dissemination of any sexually perverse, racially perverse material and any material derogatory of the Republic's leadership is strictly prohibited, and shall be meted out with an appropriate disciplinary sanction.

15. Email Usage

15.1 Acceptable use of e-mail in the Department

The acceptable use of e-mail includes, but is not restricted to, the following:

15.1.1 Headers and disclaimers

In order to protect the Department's image users must, at all times, attach the official Department disclaimers, which must be in the following format,

Disclaimer: *"This message contains information intended solely for the addressee, which is confidential or private in nature and subject to legal privilege. If you are not the intended recipient, you may not peruse, use, disseminate, distribute or copy this message or any file attached to this message. Any such unauthorized use is prohibited and may be unlawful. If you have received this message in error, please notify the sender immediately by e-mail, facsimile or telephone and thereafter delete the original message from your machine."*

*The Department of Social Development, **Northern Cape** does not endorse or accept responsibility for any personal views expressed in this e-mail, **nor shall it be held liable in the event of the sender distributing wrong and misleading information unrelated to the course and scope of the Department's business**".*

15.1.2 Sending e-mail

- 15.1.2.1 Users have to realize that the use of e-mail is a privilege and can be taken away if misused.
- 15.1.2.2 When accessing public e-mail servers for work purposes (e.g. Hotmail, Yahoo) or when connecting to public SMTP servers (e.g. MWeb, iAfrica) from a workstation linked to the network, users must ensure that any attachments are scanned for viruses on the user's workstation.



social development

Department:
Social Development
NORTHERN CAPE

- 15.1.2.3 A user who automatically or manually forwards his/her internal mail to public e-mail servers will be held responsible for security breaches resulting from this practice.
- 15.1.2.4 When a user feels offended by or uncomfortable with the content of an e-mail received, it is advisable to inform the sender and to report the matter to Security Management or IT.

15.1.3 Addressing

- 15.1.3.1 When a user sends an e-mail, it is the user's responsibility to ensure that the e-mail address of the recipient is correct.
- 15.1.3.2 Public address books/and or mailing lists have to be kept up to date.
- 15.1.3.3 When a user recognizes that an e-mail item has been incorrectly addressed to him/her, the user must inform the sender and delete the e-mail.

15.1.4 Restriction on e-mail attachments

- 15.1.4.1 Attachment types (mp3, avi, exe, etc) have a large impact on the network bandwidth and have therefore been restricted.
- 15.1.4.2 The following restrictions shall apply –
- (i) E-mails inclusive of attachments must be restricted to 1.5Mb;
 - (ii) E-mails larger than 1.5Mb must be compressed with compression software such as WinZip; and
 - (iii) E-mails exceeding 1.5Mb after compression will be rejected.

15.1.5 Reporting of suspected viruses

The user must immediately report any malfunction that may be related to a computer virus to IT.

15.2 Prohibited use of e-mail in the Department

The prohibited use of e-mail includes, but is not restricted to, the following:

15.2.1 Contravening the laws of South Africa

- 15.2.1.1 Employees are prohibited to use the email for any purpose that contravenes the laws of the Republic of South Africa, and this prohibition shall extend to use to victimize; intimidate; offend; ridicule and/or exploit other employees or third parties, in whatever way, and spreading or dissemination of false or malicious remarks about people, products or companies.



social development

Department:
Social Development
NORTHERN CAPE

- 15.2.1.2 The prohibition shall also extend to acts that amount to electronic fraud through misrepresentation of identity, anonymous identity or someone else's identity or password for the purpose of wronging or disadvantaging that person.
- 15.2.1.3 Sending or displaying material that does not adhere to the Department's code of conduct, such as pornographic material, racist remarks, sexist remarks and any other offensive or perverse remark.
- 15.2.1.4 Distributing copyright material in such a way that the copyright is infringed.
- 15.2.1.5 Intercepting, interrupting or changing electronic packages for malicious reasons or misrepresenting the original message.

15.2.2 Abusing bandwidth and wasting recipient's time

- 15.2.2.1 Causing congestion on the network by distribution of, for example, chain letters, bitmaps and applications that add no value to the Department.
- 15.2.2.2 Broadcasting unsolicited commercial e-mail to (junk e-mail or Spam) to mailing lists.
- 15.2.2.3 Sending inappropriate messages to groups or individuals, and spreading broadcasts without the permission of the department e-mail administrator(s).

15.2.3 Spreading malicious code (Viruses)

Any action (e.g. downloading software) that would knowingly lead to the distribution of computer viruses.

15.2.4 Personal gain

Using e-mail for personal gain, personal business activities, political activity, fund-raising and charitable activities not sponsored by the Department.

15.3 General

- 15.3.1 E-mails should not be used as a medium through which an official is disciplined.
- 15.3.2 Employees are required to print all important sent and received e-mails. These hard copies must then be forwarded to Registry for filing.



social development

Department:
Social Development
NORTHERN CAPE

- 15.3.3 An e-mail can constitute a contract, and as such employees must ensure that the language used in email messages does not indicate a commitment that an official cannot keep or is not authorised to make.
- 15.3.4 When publishing or transmitting information externally employees must be aware that they are representing the Department and are speaking on behalf of the Department, and as such if personal opinions are conveyed such must be made crystal clear in the email.
- 15.3.5 Employees must check their in-box tray at regular intervals during the working day, and must ensure that it is kept fairly empty so that it just contains items requiring the employee's action. It is thus recommended of employees to decide what to do with each email as they read it (e.g. delete it, reply to it, save the whole email in a folder, archive e-mails or extract just the useful information and save it somewhere logical).
- 15.3.6 Employees are required to keep electronic files of necessary electronic correspondence, and in order to prevent an unnecessary accumulation of paper these must not be printed unless absolutely necessary.
- 15.3.7 Employees are urged to use prefixes in the subject box whenever appropriate.
- 15.3.8 Each employee must exercise caution and respect when communicating with fellow employees and third parties.
- 15.3.9 Employees shall not forward e-mails warning about viruses without having checked with the IT Support first as these warnings are invariably hoaxes and some are in fact viruses themselves.
- 15.3.10 Employees must ensure that the subject headers of their emails are clear and relevant to their intended reader(s), and informal language or slang is avoided.
- 15.3.11 Employees should try to keep to one subject per email, especially if the content is complex as one email covering a large variety of issues is likely to be misunderstood or ignored. It is better for an intended reader(s) to have several emails on individual issues, which also makes them easy to file and retrieve later.
- 15.3.12 Employees shall not open emails unless they have a reasonably good expectation of what they contain. (An example of this would be opening a report.doc from a colleague one knows, unlike an explore.zip file sent from an address one has never heard of, which should be avoided at all costs, however tempting).
- 15.3.13 In order to protect the Department employees must alert IT Support if they are sent suspicious emails and unsolicited emails like the explore.net files.



social development

Department:
Social Development
NORTHERN CAPE

- 15.3.14 Employees are urged to keep their email signatures short. A typically short signature would contain one's name, title, phone/fax and work address.
- 15.3.15 Employees must understand how forwarding an email works, and the trail that the forwarded email leaves behind, and the consequences this might have to the employee and the Department should unsavory emails be sent.
- 15.3.16 If one forwards an email, it appears (to the reader) to come from the originator (like passing on a sealed envelope), and if it is forwarded and edited in the process, it appears to come from the person editing and forwarding - with the originator's details usually embedded in the message. This is to show that the original mail is no longer intact (like passing on an opened envelope).

16. Passwords

The Network Access Policy and User Account Procedures were approved by the MEC on 28 June 2013. The purpose of the policy is to prevent unauthorized user access to Department of Social Development information through deployment of user account and password management processes.

16.1 General

- 16.1.1 All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- 16.1.2 Passwords must not be inserted into email messages or other forms of electronic communication.
- 16.1.3 All user-level and system-level passwords must conform to the guidelines described below.

16.2 Guidelines

16.2.1 General Password Construction Guidelines

- (i) Passwords can be used for various purposes at the Department, and some of these include - user level accounts, email accounts and screen saver protection.
- (ii) Since very few systems have support for one-time passwords, users have to be aware of how to select strong passwords.
- (iii) Poor, weak passwords have the following characteristics -
 - (a) The password contains less than eight characters;
 - (b) The password is a word found in a dictionary (English or foreign);



social development

Department:
Social Development
NORTHERN CAPE

- (c) The password is a common usage word such as names of family, pets, friends, co-workers, fantasy characters, computer terms and names, commands, sites, companies, hardware, software, the words "Northern Cape Provincial Government", "Kimberley" or any derivation based on your physical location; birthdays and other personal information such as addresses and phone numbers; word or number patterns like aaabbb, qwerty, zyxwvuts, 123321; any of the above spelled backwards; and any of the above preceded or followed by a digit (e.g., secret1, 1secret).
- (iv) Strong passwords have the following characteristics -
 - (a) The password contains both upper and lower case characters (e.g., a-z, A-Z);
 - (b) The password has digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&*()_+|~-=\{}[]:"';<>?,./);
 - (c) The password is at least eight alphanumeric characters long;
 - (d) The password is not a word in any language, slang, dialect, jargon, etc;
 - (e) The password is not based on personal information or names of family, etc.
- (v) Passwords should never be written down or stored on-line.
- (vi) Employees are implored to create passwords that can be easily remembered but not so obvious. One way to do this is create a password based on a song title, affirmation, or other phrase, for example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

16.2.2 Password Protection Standards

- (i) Employees are urged not to use the same password for Department accounts as for other non-Departmental access (e.g., personal ISP account, etc.), and where possible, not to use the same password for various Departmental application access needs. For example, select one password for the Transversal Access systems such as BAS, PERSAL and a separate password for NOVEL access. Also, select a separate password to be used for any other accounts.
- (ii) Employees must never share the Department's passwords with anyone, including administrative assistants or secretaries.
- (iii) All passwords are to be treated as sensitive and confidential Departmental information.
- (iv) Employees must take note of and adhere to the following "don'ts" -
 - (a) Do not reveal a password over the phone to anyone
 - (b) Do not reveal a password in an email message
 - (c) Do not reveal a password to your superior, unless done in confidence;
 - (d) Do not talk about a password in front of others



social development

Department:
Social Development
NORTHERN CAPE

- (e) Do not hint at the format of a password (e.g., "my family name")
 - (f) Do not reveal a password on questionnaires or security forms
 - (g) Do not share a password with family members
 - (h) Do not reveal a password to co-workers while on vacation.
- (v) If, for whatever reason, a third party requests an employee's password, employees must refer the third party to this document or have the third party call the Information Technology Section.
- (vi) Employees must not use the "Remember Password" feature of applications (e.g., Outlook, Groupwise), and must not write passwords down and store them anywhere easily accessible in their offices.
- (vii) Employees must not store passwords in a file on any computer system (including Laptops or similar devices) without encryption.
- (viii) If an account or password is suspected to have been compromised, the employee concerned must report the incident to the IT Section and change all passwords.

17. Hardware and software

The ICT Unit should conduct periodic inspections on the network, PC's and laptops to ensure that no unauthorized hardware, unauthorized software and no Personal Electronic Devices is installed on Departmental ICT hardware or network infrastructure without the necessary approval.

17.1 Requests for Hardware and Software

- (i) Request for new IT equipment viz. computers, printers, projectors, etc has to be done on the prescribed IT requisition form and signed by the relevant user. In addition, the document has to be authorised by the relevant Programme Manager as well.
- (ii) Specifications for all IT equipment have to be done by IT, which will forward the relevant information to Supply Chain Management for the purchasing of the required equipment.

17.2 Unauthorised Hardware Installation.

Unauthorized hardware may include personal computers and laptops connected to network segments or hubs and peripheral communication or input/output equipment such as modems, terminals, printers, 3G routers and external hard disks or tape drives. Unauthorized hardware also includes data card devices, cellular phones and tablets connected to PC's and laptops. Unauthorised hardware installation will not be tolerated and IT should be contacted if these hardware devices need to be connected



social development

Department:
Social Development
NORTHERN CAPE

to Departmental hardware or network to ensure that the ICT infrastructure of the Department is not exposed to risks.

17.3 Personal Electronic Devices

Personal Electronic Devices include amongst other PC's, Laptops, Cellular phones, Tablets, wi-fi modems, routers ect. Personal Electronic Devices containing or accessing the information resources at the Department must be approved prior to connecting to the Departmental hardware, networks and information systems. This pertains to all devices connecting to the network at the Department, regardless of ownership.

17.4 Installing Software

- (i) No software (including public domain software) may be installed on equipment owned and/or operated by the Department without the permission of IT.
- (ii) Ripped DVD movies, mp3s, wma, any explicit and offensive images and material, etc may not be stored on any resources owned by the Department.

17.5 Use of facilities for leisure or personal purposes

- (i) The use of the Department's resources for leisure, for example sending and receiving personal email, playing computer games and browsing the Internet, is restrictively permitted for as long as such use does not;
 - (a) Attract any expenditure for the Department;
 - (b) Impact on the employee's job performance;
 - (c) Impact the performance of the computer;
 - (d) Break the law;
 - (e) Bring the Department into disrepute.
- (ii) Line managers are entitled to take the necessary action should an employee's leisurely use of the Department's equipment affect his or her performance or be a hindrance to the furtherance of the Department's interests.

17.6 Care of equipment

- (i) Employees must not re-arrange how equipment is plugged in (computers, power supplies, network cabling, modems etc.) without first contacting IT Support.
- (ii) Employees must never take food or drinks near IT equipment and into rooms which contain specialist equipment like servers.
- (iii) Laptop users should refrain from keeping their Laptops connected to the power supply if the battery is fully charged, since this will result in the battery to be damaged. This will be seen as negligence.



18. MANAGING OF VIRUSES AND DESTRUCTIVE PROGRAMS

18.1 General

Desktop and personal computers, including laptop computers, connected to the network are required to maintain and use an up-to-date version of Symantec Anti-Virus software.

18.2 Guidelines

17.2.1 All workstations whether connected to the network, or standalone, must use the Symantec Anti-Virus virus protection software and configuration.

17.2.2 The virus protection software must not be disabled or bypassed.

17.2.3 The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.

17.2.4 The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.

17.2.5 Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the IT Help Desk.

18.3 Protection Procedures

18.3.1 Employees must do back-ups of all important files on their computer(s) and keep a copy in a location other than the computer location;

18.3.2 Employees must never open attachments to emails from an unknown source, and must delete the email immediately. Even with E-mail from people known to the employee must only be opened unless and until one has separate information from the sender as to the type of attachment and its contents. Even then, the employee must not open it unless she/he has an up-to-date anti-virus software properly installed on his/her computer. Non-compliance with this could lead to loss of data;

18.3.3 Certain spread sheets and other programs or executable files attached to E-mails can contain viruses of which the sender is NOT aware, and as such employees must take no comfort if the sender tells them that an attachment did not damage their computer as virus actions are frequently random.

18.3.4 If one visits Web Sites linked to an unsolicited email message, those Web Sites frequently collect personal information from one's computer which, at best may cause one to be placed on more junk email lists, and at worst can steal credit card and other personal information stored on one's computer. Many such programs ONLY require that one clicks a button, usually marked "ENTER" to start this clandestine information collection process.



social development

Department:
Social Development
NORTHERN CAPE

- 18.3.5 If one has responded to random "Chain" emails in the past, whether for prayers or for the hope of winning money or vacations, these must be stopped with immediate effect. Criminal elements can easily use such tools to create millions of false trails for authorities to follow, thus thwarting efforts to locate and bring them to justice. Likewise, any unknown or outdated E-mail addresses must be removed from E-mail address books.
- 18.3.6 Employees are warned not to respond to an E-mail that offers to "remove you from an E-mail list" as these are usually simply verifying one's E-mail address so that it can be sold to others for more money.
- 18.3.7 Employees are advised to check if anti-virus software is installed and updated every two weeks, or at minimum, once each month.
- 18.3.8 Employees must use only software updates available from legitimate Vendor Website downloads such as Symantec, and should never download software offered in an unsolicited email, unless one knows it is from a legitimate source.
- 18.3.9 If one is not sure if his/her computer is running up-to-date anti-virus software, one may visit the following Web Site to run free security checks available from Symantec, publisher of Norton Antivirus software: http://www.symantec.com/business/security_response/definitions/download/detail.jsp?gid=savce, or contact the Information Technology Unit for a copy of the steps for updates manual.

19. BACKUP PROCEDURES

The objective of this procedure is to minimize the risk of losing valuable data files due to accidental operator error, malfunction of the office computers, and other catastrophic conditions. One would want to have his/her work files and some of his/her personal bookmarks available, should one's PC ever crash (hard drive failure) or if one's PC should ever need to be "restaged" (hard drive is wiped clean).

Without a backup from which to restore one's data, it must all be recreated from scratch! A copy of the backup procedural manual is available from the IT Unit.

19.1 Guidelines

19.1.1 Identify data

Employees are advised and urged to take note of the following list of the most commonly used programs and their associated file name extensions. (Extensions are the 3 letters that follow your filename. For example - **filename.ext**). The following is the most commonly used in Office 2000 and 2003; Word.doc, Excel.xls, Powerpoint.ppt, acrobat reader.pdf, Access. Mdb, Publisher. pub. Office 2007 extensions are as follows; Word.docx, Excel.xlsx, Powerpont.pptx, Access.accdb.



social development

Department:
Social Development
NORTHERN CAPE

19.1.2 Backing up one's data

- (i) If the quantity (volume) of one's data is not too large, between 10 to 30 Megs (MB), one would probably save oneself a bit of trouble by simply copying them to one's U: drive or Shared drive on the servers (the latter being the most preferred).
- (ii) If one has a CD or DVD (next preferred!) burner on one's PC, one may be able to copy all of his/her data to one or more discs, and this is done by simply locating the files and, using the CD burning software, copy those files to the disc(s). If one has a 'thumb drive' and the amount and size of the files are not too large, one may be able to back them up to that device. Memory sticks are the least preferred as they are not reliable.

19.1.3 Restoring one's data

- (i) If one is using removable media, simply copy the files from the media to the desired location on the hard drive. If the data already exists, one will be prompted to choose to either overwrite or cancel, and if one is using the Windows Backup/Restore utility, one should follow its instructions to recover his/her data.
- (ii) If employees have any problems on this aspect refer to the backup procedures or contact the Help Desk who will gladly assist.

20. **DISASTER PREVENTION**

20.1 Information assets become unavailable or inaccessible as a result of unpredictable events and it is impossible to install security measures to protect against every eventuality. Disaster prevention and recovery are the procedures and plans that are implemented to minimise the impact of a threat occurrence and to restore business continuity in the shortest possible time frame in the event of a threat occurrence.

20.2 The approved Departmental DRP/BCP specify emergency procedures, fall back procedures, resumption procedures and testing procedures.

- (i) Emergency procedures describe the immediate action that must be taken following a disaster event, which jeopardise business operations or human life.
- (ii) Fallback procedures describe the actions that need to be taken to restore essential business activities and support services. This may mean moving to a temporary location and operating in a degraded manner.
- (iii) Resumption procedures describe the actions that are required to restore the normal full business operation.
- (i) Testing procedures describe how and when the plan will be tested.



social development

Department:
Social Development
NORTHERN CAPE

20.3 Integral and disaster prevention and recovery is backup and restore procedures, which describe the strategy for taking backups and restoring the information in the event of information lost or corruption.

21. Wide Area Network (WAN) Security

SITA is responsible to provide a secure network infrastructure to Government Departments. All sites connected to the SITA WAN are protected by the SITA firewall and the Department complies with these security settings.

Apart from the SITA firewall, anti-virus software and WSUS patch management is also configured on workstations.

Satellite offices of the Department are not linked to the SITA WAN and gains access to the internet through 3G, ADSL and VSAT. The following measure should be in place at these Satellite Offices to ensure that workstations are protected:

- Install and update anti-virus software
- Activate firewall settings on workstations
- Deactivate wireless function on 3G, ADSL and VSAT devices.
- Configure passwords on 3G, ADSL and VSAT devices.
- Configure Internet settings to block sites not required for official business.
- During sites visits (as per individual workplan of Technicians) for IT maintenance workstations and network devices will be checked to determine compliance to ensure that workstations are protected. The IT Policy Compliance Audit template will be utilized and a summary report of findings will be submitted to the relevant Managers.

22. DISPOSAL OF MEDIA

22.1 Sensitive information may leak to outside persons through careless disposal of computer media, therefore computer media must be disposed of securely when no longer required.

22.2 Data must be erased from equipment prior to disposal.

22.3 Company data can be compromised through careless disposal of equipment. All items of equipment containing storage media must be checked to ensure that any sensitive data and licensed software is removed or overwritten prior to disposal.

22.4 Damaged storage devices containing very sensitive data may require a risk assessment, to determine if the item must be destroyed, repaired or discarded.



social development

Department:
Social Development
NORTHERN CAPE

23. NOTES

- 23.1 In-house software: This is software written or developed by staff or volunteers using Department's equipment. It is the Department's property and must not be used for any external purpose. Software developers employed at the Department are permitted to take a small "portfolio" of such in-house software source code/executables, which they may have developed, for use in subsequent work, subject to agreement with the IT Manager.
- 23.2 Personal passwords: Disclosure to other staff, volunteers or external agents: This may be necessary in some circumstances. Such a practice is allowed only if sanctioned by a member of the Management Team after discussion with IT Support. If the password is disclosed for a one-off task, the owner must ensure that his / her password is changed (by contacting IT Support) as soon as the task is completed.
- 23.3 Email aliases are pre-defined 'shortcuts' for distributing internal email to specific groups of people. IT Support can advise what these are and how to use them.
- 23.4 Web mail accounts are personal email accounts that are stored on the Internet and can be accessed from anywhere with a standard browser, e.g. home or cyber café. IT Support can advise on setting up such an account.
- 23.5 Subject box prefixes: These are "U:" for Urgent, 'FYI' for your information and 'AC:' requires action. If the email is a very brief message confined solely to the subject line, it should in addition be prefixed with "***" to indicate "just read this line".
- 23.6 Public domain software or Freeware: This is software that is available free of charge, usually by downloading from the internet.
- 23.7 Personal Data: As a guideline, employees must keep their personal data down to 10MB. Ten emails require 0.15MB on average (depends a lot on whether they have attachments). A 10-page word processed document requires about 0.1MB. Screen saver images require much more disc space and vary greatly - some may be as large as 2MB.
- 23.8 Computer Room: This room in Block H contains the Department of Social Development's servers. Only authorized personnel are allowed access to this room. This room will remain locked at all times.

24. Disciplinary Action

- 24.1 Non-compliance, violation and disregard of this policy shall result in disciplinary action and sanction against the employee concerned, and such sanction may include, depending on the circumstances and the gravity of the transgression, termination of one's contract of employment.



social development

Department:
Social Development
NORTHERN CAPE

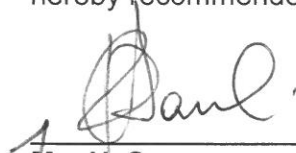
- 24.2 In addition to the above, employees shall further be bound by the Department's loss control policy, and any other policy that controls the Department's information resources.
- 24.3 In the event of the Department incurring any financial loss as a result of non-compliance, violation and/or disregard of this policy, the Department shall be entitled to institute legal proceedings to recoup the loss it has incurred from the concerned employee, and this shall be in addition to the disciplinary action the Department would have taken against the said employee.

25. Version Control

Version	Status	Date Approved
1	Approved	28 January 2008
2	Approved	14 April 2009
3	Approved	18 February 2011
4	Approved	16 February 2014
5	Approved	03 September 2014
6	Approved	15 December 2016
7	Final Draft	November 2017

Recommended

The revised Information Technology Policy for the Department of Social Development is hereby recommended by the Head of Department.



Ms. H. Samson
Head of Department

27.12.2017
Date

Approval

The revised Information Technology Policy for the Department of Social Development is approved by the Member of the Executive Council and shall come into effect from date of approval thereof.



G. van Staden (MPL)
Member of the Executive Council
Social Development

07.05.2018
Date