the dr&pw

Department:
Roads and Public Works
NORTHERN CAPE PROVINCE
**REPUBLIC OF SOUTH AFRICA**

# DEPARTMENTAL INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) ACCEPTABLE USE POLICY

**Version 1**

**(March 2015)**

# TABLE OF CONTENTS

Contents Page

# 1. DEFINITIONS AND ACRONYMS

| | |
|---|---|
| **"bandwidth"** | In computer networking and computer science, bandwidth, network bandwidth, data bandwidth, or digital bandwidth is a measurement of bit-rate of available or consumed data communication resources expressed in bits per second or multiples of it (bit/s, kbit/s, Mbit/s, Gbit/s, etc.). |
| **"bit"** | A bit is the basic unit of information in computing and digital communications. A bit can have only one of two values, and may therefore be physically implemented with a two-state device. The most common representation of these values are 0 and 1. The term *bit* is a portmanteau of binary digit. |
| **"chain letters"** | A typical chain letter consists of a message that attempts to convince the recipient to make a number of copies of the letter and then pass them on to as many recipients as possible. Common methods used in chain letters include emotionally manipulative stories, get-rich-quickly pyramid schemes, and the exploitation of superstition to threaten the recipient with bad luck or even physical violence or death if he or she "breaks the chain" and refuses to adhere to the conditions set out in the letter. Chain letters started as actual letters that one received in the mail. Today, chain letters are generally no longer actual letters. They are sent through email messages, postings on social network sites, and text messages. |
| **"Department"** | Department of Roads and Public Works, Northern Cape Province (DRPW). |
| **"denial-of- service attack"** | In computing, a denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. As clarification, DDoS (Distributed Denial of Service) attacks are sent by two or more persons, or bots. DoS (Denial of Service) attacks are sent by one person or system. |
| **"DPSA"** | Department of Public Service and Administration. |
| **"DMZ"** | In computer security, a DMZ or Demilitarized Zone (sometimes referred to as a perimeter network) is a physical or logical sub network that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of |

| | |
|---|---|
| | security to an organization's local area network (LAN); an external attacker only has direct access to equipment in the DMZ, rather than any other part of the network. |
| **"ECT Act"** | Electronic Communications and Transactions Act, Act No. 25 of 2002. |
| **"E-mail bomb"** | In Internet usage, an e-mail bomb is a form of net abuse consisting of sending huge volumes of e-mail to an address in an attempt to overflow the mailbox or overwhelm the server where the e-mail address is hosted in a denial-of-service attack. |
| **"Extranet"** | An extranet is a computer network that allows controlled access from the outside, for specific business or educational purposes. In a business-to-business context, an extranet can be viewed as an extension of an organization's intranet that is extended to users outside the organization, usually partners, vendors and suppliers, in isolation from all other Internet users. An extranet is similar to a DMZ in that it provides access to needed services for channel partners, without granting access to an organization's entire network. |
| **"Facebook"** | Facebook is an online social networking service. Its name comes from a colloquialism for the directory given to students at some American universities. Facebook was founded on February 4, 2004 by Mark Zuckerberg with his college roommates and fellow Harvard University students. The founders had initially limited the website's membership to Harvard students, but later expanded it to colleges in the Boston area, the Ivy League, and Stanford University. It gradually added support for students at various other universities before it opened to high-school students, and eventually to anyone aged 13 and over. Facebook now allows anyone who claims to be at least 13 years old to become a registered user of the website. |
| **"FTP"** | File Transfer Protocol. |
| **"Gito"** | Government Information Technology Council. |
| **"HOD"** | Head of Department, who, in terms of the PFMA is also the Accounting Officer. |
| **"ICT"** | Information and Communication Technology. |
| **"Internet"** | The Internet is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to serve several billion users worldwide. It is a *network of networks* that consists of millions of private, public, academic, business, and |

| | |
|---|---|
| | government networks, of local to global scope, that are linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support e-mail. |
| **"Intranet"** | An intranet is a computer network that uses Internet Protocol (IP) technology to share information, operational systems, or computing services within an organization. It thus refers to a network within an organization. |
| **"junk mail"** | This is a form of e-mail spam, also known as junk e-mail or unsolicited bulk e-mail (UBE), and is a subset of electronic spam involving nearly identical messages sent to numerous recipients by e-mail. |
| **"IT"** | Information Technology. |
| **"Malware"** | Malware, short for malicious software, is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. "Malware" is a general term used to refer to a variety of forms of hostile or intrusive software. |
| **"MISS"** | Minimum Information Security Standards. |
| **"MPSS"** | Minimum Physical Security Standards. |
| **"MIOS"** | Minimum Interoperability Standards. |
| **"PC"** | Personal Computer. |
| **"pyramid scheme"** | A pyramid scheme is an unsustainable business model that involves promising participants payment or services, primarily for enrolling other people into the scheme, rather than supplying any real investment or sale of products or services to the public. |
| **"SITA"** | State Information Technology Agency. |
| **"SMS"** | Short Message Service, which is a text messaging service component of phone, Web, or mobile communication systems. It uses standardized communications protocols to allow fixed line or mobile phone devices to exchange short text messages. |
| **"spam"** | Spam or Electronic spamming is the use of electronic messaging systems to send unsolicited bulk messages (spam), especially advertising, indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup |

| | |
|---|---|
| | spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social spam, television advertising and file sharing spam. It is named after Spam, a luncheon meat, by way of a Monty Python sketch in which Spam is included in every dish. |
| **"Spyware"** | Spyware is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge. |
| **"SSA"** | State Security Agency. |
| **"Trojan horse"** | A Trojan horse, or Trojan, in computing is a non-self-replicating type of Malware program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm. The term is derived from the story of the wooden horse used to trick defenders of Troy into taking concealed warriors into their city in ancient Greece, because computer Trojans often employ a form of social engineering, presenting themselves as routine, useful, or interesting in order to persuade victims to install them on their computers. |
| **"Twitter"** | Twitter is an online social networking and microblogging service that enables users to send and read "tweets", which are text messages limited to 140 characters. Registered users can read and post tweets, but unregistered users can only read them. Users access Twitter through the website interface, SMS, or mobile device app. Twitter Inc. is based in San Francisco. |
| **"Virus"** | A computer Virus is a type of malware that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected". |
| **"Worm"** | A computer Worm is a standalone Malware computer programme that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer Virus, it does not need to attach itself to an existing programme. Worms almost always cause at least some harm to the network, |

| | |
|---|---|
| | even if only by consuming bandwidth, whereas Viruses almost always corrupt or modify files on a targeted computer. |
| "WWW" | World Wide Web. |

## 2. INTRODUCTION

2.1 The departmental ICT administration's intention with an ICT Acceptable Use Policy is not to impose restrictions that are contrary to the DRPW's established culture of openness, trust and integrity. The ICT administration is committed to protecting DRPW employees and partners from illegal or damaging actions by individuals, either knowingly or unknowingly.

2.2 Intranet / Internet / Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing and FTP are the property of the DRPW. These systems are to be used for departmental business purposes, in serving the interests of the Department and the Provincial Government and of our clients and customers in the course of normal operations.

2.3 Responsible ICT use is a team effort involving the participation and support of every DRPW employee and affiliate who deals with departmental information and/or information systems. It is the responsibility of every departmental computer user to know these guidelines and to conduct their activities accordingly.

## 3. POLICY OBJECTIVE

3.1 The objective of this policy is to outline the acceptable use of computer equipment, networks and data in the DRPW. These rules are in place to protect the employee and the Department. Inappropriate use of ICT exposes the DRPW to risks, including computer Virus attacks and can compromise departmental network systems and services and have legal repercussions.

## 4. POLICY SCOPE AND APPLICATION

4.1 This policy is applicable to all employees, contractors, consultants, temporary and other workers of the Department, including all personnel affiliated with third parties. This policy applies to all ICT equipment that is owned or leased by the DRPW.

## 5. REGULATORY FRAMEWORK

5.1 The Constitution of the Republic of South Africa Act, Act No. 108 of 1996.

5.2 The Public Service Act, Act No. 103 of 1994, as amended.

5.3 The Telecommunications Act, Act No. 103 of 1996.

5.4 The Electronic Communications and Transactions Act, Act No. 25 of 2002 (the ECT Act).

5.5 The Regulation of Interception of Communications and Provision of Communication-Related Information Act, Act No. 70 of 2002.

5.6 The State Information Technology Agency Act, (SITA Act), Act No. 88 of 1998, as amended.

5.7 The Criminal Procedure Act, Act No. 51 of 1977.

5.8 The Minimum Information Security Standards (MISS) policy as approved by Cabinet on 04 December 1996, as amended.

5.9 The Minimum Information Security Standards (MISS), Second Edition March 1998.

5.10 The Minimum Physical Security Standards (MPSS) of 2009.

5.11 The Protection of Information Act, Act No. 84 of 1982.

5.12 The Promotion of Access to Information Act, Act No. 2 of 2000.

5.13 The Promotion of Administrative Justice Act, Act No. 3 of 2000.

5.14 The National Archives of South Africa Act, Act No. 43 of 1996.

5.15 The General Intelligence Law Amendment Act, Act No. 66 of 2000.

5.16 The National Strategic Intelligence Act, Act No. 39 of 1994.

5.17 The Protected Disclosures Act, Act No. 26 of 2000.

5.18 Prevention and Combating of Corrupt Activities Act, Act No. 12 of 2004.

5.19 The South African Communication Security Agency, SACSA/090/1(4) Communication Security in the RSA.

5.20 The Intelligence Service Control Act, Act No. 40 of 1994.

5.21 The Copyright Act, Act No. 98 of 1978, as amended up to Copyright Amendment Act No. 9 of 2002.

5.2.2 The Protection of Personal Information Act, Act No.4 of 2013.

5.22 The Public Service Regulations, 2001, as amended in 2002.

5.23 The Gito Council, as approved by the DPSA: Information Technology Planning Framework, 2002.

5.24 DPSA: Handbook on MISS, 2002: Chapter 6, Chapter 7, Chapter 8.

5.25 DPSA: Handbook on MIOS, 2002.

5.26 DPSA: Public Service Corporate Governance of Information and Communication Technology Policy Framework, 2012.

5.27 DPSA: Public Service Corporate Governance of Information and Communication Technology Policy Framework, Version 2, 2014.

5.28 The Northern Cape Provincial Government Information Security Policy.

5.29 The Northern Cape Provincial Government IT Governance and Governance of IT Model.

5.30 The departmental Security Policy.

5.31 The departmental policy on ICT: Standards and Guidelines.

5.32 The departmental ICT Strategic Plan.

5.33 The departmental Supply Chain Management Policy.

5.34 The departmental Asset Management Policy.

5.35 The departmental Risk Management Policy.

5.36 The departmental Risk Management Strategy.

## 6. GENERAL USE AND OWNERSHIP

6.1 While the DRPW ICT network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the departmental systems remains the property of the DRPW. Because of the need to protect the Department's network,

management cannot guarantee the confidentiality of information stored on any network devices belonging to the DRPW.

6.2 Employees are responsible for exercising good judgement regarding the reasonableness of personal use and if there is any uncertainty, employees should consult their supervisor or immediate manager.

6.3 The DRPW ICT network administration recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines and further information, kindly refer to the DRPW ICT personnel for more information.

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

6.5 The DRPW ICT administration reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

## 7. SECURITY AND PROPRIETARY INFORMATION

7.1 The user interface for information contained in Internet / Intranet / Extranet-related systems should be classified as either confidential or not confidential. Examples of confidential information include but are not limited to: government private, strategies, specifications, customer lists and research data. Employees should take all necessary steps to prevent unauthorized access to this information.

7.2 Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly: user level passwords should be changed every six months.

7.3 All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation set at 10 minutes or less, or by logging off (control-alt-delete for Windows 2000 + users) when the PC, laptop or workstations will be unattended.

7.4 Use encryption of information in compliance with SSA policy.

7.5 Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the departmental policy on Utilization of Laptop Computers.

7.6 Posting electronic mail by employees from the DRPW, using an e-mail address to newsgroups

or private companies / individuals should contain a disclaimer stating that the opinions are strictly their own and not necessarily those of the DRPW, unless postings is in the course of departmental business duties.

7.7 All hosts used by the employee that are connected to the departmental Internet / Intranet / Extranet, whether owned by the employee or the DRPW, shall be continually executing approved Virus-scanning software with a current Virus database, unless otherwise authorised by the HOD.

7.8 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain computer Viruses, e-mail bombs, Spyware or Malware.

7.9 Employees must use extreme caution when browsing the Internet, some Web Pages and Internet sites may contain Spyware, Malware or Viruses.

## 8. UNACCEPTABLE USE

8.1 The activities stipulated in this section are prohibited. Employees may be exempted from those restrictions during the course of their legitimate responsibilities (e.g. systems administration staff may have a need to disable the network access of a host if that host is disrupting departmental business operations and / or services).

8.2 Under no circumstances is an employee of the DRPW authorized to engage in any activity that is illegal under the laws of the Republic of South Africa or International Law while utilizing DRPW-owned ICT resources.

### 8.3 Systems and Network Activities

8.3.1 Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the DRPW.

8.3.2 Unauthorized copying of copyrighted material, including but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music and the installation of copyrighted software for which the DRPW or the end user does not have an active license is strictly prohibited. The end-user will be liable for fines imposed as a result of transgression of copyright laws.

8.3.3 Introduction of malicious programmes into the network or server (e.g. computer Worms, Viruses, Trojan horses or simply "Trojans", Malware, Spyware or e-mail bombs, etc.).

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

8.3.5 Using a DRPW computing asset to actively engage in procuring or transmitting material that is in violation of privacy, harassment, sexual harassment, child protection or hostile workplace laws.

8.3.6 Making fraudulent offers of products, items or services originating from any DRPW account.

8.3.7 Making statements about warranty, expressly or implied, unless it is a part of the normal job duties.

8.3.8 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, disruption includes, but is not limited to, network sniffing, pinged floods, packet spoiling, denial-of- service and forged routing information for malicious purposes.

8.3.9 Port scanning or security scanning is expressly prohibited unless prior notification to the Department's ICT administration is made.

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

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

8.3.12 Interfering with or denying service to, any authorized DRPW user (e.g. denial-of-service attack).

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

8.3.14 Providing information about, or lists of, DRPW and / or Provincial Government employees to parties outside of the DRPW and Provincial Government without the approval of the DRPW ICT administration and / or the Provincial ICT administration.

8.3.15 This list is by no means exhaustive, but attempts to provide a framework which falls into the category of unacceptable use. The above activities are strictly prohibited, with no exceptions.

**8.4 E-Mail and Communication Activities**

8.4.1 Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).

8.4.2 Any form of harassment via e-mail, telephone, SMS, Twitter, Facebook, or any form of social networking whether through language frequency or size of message.

8.4.3 Unauthorized use or forging of e-mail header information.

8.4.4 Solicitation of e-mail for any other e-mail address, other than that of the poster's account with the intent to harass or to collect replies.

8.4.5 Creating or forwarding "chain letters" or other "pyramid" schemes of any type.

8.4.6 Use of unsolicited e-mail originating from with the DRPW's networks of other Internet / Extranet / Intranet service providers on behalf of, or to advertise, any service hosted by the DRPW or connected via the DRPW's network.

8.4.7 Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam).

## 9. ENFORCEMENT

9.1 Any employees, contractors, consultants, temporary and other workers of the Department who are found to have violated this policy may be subject to disciplinary / legal action and / or criminal prosecution, including termination of employment contracts as well as any other types of contracts with the Department.

## 10. POLICY REVIEW AND AMENDMENT

10.1 This policy is effective from date of signature.

10.2 The assessment to determine the effectiveness and appropriateness of this policy will be done two (2) years after its effective date and thereafter on a bi-annual basis. The assessment could be performed earlier than two years to accommodate any substantial structural or other organizational changes at the Department or any change required by law.

10.3 If and when any provision of this policy is amended, the amended provision will supersede the previous one.

10.4 Deviations from this policy must be approved by the Accounting Officer.

## 11. APPROVAL OF POLICY AND DATE OF EFFECT

*This policy is Approved / Not Approved*

*Comments:*

.....

.....

.....

.....

.....

HEAD OF DEPARTMENT

16/04/2015
DATE

---