Northern Cape

Department of Economic Development and Tourism

Acceptable Computer Use Policy

1.0 Introduction

The department of Economic Development and Tourism Information Technology Unit's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the Department of Economic Development and Tourism's hereafter referred to as the DEDaT, established culture of openness, trust and integrity. Information technology is committed to protecting DEDaT employees, departments and partner from illegal or damaging actions by individuals, either knowingly or unknowingly.
Intranet/Internet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, World Wide Web (WWW) browsing and File Transfer Protocol (FTP) are the property of NCPG. These systems are to be used for business purposes in serving the interests of Department of Economic Development and Tourism and of our clients and customers in the course of normal operations.
Effective security is a team effort involving the participation and support of every DEDaT employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment in the DEDaT. These rules are in place to protect the employee and DEDaT. Inappropriate use exposes the DEDaT to risks including virus attacks, compromise of network systems and services and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by DEDaT

4.0 Policy

4.1 General Use and Ownership

4.1.1 While Department of Economic Development and Tourism's network

Administration desires to provide a reasonable level of privacy; users should guarantee the confidentiality of information stored on any network device belonging to DEDaT.

4.1.2 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Extranet/Intranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or immediate manager.

4.1.3 Provincial IT recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines and further information, kindly refer to the Provincial IT personnel for more information.

4.1.4 For security and network maintenance purposes, authorized individuals within Department of Economic Development and Tourism may monitor equipment, systems and network traffic at any time.

4.1.5 Provincial IT reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 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.

4.2.2 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.

4.2.3 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 users) when the PC, laptop or workstations will be unattended.

4.2.4 Use encryption of information in compliance with National Intelligence Agency (NIA) policy.

4.2.5 Because infomiation contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with "Laptop Security Tips".

4.2.6 Postings/Electronic mail by employees from Department of Economic Development and Tourism using an email address to newsgroups or private companies/individuals should contain a disclaimer stating that the opinions are strictly their

own and not necessarily those of Department of Economic Development and Tourism, unless posting is in the course of business duties.

4.2.7 All hosts used by the employee that are connected to the DEDaT's Internet/Intranet/Extranet, whether owned by the employee or Department of Economic Development and Tourism, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental policy.

4.2.8 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs or Trojan horse code.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these 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 production services.)

Under no circumstances is an employee of DEDaT authorized to engage in any activity that is illegal under the laws of the Republic of South Africa or international law while utilizing DEDaT-owned resources.

The list below is by no means exhaustive, but attempts to provide a framework which falls into the category of unacceptable use.

Systems and Network Activities

The following activities are strictly prohibited, with no exceptions:

4.3.1) 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 DEDaT.

4.3.2 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 DEDaT 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.

4.3.3 Introduction of malicious programmes into the network or server (e.g. worms, viruses, Trojans horses, email-bombs, etc.)

4.3.4 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.

4.3.5 Using a DEDaT computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.

4.3.6 Making fraudulent offered of products, items or services originating from any Department of Economic Development and Tourism account.

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

4.3.8 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 purpose of this section, disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service and forged routing information for malicious purposes.

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

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

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

4.3.12 Interfering with or denying service to any user other than the employee's department (e.g. denial of service attack)

4.3.13 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.

4.3.14 Providing information about, or lists of, DEDaT employees to parties outside of DEDaT, without the approval of Hardware and Software Support Unit.

4.4 Email and Communication Activities

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

4.4.2 Any form of harassment via email, telephone, Shoi1 Message Service (SMS), whether through language frequency or size of message.

4.4.3 Unauthorized use or forging of email header information,

4.4.4 Solicitation of email for any other, email address, other than that of the poster's account, with the intent to harass or to collect replies.

4.4.5 Creating or forwarding "chain letters" or other "pyramid" schemes of any type,

4.4.6 Use of unsolicited email originating from with DEDaT's networks of other Internet/Extranet/Intranet service providers on behalf of, or to advertise, any service hosted by DEDaT or connected via Provincial IT's network,

4.4,7 Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam).

5.0 Enforcement

Any employees found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Included below is a list of terms used in this policy and its corresponding definition:

Term	Definition
Spam	Unauthorized and/or unsolicited electronic mass mailings
Network	A network is a collection of terminals, computers, services, and components which allows for the easy flow of data and use of resources between one another,
Programmes	Also known as software. A program is simply something that allows you to work or play on the computer. Windows is a programme. Programmes are used to create documents and files for the user. Programmes are what actually put your computer to good use.
Intranet	Internal network. Companies use Intranets to share files, utilize websites, and collaborate. Usually cannot be accessed from the Internet.
WWW	World Wide Web

FTP	File Transfer Protocol. A protocol by which clients can transfer files to a server. Conunonly used to transfer files to a web server for websites or to download files from the web to install
Virus	A malicious program which attempts to replicate itself and spread. Sometimes causes problems, other times written for the enjoyment of the author.
Server	A server is a computer/device which provides Information or services to computers on a network.
Host	Host is a node or computer on a network which your workstation can log into or use resources from.
Email	E-mail (electronic mail) is the exchange of computer-stored messages by telecommunication. E-mail messages are usually encoded in ASCII text. However, you can also send non-text files, such as graphic images and sound files, as attachments sent in binaiy streams.
Internet	The Internet, sometimes called simply "the Net," is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer and sometimes talk directly to users at other computers.
Newsgroup	A newsgroup is a discussion about a particular subject consisting of notes written to a central Internet site and redistributed through Usenet, a worldwide network of news discussion groups. Usenet uses the Network News Transfer Protocol (NNTP).
Extranet	An extranet is a private network that uses the Internet protocol and the public teleconmiunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses. An extranet can be viewed as part of a company's intranet that is extended to users outside the company.