LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
COOPERATIVE GOVERNANCE,
HUMAN SETTLEMENTS & TRADITIONAL AFFAIRS

INTERNET ACCEPTABLE USE POLICY

Revised Date: 26 September 2011
Version: Final

Version Control

Version	Date	Author(s)	Details
Draft 1.0	09/05/2007	Leonard Langa	Draft Internet Policy
Draft 1.1	06/06/2007	Leonard Langa	Consolidation of GITO inputs and inclusion of Annexure A and B
2	27/05/2008	Leonard Langa	Adoption by Labour Management Forum
3	21/07/2011	Nieuwoudt Leon	Adoption by Labour Management Forum
Final	22/09/2011	Leon Nieuwoudt	Departmental name change update

Annexure A

SYS	System Config/Driver File
OCX	Active-X Components

NB: This list will be changed as and when new threats are detected.

Contents

1. Preamble

1.1 The World Wide Web is a worldwide network of computers that contains millions of pages of information. The internet is a necessary job-enhancing tool because it allows internet users access to information required to carryout and enhance their jobs when required. Recognising the importance of the internet, many organisations and government departments have implemented information systems to provide staff members with access to the internet.

1.2 However, an organisation which connects its networks to the internet exposes its information systems to all kinds of internet-borne security risks due to the open nature of the internet. Furthermore, current-day applications like e-mail, www, etc require relatively large amounts of bandwidth, of which the demand and cost is very high. As a result organisations connected to the internet need to implement technical and procedural measures to mitigate risks from untrusted networks and to ensure that internet resources are utilised in a manner which does not adversely impact normal business operations.

2. Terms and definitions

Accountability: ensuring that the actions of an entity/individual may be traced uniquely to that entity/individual, who may then be held responsible for that action

Authentication: establishing the validity of a claimed entity/verification of the identity of an individual or application

Availability: being accessible and useable upon demand by an authorised entity

Confidentiality: the principle that information is not made available or disclosed to unauthorised individuals, entities or processes

Identification and authentication: functions to establish and verify the validity of the claimed identity of a user

Information and communication systems: applications and systems to support the business, utilising information technology as an enabler or tool

Information technology: any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of vocal, pictorial, textual and numerical data or information

Integrity: the inherent quality of protection that maintains the accuracy of entities of an information and communication system and ensures that the entities are not altered or destroyed in an unauthorised manner

Monitoring: performance measurement to ensure the confidentiality, availability and integrity of operational systems and information

Password: confidential authentication information composed of a string of characters

Remote access: the access of remote users to corporate IT services by means of telephone lines or 3G data card through a gateway/computing that is performed at a location that is distant from a central site, over a network connection

GITO: Government Information Technology Office(r)

COGHSTA: Department of Co-operative Governance, Human Settlements and Traditional Affairs

VPN: Virtual Private Network

RAS DIAL-BACK: Method of using a telephone line to dial into the network

Espionage: Obtaining electronic data while not being authorised for personal gain

Cryptographic devices: Devices to encrypt and decrypt electronic data

3. Purpose

3.1 COGHSTA provides internet and World Wide Web access to all its employees and employees are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the internet. Even harmless search requests may lead to web sites with highly offensive and/or malicious content. Additionally, having a web-based email account on the internet may lead to receipt of unsolicited e-mail containing offensive and malicious content.

3.2 While COGHSTA implements adequate measures to govern internet usage, employees are ultimately responsible for any internet-related activities and any material viewed or downloaded by users from the Internet. To minimise these risks, the use of the Internet facilities at Department of Co-operative Governance, Human Settlements and Traditional Affairs is governed by this Internet Acceptable Use policy.

4. Policy Objectives

The objectives of this policy are:

4.1 To define security "laws and governance" that shall be enforced departmental wide to ensure that COGHSTA internet information systems are adequately protected from misuse or direct/indirect exposure to security risks;

4.2 To ensure the highest possible level of Confidentiality, Availability, Reliability and Integrity for the COGHSTA network, Information and information systems;

4.3 To encourage cost-effective and productive use of COGHSTA internet systems;

4.4 To clearly define user responsibilities and liability when using departmental internet facilities in day-to-day activities;

4.5 To ensure compliance with regulations of RSA and other relevant international laws, regulations, standards and best practices.

5. References, Related Legislations and Regulations

The following publications govern the execution of the internet use policy and were taken into consideration during the drafting of the internet use guidelines and policy:

SABS State Information Technology Act (Act no 88 of 1998).
Protection of Information Act (Act no 84 of 1982).
Minimum Information Security Standards (MISS), Second Edition March 1998
Departmental Internet Usage Policy,
Departmental Email Policy,
Departmental Password Policy,
Departmental ICT Security Policy,
Departmental ICT Equipment Usage Policy.

6. Scope of the policy

This policy applies to all employees (including service providers, contractors and temporary staff) utilising departmental internet systems via 3G cards, departmental computers and laptops as well as COGHSTA networks.

7. Policy Statement

Internet users are expected to use COGHSTA's internet facilities in a responsible manner which complies to the laws and regulations of RSA, other international laws as well as policies, standards and guidelines as set by COGHSTA. Access to COGHSTA's internet facilities is a privilege that may be wholly or partially restricted by the department without prior notice and without the consent of the internet user when required by and consistent with

the law, when there is substantiated reason to believe that violations of policy or law have taken place, or, in exceptional cases, when required to meet time-dependent, critical operational needs. Such restriction is subject to COGHSTA procedures or, in the absence of such procedures, to the approval of the general manager of GITO.

8. Methods of Connecting to the Internet

8.1 To ensure security and avoid the spread of viruses and other security threats, Users accessing the Internet through a computer attached to COGHSTA's network shall do so through the departmental Internet proxy server or other information security systems like firewalls, Intrusion Prevention Systems, etc. Every employee will use his or her network username and password to access the internet for accountability and reporting purposes

8.2 Bypassing COGHSTA's computer network security by accessing the Internet directly by modems, 3G cards, mobile phones connected to computers, non-departmental wireless networks or other means shall strictly be prohibited unless the computer you are using is not connected to COGHSTA's network. Disabling of or subverting any security software installed on departmental computers shall also constitute breach of this policy

9. Detection of Viruses

Files obtained from sources outside COGHSTA, including fixed and/or removable disks brought from home, files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to e-mail, and files provided by vendors, may contain security risks that may damage COGHSTA's computer network. Users shall never download files from the Internet, accept e-mail attachments from outsiders, or use disks from non-COGHSTA sources, without first scanning the material with COGHSTA-approved virus checking software. If you suspect that a virus has been introduced into COGHSTA's network, notify COGHSTA GITO immediately. If you are uncertain how to scan for viruses immediately contact GITO for assistance.

10. External Email Accounts and Instant Messaging

10.1 While external web mail accounts are not disallowed, users must ensure that these email accounts are not used to distribute and/or store official information as this might lead to intentional/unintentional disclose of sensitive official information. Only departmental email systems shall be used when distributing official information.

10.2 Due to high number of security risks associated with Instant Messaging applications like msn messenger, yahoo messenger, etc users shall not be allowed to use and install any instant messaging application on departmental computers or networks.

11. Distribution of information and data

Without prior written permission from COGHSTA, the COGHSTA's computer network shall not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, trojan horse programs, etc.) or any other unauthorised materials. Occasional limited appropriate personal use of the computer is permitted if such use does not a) interfere with the users or any other employee's job performance; b) have an undue effect on the computer or COGHSTA network's performance; c) or violate any other policies, provisions, guidelines or standards of this agreement or any other of COGHSTA. Furthermore, at all times users shall be responsible for the professional, ethical and lawful use of the departmental internet facilities.

12. Communication of Official Information

Unless expressly authorised to do so, users shall be prohibited from sending, transmitting, or otherwise distributing official information, data or other sensitive/confidential information belonging to COGHSTA through the World Wide Web. Unauthorised dissemination of such material shall result in severe disciplinary action and other appropriate actions under the laws and regulations of RSA or any international laws.

13. Discussion Groups

No COGHSTA employee shall in his/her official capacity create, participate in discussion groups on the internet without authorisation from his or her manager.

14. Copyright Restrictions

Users shall not illegally copy material protected under national and international copyright laws or distribute that material to other people. Users shall be responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. Users shall not under official duties agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of the Department.

15. Frivolous Use

15.1 Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all internet users have a responsibility to conserve these resources. As such, users shall not deliberately perform acts that waste computer/network resources or unfairly monopolise resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing online games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, accessing P2P networks/applications or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet. Furthermore, every user will have a daily limit of 30MB.

15.2 If a user exceeds this limit, his or her internet access shall be revoked and re-enabled the next day. This quota limit does not apply to authorised GITO employees who are required to download large files for purposes of computer and network supports functions. A user who requires a higher daily limit for official purposes shall send a memo to GITO clearly stating the reasons for request. Requests will be approved or declined on their individual merits and at the discretion of GITO.

16. Limitation of Privacy

16.1 Employees are given computers and Internet access to assist them in the performance of their jobs. Employees shall acknowledge and understand the openness and privacy issues relating to the internet and as such have no expectation of privacy in anything they store or distribute using the COGHSTA's internet facilities.

16.2 Employees shall consents to allow authorised GITO personnel to access and review of all materials created, stored, sent or received by users through departmental Internet facilities for the purposes of accounting, monitoring of policy compliance and internet usage statistics.

17. Discriminatory, harassing and/or offensive language

Users shall refrain from using obscene, defamatory, derogatory, discriminatory or any offensive language while using COGHSTA's internet facilities as such actions could have serious criminal, civil and moral consequences.

18. Installation and Downloading of Software

18.1 Recognising the many security risks on the internet, users are cautioned not to install or download any software from the internet as this might result in copyright violations, virus infections, and installation of adware, spyware and malicious monitoring software. Opening malicious web sites can often lead to automatic installation of malicious software and users are also cautioned not to agree to any automatic installation presented by web sites.

18.2 If a user is uncertain about how to proceed, it is his or her responsibility to get advice from GITO. A user knowingly downloads and installs any software from the internet that can compromise the COGHSTA network, information systems or other users will be in violation of this policy.

19. Additional Connections to the Internet

19.1 The department offers additional tools like 3G cards to selected employees to help enable remote internet connection and access to emails from remote locations. It must be understood that the usage of these 3G cards are governed by this Internet Acceptable Use Policy and as such 3G users shall ensure that they utilise these 3G cards for official purposes. 3G users are more vulnerable to virus attacks and other security risks from the internet as they are not protected by departmental information security systems. This means that a 3G user visiting malicious sites could unknowingly distribute security risks to other computers while connected to the COGHSTA network.

19.2 To exercise control over security risks and maintain a single point of internet connection, all users connected to the departmental network shall not be allowed to connect their 3G cards. Additionally the use of 3G cards applies only to users at remote locations. 3G cards are only intended for internet access and they shall not be used for any other purposes like making phone calls. In the instance that a 3G user uses the 3G card for making phones calls, the user shall be liable for any costs incurred and may be subject to disciplinary actions and/or revoking of the 3G card.

19.3 No internet user shall be allowed to configure or enable other connections to the internet via modems, wireless networks and cell phones on departmental computers. Any additional internet connections should be reported to GITO.

20. Monitoring and Reporting

20.1 COGHSTA accepts that the use of the Internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the Department. In addition, all of the department's Internet facilities are provided for primarily official purposes. Therefore, the Department maintains the right to monitor and log the

volume of Internet and network traffic, including but not limited to Internet sites visited, files downloaded by users, etc.

20.2 The specific content of any transactions will not be monitored unless there is a suspicion of improper use or policy violation. It may also be necessary for authorised GITO personnel to view the contents of employees' electronic communications and internet activity history in the course of problem resolution. GITO support personnel may not view an employee's electronic communication out of curiosity or at the request of individuals who have not followed the correct authorisation procedures.

20.3 Furthermore internet activities will be logged for reporting/statistics purposes and provided occasionally or on demand to GITO management to enable proper implementation of systems that will cater for the future growth demands and to ensure ongoing availability, scalability and reliability of these systems.

21. Prohibited Use

21.1 Accessing streaming audio or video, play online games

21.2 Accessing chat sites

21.3 Installing and using instant messaging applications

21.4 Download of copyrighted material including videos, music, software or any intellectual property

21.5 Accessing web sites and material that may be offensive to other employees. This includes but not limited to pornography, hate speech web sites, criminal/illegal activities, etc

21.6 Using the internet to conduct criminal or fraudulent activities

21.7 Using the internet to illegally monitor, gather information about any individual, entity or organisation.

21.8 Using the internet to intentionally subvert security systems or initiate a denial of service against any information system or network

21.9 Using the internet to conduct any personal business operations at the expense of the department's bandwidth and resources

21.10 Connecting to the internet via 3G while the computer or laptop is connected to the Departmental network.

21.11 Using the internet such that it interferes with employee productivity

21.12 Sharing of usernames and passwords used to access the internet with other people including employees

21.13 Distributing of passwords or any sensitive user account information through the internet

21.14 Impersonating, misrepresenting or suppressing a user's identity when accessing the internet

21.15 Using the departmental internet facilities to intercept or disclose, or assist in intercepting or disclosing electronic data or information.

21.16 Accessing P2P networks and web sites

21.17 Using profanity, obscenities or derogatory, sexist, racist, highly sensitive, offensive or defamatory remarks while using the internet.

21.18 Using the internet to access malicious sites and download illegal material

21.19 Use of VoIP applications not necessary for official duties e.g. skype, eyebeam, x-lite, etc.

22. Conditions for internet Access

An employee shall sign and accept the conditions and liabilities of this internet acceptable use policy before being granted access to the network. If the internet user then violates any part of this policy, remedial actions such as revoking the user's internet access and/or disciplinary may be taken. Depending on the outcome of the investigations the user shall be required to reapply for internet access by filling in the relevant forms.

23. Authorisation Procedures

23.1 For purposes of ensuring proper use accountability, control and proper use of the Internet, every employee utilising a departmental notebook, computer, 3G card shall sign an undertaking in the format Annexure B, through which, he/she will abide by the policy stipulations contained in this policy. This undertaking will be presented by GITO or the Personnel Office to the employee. The signed undertaking will be filled in the staff file of the employee. GITO/Personnel Office will take all steps to ensure that all the employees are provided with these undertaking forms. Failure to sign shall lead to existing internet access for that employee revoked.

23.2 In addition to signing the undertaking, a network logon message shall be presented through which an employee will further agree to abide by the provisions and aspects of this policy and any other relevant policy. This logon message shall clearly indicate where the user can locate the policies for review. At this point the user shall also be presented with an option to either agree to the policies by clicking the OK button or disagree by clicking the cancel

button. Network resources shall not be available to any user who does not agree to abide by and be legally bound by the internet acceptable use policy.

24. Internet User's Responsibilities

All internet users shall be responsible, accountable and liable for all their activities while browsing the internet. As such the internet user has the following responsibilities:

24.1 Ensure that their usernames and passwords are kept secure and not shared

24.2 Fully comply with all aspects of this policy

24.3 Immediately alert GITO (Information Security/Incident Response) about any misuse and non-compliance.

24.4 Duty not to waste computer/network resources

24.5 Understand that the information or data sent via the internet may/can be intercepted by other individuals and ensure that they fully acknowledge this privacy concern.

25. Consequences of Non-Compliance

Non-compliance of this policy may lead to disciplinary actions, legal liability as well as internet privileges for the user in violation revoked.

26. Implementation

This policy comes into effect from the date of approval.

27. Policy Review

This policy shall be reviewed annually.

COMPILED BY

---------- ----------

SENIOR MANAGER: Acting

INFORMATION TECHNOLOGY

28/09/2011

DATE

ACKNOWLEDGED BY:

departmental internet acceptable use policy has been revised to incorporate AGIs comments & departmental name change.

28/09/2011

GENERAL MANAGER: **DATE**

GOVERNMENT INFORMATION TECHNOLOGY OFFICE

ACKNOWLEDGED BY:

Noted and Supported.

24/10/2011

SENIOR GENERAL MANAGER: **DATE**

SHARED SERVICES

ADOPTED /~~NOT ADOPTED~~:

02/11/11

HEAD OF DEPARTMENT **DATE**

APPROVED/~~NOT APPROVED~~

Approved

Mokhaura

HONOURABLE MEC

04/11/2011

DATE