DEPARTMENT OF AGRICULTURE

INTERNET USAGE POLICY

1. INTRODUCTION

This policy objective is to guide the behaviour and usage of departmental Internet services in view of the fact that these services are becoming a critical lifeline for conducting business in the electronic business environment. Any user of a workstation linked to the department of Agriculture Network and who has access to the non-governmental sector is subject to this policy.

The department has acquired access to the Internet via the OpeNet Wide Area Network (WAN). Offices connected to the OpeNet can access the Internet through their Local Area Network (LAN).

The Internet is one of many efficient and timely communication tools that can be used to accomplish government, with other governmental departments, with business partners, and with the public. It can facilities communication and dissemination knowledge, encourage collaborative projects, resource sharing, and service provision, and build a broader infrastructure to support the performance of professional, work-related activities. As with any department-provide resource, the use if this resource should be limited to legitimate department business and is governed by rules of conduct similar to those applicable to the use of other information technology resources.

Although Internet access can provide significant benefit for the department, it is important to point out that use of the Internet exposes the department, its components, and users to Internet related risks. The internet is not one administrative entity, but rather is a co-operative effort between educational institutions, government departments, and various commercial and non-profit organizations Internet is now an exclusive domain of research and is made for educational groups to shared information in the business and government sector.

Even with the extensive effort that been made by the department to minimize risks, there is no known way to protect the department from all related risks. The department must therefore address legal, security, and productivity issues associated with how the Internet is used. Examples of such are:

- Litigation could be brought against the department if Internet users contravene the laws of the Republic of South Africa. Similar litigation could be brought against a user impacting on the rights of other people. Users could be using practices that are unacceptable in the international arena, thereby having a negative impact on the image.
- Receiving computer viruses from the downloading and use of programs and/or -files -from Internet sources. Viruses are spread through inappropriate use of the Internet and recovery of lost data costs department dearly.

- Employee could transmit information which might include passwords, sensitive data or correspondence
- Users could also be induced by the vast social and informational forums of the Internet and spend *significant* work time on non-state business related activities. Users could be wasting their productive time that department contracted them for.
- Users could consume limited disk storage on department serves and on user PC's with information that has been downloaded from the Internet. Expensive bandwidth could congest by non-productive internet traffic this will cause poor response time for internet.
- The confidential information, data security, WAN and LAN can be intruded by hackers.

Thus, the department should ensure that Internet users must exercise prudence and caution in using this powerful information resource. The sections which follow outline policy and address responsibilities are available for all approved . users.

2. PURPOSE

This policy is to establish guidelines and minimum requirements governing the acceptable usage of the department-provided Internet access. By establishing and maintaining compliance with this policy, risks and costs can be reduced while the valuable potential of this information resource tool is realized. The objectives of this policy are to assure that:

2.1 The Internet access is utilized for official purposes for the benefit of the department.

2.2 Disruptions to department activities from inappropriate use of department-provided Internet access are avoided

2.3 Users are provided with guidelines describing their personal responsibilities regarding confidentiality, privacy and acceptable use of department-provided Internet access as defined by this policy

3. SCOPE

This policy applies to all employees of the department and contracted personnel (hereinafter referred to as 'users') whose access to or use of Internet services is funded by the department or is available through equipment owned or leased by the department.

4. PROCEDURES FOR APPLICATION OF INTERNET CONNECTION

User request for Internet connection must be in writing and authorized by the Head of Component. The appropriate IT request form should be completed adequately. Section 6 (motivation part) of IT request form should be dealt with

adequately. Do not assume that the committee knows your job, but motivate in full to ensure that the committee will have clear picture of your situation.

He requested IT request form will be submitted to the committee meeting for recommendations. After, approval by the Head of Department, the IT section will complete the required form requesting SITA to provide access for the user. The Internet usage account will be monitored and reports will be circulated to the relevant line function management on the monthly basis.

5. DIRECTORATE'S RESPONSIBILITY

5.1 Each directorate is responsible for the activity of its users and must familiarize each user with what is considered appropriate use of department-provided Internet access. A 'Use Agreement' which stipulates compliance to this 'Internet Policy' must be signed by each user if they are to retain or be provided Internet access by the department.

5.2 Failure to sign the use agreement will result in denial of Internet access privileges to the user. Directorates may consider providing additional restrictions and guidelines regarding the use of the Internet within their local environments (e.g. time restrictions). Directorates are directly responsible for management of staff Internet usage.

5.3 Information Technology section must provide reports on the use and misuse of the Internet facilities of the department network. The reports must be provided regularly on monthly basis to line-function managers of the department.

5.4 The head of Section/Directorate/Immediate supervisors must ensure that the user gives an employer/government a written consent that he/she gives a permission to employer to intercept his/her communication in terms of the regulations of the Interception of Communication Related Information Act, 2002 (Act No. 70 of 2002).

5.5 Directorate must assume financial responsibilities for the usage.

6. USER'S **RESPONSIBILITY**

6.1 This policy is intended to illustrate the range of acceptable and unacceptable uses of the department's Internet facilities and is not necessarily exhaustive. Questions about specific matter related to security issues not highlighted in this policy document and reports of specific unacceptable uses, should be directed to the IT section.

6.2 Because of the security, legal, and productivity issues related to in this policy, each user has the following responsibilities:

6.2.1 a portable computer or other PC for official purposes, may such software program be loaded on a portable computer or other personal computer.

6.2.1 users must be aware of the classification of any information contained in data files or correspondence, which they are transporting/transmitting using Internet access. They must also not exchange confidential information in un-encrypted form. Under no circumstances should data ever be transported/transmitted, which if intercepted, would place the Department of Agriculture in violation of any law.

6.2.3 the contents of anything exchanged (sent or received via Internet access (regardless of its state of encryption) must be appropriate and consistent with department of Agriculture policy, subject to the same restrictions as any other correspondence.

6.2.4 users granted legitimate access to Internet connection, has the permission to use Internet resources provided information required is job related.

7. **PROHIBITED** USE **OF THE** INTERNET

The prohibited use of the Internet includes, but is not restricted to, the following:

7.1 **Violating the values of department of Agriculture**

7.1.1 Visiting sites or displaying material downloaded from sites that do not adhere to the Department of Agriculture's code of conduct, e.g. pornographic sites, etc.

7.1.2 Participating in chat rooms where the subject and/or discussion do not adhere to the Department's of Agriculture code of conduct.

7.2 Conducting **Internet** practices **that could lead to litigation** against the **Department of Agriculture**

7.2.1 Intercepting, interrupting or changing electronic messages for malevolent reasons or misrepresenting the original message

7.2.2 Attempting to gain, or gaining unauthorised access to computer resources on the Department of Agriculture network or any external network (hacking)

7.2.3 Attempting to bypass, or bypassing, the security measures of the Department of Agriculture or any other company.

7.3 Contravening laws of the Republic of South Africa

7.3.1 Uses that could lead to civil or criminal litigation against department of Agriculture by, for example, placing libellous remarks about products or companies or persons on websites.

7.3.2 Electronic fraud through misrepresentation of identity, the use of an anonymous identity or someone else's identity or password, for the purpose of disadvantaging that person.

7.3.3 Distributing or using copyright material in such a way that the copyright is infringed.

7.4 Disclosing confidential information

7.4.1 Unsecured sending of Department of Agriculture confidential information that could lead to accidental or premature disclosure.

7.5 Abusing bandwidth

7.5.1 Internet bandwidth is shared between all users with the effect that inconsiderate behaviour will impact on all fellow-users. The following statements about prohibited behaviour specifically address this issue:

7.5.2 Causing congestion on the network by, for example, watching webcams or loading video clips, audio files or applications that are no value to the department.

7.5.3 Excessively using automated downloads, search programs, polling programs (e.g. web pages that continuously update sports results and music) on the Internet

7.6 Unauthorised use of User ID's

7.6.1 Using someone else's user Id without proper permission

7.7 Spreading malicious code (viruses)

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

7.7.2 Establishing any type of connection that bypasses a properly configured and authorised firewall infrastructure that filters traffic and blocks unauthorised access.

7.8. Personal gain

7.8,1 Using Internet facilities for personal gain, outside business activities, political activities, fund raising or charitable activities not sponsored by Department of Agriculture.

8. PRINCIPLES OF ACCEPTABLE USE

8.1 Employees with Internet access should be encouraged to use the Internet for research, education, and communications, provided it is for furthering their component's mission, to provide effective service of the highest quality to the Department's clients, to discover innovative and creative ways of using resources and improving services, and promoting staff development.

8.2 Use of the Internet has the potential to enhance its users' access to and use of relevant job-related information and knowledge. Use of the Internet is a privilege that implies the acceptance of responsibilities and obligations that are subject to government policies and laws.

8.3 Acceptable use must be legal and ethical, and respects of intellectual property, ownership of data, systems security mechanisms, and individual rights to privacy and freedom from intimidation, harassment and annoyance. Users may be subject to limitations on their use of the Internet as determined by the appropriate supervising authority.

8.4 Department of Agriculture Internet users are required to:

8.4.1 Respect the privacy of others;

8.4.2 Respect the legal protection provided to programs and data by copyright and license;

8.4.3 Protect data from unauthorised use or disclosure as required by Provincial and National laws and regulations;

8.4.4 Respect the integrity of computing systems;

8.4.5 Safeguard their accounts and passwords; and

8.4.6 Respect the Internet as a shared resource.

9. ACCEPTABLE ACTIVITIES

Acceptable Internet activities are those that conform to the purpose, goals, and mission of the Department of Agriculture and to each user's job duties and responsibilities. The following list, although not all-inclusive, provides some examples of acceptable uses:

9.1 Access to other state, or local government Internet home pages;

9.2 Communications, including information access and exchange, for professional development or to maintain job knowledge or skills;

9.3 Activities involving research and information gathering; and

9.4 Communications for administrative purposes.

10. SECURITY IMPLICATIONS

10.1 IT Services Component must recognise that additional security threats exist when connected to the Internet. With World-Wide Internet connections, it may be possible for someone to access Departmental systems from the other side of the world and exploit any vulnerabilities.

Since the Internet and its tools adhere to open and documented standards and specifications, it is inherently an unsecured network that has no built-in security controls. Confidential and sensitive information must not reside on Internet servers or systems, or be included in electronic communication available for public access unless proper, formalised security precautions have been established.

10.2 It is the responsibility of the IT Services Component to protect confidential and sensitive information where intentional, inappropriate or accidental disclosure of the information might expose the Department or an individual to loss or harm. The Department must take all appropriate measures to secure information systems and comply with state security standards.

10.3 It is the IT Services Component's responsibility to implement internal security against compromise from any source, including access to and from the Internet, and for keeping their organisational systems free from unauthorised access. OpeNet will take steps to make the WAN as secure as possible, but the Department of Agriculture shares in the responsibility to protect its LANs and systems.

11. ENFORCEMENT AND VIOLATIONS

The IT Services Component, together with the various Directorate management teams is responsible for implementation and enforcement of this " Internet Policy". These duties include, but are not limited to:

11.1 Investigation of alleged or suspected non-compliance with the provisions of this policy;

11.2 Suspension of service to users, with or without notice, when deemed necessary for the operation and/or integrity of the communications infrastructure, connected networks, or data. OpeNet is able and reserves the right to monitor and/or log on to all network activity without notice, including all Internet communications, Therefore, users should have no reasonable expectation of privacy in the use of these resources. By participating in the use of networks and systems provided by the Department, users agree to be subject to and to abide by policies governing their usage.

11.3 Employees who violate the content of this policy or perform any illegal action in relation to rules and regulations outlined in this policy will be subject to disciplinary actions in terms of the Disciplinary Code and Procedures of the Public Service.

11.4 Directorate management will review alleged violations of this policy on a case-by-case basis. Clear and willful violations or abuse of what is considered to be acceptable use will be subject to appropriate disciplinary actions and depending upon the severity of the transgression and policy abuse, disciplinary action may be initiated in appropriate instances.

11.5 Should the department suffer any loss or damage through the illegal actions of a computer user, such value of loss or damage will be recovered from the person responsible in accordance with Regulation 12 of the Treasury Regulation 2001.

12. **WRITTEN** AGREEMENT **REQUIRED**

12.1 Users having access to the Internet are advised that all such network activity is the property of the Department, and therefore, they should not consider any activity to be private. All users of Internet services are required to acknowledge acceptance of and intention to comply with this "Internet Policy" by signing the Department's Information Technology User Declaration Agreement.

12.2 The "Use Agreement" is attached at Annexure 'A'. Signed agreements will be maintained by each Directorate and a copy thereof, forwarded to the IT Services Component.

13. PARTIES CONSULTED

- National Intelligence Agency
- Department of the Premier: State Law Advisor

ANNEXURE B

DECLARATION

INTERNET USER
NAME _____
PERSAL NUMBER _____
IP ADDRESS _____

I hereby declare that I:

1) have read and understand the contents of the 'Internet' Policy
2) agree to comply with the above-mentioned policy,
3) will be subject to disciplinary action in terms of the Disciplinary Code and Procedures of the Public Service for violation of this policy,
4) will use the internet provided to me only for official purposes,
5) will allow my employer to investigate and institute charges against me for any violation of this policy.
6) will be held responsible and liable for any misuse of the Internet,

Signed at_____ on this_____ day of _____

Internet user _____

Witness _____

Annexure B

DEPARTMENTOFAGRICULTURE

CONFIDENTIALITY OF INFORMATIONFORM

The department information is considered confidential unless otherwise indicated. Department information is any information which is in the possession of a department or that contains information on the department works, function, etc, whether verbal, written or in any electronic or computer format.

No portion of document or data may be reproduced, stored in a retrieval system or transmitted in any form or by means, electronic, mechanical, or otherwise, for commercial or other gain, without the prior written permission of the department.

Your attention is also drawn to Item M4.412, Chapter M, Code of Conduct for Public Service, Public Service Act, 1994, where in the performance of his/her duties an employee 'honours the confidentiality of matters, documents and discussion, classified or implied as being confidential or secret.'

You are therefore reminded of the above and must ensure that you understand it and adhere to it all times. Failure to d o so will constitute and act of misconduct and disciplinary action may be followed accordingly.

I _____ hereby declare that I have been made aware of the above contents and will endeavour to abide by it all times.

Name; _____

Rank: _____

Persal number: _____

Place: _____

Date: _____

Witness 1: _____

Witness 2: _____