DEPARTMENT OF AGRICULTURE

E-MAIL POLICY

1. INTRODUCTION

The policy will be able to prevent threats, legal charges and litigations against the department since al employees would be aware of the corporate rules and regulations. The e-mail policy should be implemented to protect the government and can minimize the department liability for employee's actions. It can also prove that the department has taken steps to prevent inappropriate use of the e-mail system and therefore can be freed of liability.

It is essential to place an e-mail policy that states the possibility of e-mail monitoring systems, when the department can decides to use e-mail filtering software to check the contents of employee's e-mails, otherwise, it can be held liable for privacy infringement. The contents of e-mail policy should be made available and easily accessible to all employees.

2. OBJECTIVE

The aim of this policy is to promote responsibility and accountability for e-mail use. This is to ensure that procedures and controlling mechanisms are implemented, evaluated and monitored to ensure efficiency and effectiveness of utilization of e-mail facilities. This policy is to establish criteria for measurement of risk management and prevention of legal threads and litigation against the department.
This policy is in compliance and guided by the following principles:

- SITA Act
- Treasury Regulations
- Disciplinary Code and Procedures of the Public Service
- PFMA

3. LEGAL RISKS

E-Mail is a communication tool and resource asset that needs to be used and managed in a responsible, effective and lawful manner. The e-mail users must be aware of the following legal risks of e-mail:

3.1 If an employee send message or and attachments(s) that contains virus, the employee and the government can be held liable.

3.2 If an employee send e-mail with any libelous, defamatory, offensive, racist or obscene remarks, the employee and or government can be held liable.

3.3 If employee forward e-mail with libelous, defamatory, offensive, racist or obscene remarks, the employee and or government can be held liable.

3.4 If employee unlawfully forward or copy message without permission, the employee and or government can be held liable.

3.5 If employee unlawfully forward or send confidential information, the employee and or government can be held liable.

3.6 Users are not allowed to subscribe to any other private E-Mail box, e.g. hot mail.

3.7 Not to connect modem at the book of PC without prior approval.

3.8 Not to connect to LAN and Built-in modem at the same time

By following the guidelines in this policy, the user can minimize the legal risks involved in the use of e-mail. If the user disregards the rules set out in this e-mail policy, the user will be fully liable and department will disassociate itself from user as far as legally possible.

4. LEGAL REQUIREMENTS

The following rules are required by law and are to be strictly adhering to. It is prohibited to:

4.1 Send unsolicited e-mail messages including 'junk e-mail' or other advertising material to individuals. This includes but not limited to, bulk mailing of commercial advertising, information announcements and political tracts. Such material may only be sent to those who have explicitly requested it. If recipient asks to stop receiving e-mail, then the user must not send that person any further e-mail. This doe not apply to normal business information messages.

4.2 Send or forward e-mails containing offensive or disruptive content, which includes, but not limited to defamatory, offensive, racist or obscene remarks.

4.3 Forge or attempt to forge e-mail messages. It is a violation of this policy to forge an electronic mail signature to make it appear as though it originated from a different person, whether through unauthorized used or forging, or mail header information alteration. Disguise or attempt to disguise identity when sending mails.

4.4 Copy a message or attachment belonging to another user without permission of the originator. It is a violation to use other user's name, password, IP address, account to retrieve other user's messages.

4.5 Sending chain letters and 'pyramid schemes' or any nature whether or not the recipient wishes to receive such mailings.

4.6 A person's e-mail address is considered public information. User name and password can not be release to another user without authorization from higher authority. Authority must be obtained from Director. If the employee is permitted to give out user address to other individual, but it must not be for the purpose of advertising, mass mailing or other commercial.

4.7 Newsgroup spasms or USENET spasm (posting same or similar messages to large number of newsgroups or individual) are strictly prohibited. User need to request permission from their supervisor before subscribing to a newsletter or newsgroup.

4.8 User whose service with department of Agriculture has been terminated will have no right of access e-mail facilities.

5. PROCEDURES

5.1 User should complete required IT request form and be submitted to the IT section for evaluation.

5.2 The IT section should submit adequate motivated and completed form to the D1TC meeting for recommendation and approval by the Head of Department.

5.3 Written approval IT request must be channeled to the relevant e-mail system controller for further processing. The e-mail connection together with e-mail address and account will be made available to the user, after approval been granted.

5.4 No amendments should be made on approved IT request unless again approved by the Head of Department.

5.5 After, approval the user will receive a copy of approved IT request (e-mail connection).

5.6 IT Manager must ensure that 'Confidentiality of Information' and 'Declaration' forms are signed by the user.

5.7 IT Manager should provide information session on the contents of this policy to ensure that user understands what is expected of him/her.

6. THE MANAGERS **AND SUPPORT STRUCTURES**

The implementation, monitoring and control of this policy shall be a shared responsibility of all members.

They must ensure that users are strictly adhering to the contents of this policy by making user to sign the 'declaration' and 'confidentiality of information' forms.

7. IT MANAGER

The IT Manager should ensure the following;

7.1 Logical access to the e-mail system shall be restricted to authorized users and unique IP address, surname, password shall be sued to validate a user's identity before access to the system.

7.2 Establish and implement mechanisms and software to filter and prevent unlawful and commercial use of e-mail.

7.3 Install software that will filter and prevent newsgroup spasm or USENET spasm.

7.4 Provide sound back-up system facilities to restore data after disaster has occurred. Back-up copies of essential business information and software should be taken regularly. Adequate back-up facilities should be provided to ensure that all essential business information can be recovered.

8. USERS RESPONSIBILITY

8.1 User must obtain a written approval before he/she accesses e-mail facilities.

8.2 User must sign the 'Confidentiality of information' and 'Declaration' form.

8.3 E-Mail should be written in a well structured manner, short and with descriptive subjects. E-Mail must not be written in capitals. They should be

marked important if they are really important. Unnecessary attachments should not be sent. E-Mail should be checked everyday.

8.4 User should maintain e-mail by deleting unnecessary copies and empty the 'deleted item' folder. Essential copies/documents should be send to registry for record purpose or make book of critical information.

8.5 Sending of personal e-mails, chain letters, junk mail, jokes is prohibited.

8.6 User should request permission from supervisor before subscribing to a newsletter r newsgroup.

8.7 Confidential information must never be sent via e-mail.

8.8 The following disclaimer should be added to outgoing mail: "This e-mail and any files transmitted with it are confidential and intended solely for use of the individual or entity to whom they addressed. If you have received this e-mail in error please notify the system manager. Please note that any views or opinions presented in this e-mail are solely those of the author and do not necessarily represent those of the department. The recipient should check this email and any attachment for presence of viruses. The department accepts no liability for any damage caused by any virus transmitted by this e-mail".

9. MONITORING AND COMPLIANCE

9.1 Compliance with this policy shall be monitored by IT security structures in conjunction with the IT Manager and support structures. The real-time system monitoring mechanism shall be implemented in sensitive and classified system to ensure the timeous detection of any deficiency. Monitoring tools shall be utilized by authorized personnel to perform integrity checks on system software and to check configuration vulnerabilities.

9.2 Internal control measures may include frequent and periodic assessment of messages send and received announced and unannounced audits of computers to ensure compliance with this policy and applicable legal provisions.

9.3 Users expressly waive any right of privacy in anything they create, store, send or receive on the department's computer system. The government can, but not obliged to monitor e-mails with prior notification. If there is evidence that a user is not adhering to the guidelines set out in this policy, the government reserves the right to take disciplinary actions, including termination and or legal action.

10 LAW ENFORCEMENT AND VIOLATIONS

10.1 IT Manager and Support structures shall investigate any violation of this policy. They should prepare and maintain records on any incidents or violations.

10.2 The employee who violate the contents of this policy or perform any other illegal action in relation to e-mail program will be subject to disciplinary action in terms of Disciplinary Code and Procedures of the Public Service.

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

11 WRITTEN AGREEMENT REQUIRED

11.1 All employee of the department must acknowledge acceptance and compliance with the 'E-Mail' policy by signing the attached 'Confidentiality of information' and 'Declaration' forms.

11.2 The 'declaration' form is attached as annexure 'A' and 'Confidentiality of Information' form is attached as annexure B. The IT Manager and Support structures must ensure that signed forms of all employees are received and placed on record.

12. PARTIES CONSULTED

National Intelligent Agency

Department of Premier - State Law Advisors

ANNEXURE 'A'

DEPARTMENT OF AGRICULTURE

DECLARATION BY

Name: _____

Persal: _____

IPAddress: _____

Directorate: _____

I hereby declare that I:

1. Read and understood the contents of the Policy – 'E-Mail'

2. Agree to comply with the contents mentioned in 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 the above-mentioned policy.

4. Will use the computer equipment provided to me only for official purpose.

5. Will allow my employer to investigate and institute charges against me for any violation of this policy.

Signed at _____ on this _____ day

of _____ year _____