



LIMPOPO

PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
COOPERATIVE GOVERNANCE,
HUMAN SETTLEMENTS & TRADITIONAL AFFAIRS

ELECTRONIC MAIL ACCEPTABLE USE POLICY

Date: 12 March 2013
Version: 3.0

TABLE OF CONTENTS

TERMS AND DEFINITIONS	3
ACRONYMS	5
1. PREAMBLE	6
2. PURPOSE AND OBJECTIVES	6
3. LEGAL FRAMEWORK.....	7
4. SCOPE OF APPLICATION.....	7
5. EXTERNAL EMAIL, INSTANT MESSAGING AND MOBILE DEVICES	7
6. PREVENTION OF MALICIOUS SOFTWARE.....	8
7. COMMUNICATION OF OFFICIAL INFORMATION.....	9
8. FRIVOLOUS.....	9
9. LIMITATIONS OF PRIVACY.....	10
10. DISCRIMINATORY, HARASSING, AND OFFENSIVE LANGUAGE	11
11. MONITORING AND REPORTING.....	11
12. ACCESS TO ANOTHER EMPLOYEE EMAIL	11
13. AUTOMATIC FORWARDING OF EMAILS	12
14. MAILBOX LIMITATION.....	13
15. EMAIL RETENTION AND ARCHIVING	13
16. CHAIN LETTERS, HOAX, AND SPAM EMAILS	13
17. PROHIBITED USE	13
18. DISCLAIMER.....	14
19. AUTHORIZATION PROCEDURE.....	15
20. EMAIL USER RESPONSIBILITY	16
21. GITO RESPONSIBILITY	16
22. CONSEQUENCES OF NON- COMPLIANCE.....	16
23. INCEPTION DATE	16

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 authorized entity

Confidentiality: the principle that information is not made available or disclosed to unauthorized 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, utilizing 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 unauthorized 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

ACRONYMS

3G	3 rd Generation Networks
CoGHSTA	Department of Co-operative Governance, Human Settlements and Traditional Affairs
GITO	Government Information Technology Office(r)

1. PREAMBLE

- 1.1. CoGHSTA provides Email facilities to all employees, contractors and service providers who utilize its network and/or network resources to enhance business operations, improve the sharing of information in an effort to accelerate service delivery to the public.
- 1.2. CoGHSTA recognizes that principles of freedom of speech, confidentiality and integrity of information have such that CoGHSTA has implemented Email content filtering systems implications on the use of email facilities to ensure that the use of Email facilities is in line with departmental requirements and objectives.

2. PURPOSE AND OBJECTIVES

The purpose of this policy is to establish minimum rules, guidelines and standards for controlling email access, usage, and administration.

The objective of this policy is to:

- 2.1. Protect the integrity and public image of CoGHSTA;
- 2.2. Help boost productivity and prevent misuse of email facilities and network resources by clearly defining rules and restrictions for personal use;
- 2.3. Ensure that Email users are notified about the applicability of laws, regulations, standards, guidelines and best practices;
- 2.4. Ensure cost-efficient use of CoGHSTA email facilities and prevent monopolizing of resources;
- 2.5. Ensure that disruptions to CoGHSTA email facilities are minimized;
- 2.6. Ensure that Email users are informed on how concepts of privacy and security are applied to Email use.

3. LEGAL FRAMEWORK

The following publications govern the execution of the Email Acceptable Use Policy and were taken into consideration during the drafting of this guidelines and policy:

- 3.1. State Information Technology Agency Act (Act no 88 of 1998).
- 3.2. Protection of Information Act (Act no 84 of 1982).
- 3.3. Minimum Information Security Standards (MISS), Second Edition March 1998
- 3.4. Departmental Internet Usage Policy,
- 3.5. Departmental Password Policy,
- 3.6. Departmental ICT Equipment Usage Policy,
- 3.7. Departmental ICT Security Policy.
- 3.8. Departmental Communication Policy.

4. SCOPE OF APPLICATION

This policy is applicable to all employees of the CoGHSTA, including learners and interns as well as all other stakeholders who make use of the CoGHSTA ICT network.

5. EXTERNAL EMAIL, INSTANT MESSAGING AND MOBILE DEVICES

- 5.1 The use of external email accounts such as web mail, etc is not prohibited but for security reasons, email users shall not use these external email accounts to send, receive and store any official information and/or data. These email accounts are outside the control of GITO or CoGHSTA and as such their confidentiality, integrity and availability cannot be assured.
- 5.2 Instant Messaging applications such as MSN, Yahoo messenger, etc are prone to malicious code. More precisely, these applications can be used as entry points for viruses and worms into CoGHSTA computer network. There are also confidentiality concerns with these applications and as a result Instant

Messaging Applications other than those authorized by CoGHSTA shall be prohibited.

- 5.3 The use of other means to access email facilities is not prohibited. Facilities like I-Pads and mobile smart phones shall be correctly configured to access the Departmental email facilities. Users shall familiarize themselves with the operation of these devices and the security risks involved. Users must be aware that there will be cost involved from the mobile operator regarding data. Neither the Department nor GiTO will be held liable for any costs relating to the sending or receiving of emails using such devices, or any related costs.

6. PREVENTION OF MALICIOUS SOFTWARE

Emails are subjected to huge amounts of malicious software including viruses, computer worms and spyware. As a result, CoGHSTA shall implement technical measures to ensure that computer malicious software is prevented from entering the network and infecting computer systems. The following will govern incoming and outgoing malicious or potentially harmful attachments:

- 6.1. By default all virus infected mails shall be blocked
- 6.2. All attachments that cannot be scanned for viruses shall be blocked
- 6.3. Typical virus hoaxes shall be blocked
- 6.4. All executable files or documents with embedded executable shall be blocked.
(Please refer to Annexure A for a list of prohibited executable files)
- 6.5. All unknown/unrecognizable attachments shall be blocked

7. COMMUNICATION OF OFFICIAL INFORMATION

- 7.1. Email users are expected to use CoGHSTA email facilities in accordance to departmental policies and procedures including but not limited to the communication policy.
- 7.2. Only authorized personnel shall distribute official information to both internal and external entities. This also means that in accordance with the communication policy, not everyone is authorized to send official emails to the All Staff Members and other distribution lists.
- 7.3. Every branch shall select one member as the only authorized delegate to send official emails to distribution lists. These distribution lists shall not be used for personal purposes, personal advertisements or distribution of junk mails.
- 7.4. Moderators shall be nominated for the sending of email to External distribution lists.

8. FRIVOLOUS

- 8.1. Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all Email users have a responsibility to conserve these resources. As such, the user shall not deliberately perform acts that waste computer/network resources or unfairly monopolize resources to the exclusion of others.
- 8.2. These acts includes, but are not limited to, sending mass mailings or chain letters, or distributing of large files, music, video files and creating unnecessary loads on network traffic associated with non-business-related uses of Email facilities.

8.3. To minimize network load, an Email size restriction is set at 10 Megabytes for internal sending of emails and 5 Megabytes for sending emails outside CoGHSTA or as determined by Department of Public Service and Administration.

9. LIMITATIONS OF PRIVACY

9.1. Email facilities are provided to employees to improve information sharing and assist them in the performance of their jobs. Employees should acknowledge and understand the openness and privacy issues relating to the Email and as such have no expectation of privacy in anything they store or distribute using the CoGHSTA Email facilities.

9.2. While CoGHSTA shall put measures in place to ensure adequate Email security, users are cautioned that Email messages may be accessed and/or tampered-with by unauthorized third parties before reaching intended recipients. Additionally CoGHSTA Email content-filtering systems shall automatically scan all incoming and outgoing emails to ensure policy compliance. If a policy breach is detected, the email message shall be blocked and the sender or receiver of the message shall receive a notification clearly indicating the conditions of the blockage to afford him or her opportunity to request the release of the message should the message be business related.

9.3. This request shall be verbal through logging of a call with the IT Helpdesk or via email reply to the email message indicating policy breach. Authorized GITO personnel upon this request access the blocked email as to carry out further investigation. Thus by sending a message release request, the Email user consents GITO to access only the email message in question. Furthermore GITO personnel shall not inspect the specific content of blocked email messages unless if the concerned contains a virus. For purposes of ensuring reliable Email facilities and diagnosing network problems GITO may

access the email history logs. These logs do not need to reveal email contents.

10. DISCRIMINATORY, HARASSING, AND OFFENSIVE LANGUAGE

Users are to refrain from using obscene, defamatory, derogatory, discriminatory or any offensive language while using CoGHSTA email facilities as such actions could have serious criminal, civil and moral consequences.

11. MONITORING AND REPORTING

11.1. It must be understood that CoGHSTA provides email facilities to all staff members primarily for work-related purposes.

11.2. While personal use of email facilities is not discouraged, it can often lead to decreased employee productivity, misuse and violations of laws and regulations if not controlled. Therefore, GITO reserves the right to monitor email traffic from time to time for statistics, operation efficiency and reporting.

11.3. This will ensure that GITO can predict email trends so as to proactively plan for future growth, continuously improve Email security and ensure compliance.

12. ACCESS TO ANOTHER EMPLOYEE EMAIL

12.1. By default no employee except authorized GITO personnel is allowed to access another employee's emails or mailbox. If an email user requires another employee, (the delegate) to access his or her emails, then he or she must complete the Email Authorization Form (Annexure B) to GITO. GITO personnel will not actively monitor employee mailboxes but it may be necessary for authorized GITO personnel to view the contents of employee's electronic communications and Email activity or history in the course of problem resolution, system maintenance and operational duties. 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 authorization procedures.

- 12.2. By completing the Email Authorization Form (Annexure B), the individual user grants the requestor permission to access and or receive copies of all emails. For this purpose GITO shall not be held liable for any privacy violation or unforeseen activity that may arise out of this request. The user acknowledge that he / she is aware of the confidential and integrity concerns and shall take full responsibility in ensuring that the delegate's use shall be in accordance with this Email Acceptable Use Policy.

13. AUTOMATIC FORWARDING OF EMAILS

- 13.1. Users are cautioned not to forward or create rules to automatically forward any official Emails to external email addresses such as web mail, mail accounts hosted by internet service providers, etc as this might result in disclosure of sensitive official information.
- 13.1. If an Email user leaves his or her employ at CoGHSTA or his or her services are terminated, GITO will at the request of the departing employee, forward all new incoming Emails to the Email address provided by the user. This is to ensure that the user will continue receiving important emails until he or she can notify contacts about the new email address. These emails will be automatically forwarded for a period of one month. To prevent intentional and unintentional information disclosures, all official emails will be exempt from this automatic forwarding.

14. MAILBOX LIMITATION

- 14.2. All Email users have uniform quota limits set on their individual mailboxes of 120 (MB) Megabytes. Users close to their limit will be notified and the mailbox will be closed once this limit is exceeded.
- 14.3. GITO shall ensure that every user is aware of the different mailbox management methods including the use of personal folders and email archiving. In the absence or non-implementation of these mailbox management methods, email users shall ensure that they notify GITO for advice on mailbox management.

15. EMAIL RETENTION AND ARCHIVING

E-mail users are notified that in accordance with the National Archives of SA Act 43 of 1996, all electronic messages will be archived for a period of 5 years.

16. CHAIN LETTERS, HOAX, AND SPAM EMAILS

Users shall not use CoGHSTA Email facilities to distribute chain letters, hoax and spam emails to other users.

17. PROHIBITED USE

Prohibited uses of Email facilities include but are not limited to;

- 17.1. Distributing chain letters, junk mail and/or hoax email messages
- 17.2. Sending, receiving and storing of pornography and profanity
- 17.3. Sending, receiving and storing of audio and video files
- 17.4. Sending of emails to distribution lists to which you have not been granted the authorization
- 17.5. Sending of classified departmental information
- 17.6. Sending of emails of racial, hate, discrimination or sexist nature

- 17.7. Sending of unsolicited personal and commercial advertisements or promotions to other staff members or external email recipients
- 17.8. Sending of other people's confidential and personal information
- 17.9. Sending of data that violates copyright laws
- 17.10. Capturing and viewing of emails except when required for authorized GITO personnel to diagnose and correct delivery problems as well as investigate policy breaches
- 17.11. Use of electronic mail to harass or intimidate others or to interfere with or deny other legitimate users the ability to effectively carry out their official duties
- 17.12. Use of electronic mail in any manner prohibited by national and international laws and regulations
- 17.13. "Email Spoofing" i.e. constructing emails so it appears to be from someone else
- 17.14. "Snooping" i.e. obtaining access to other people's emails for the purpose of satisfying curiosity
- 17.15. Attempting unauthorized access to electronic emails or attempting to breach security systems of any email system or "eavesdropping" i.e. attempting to intercept any electronic mail transactions without proper authorization

18. **DISCLAIMER**

All email messages sent from CoGHSTA email facilities will automatically be stamped with the following disclaimer:

"The contents of this e-mail and any attachments are confidential. It is intended for the named recipient(s) only. If you have received this email in error please notify the sender immediately and do not disclose the contents to any one or make copies. Please note that the recipient must scan this e-mail and any attached files for viruses and the like. While we do everything possible to protect information from viruses, the Limpopo Department of Co-operative Governance, Human Settlements and Traditional Affairs accepts no liability of whatever nature for any loss, liability, damage or expense

resulting directly or indirectly from the access and/or downloading of any files which are attached to this e-mail message. Opinions, conclusions and other information in this message that do not relate to the official business of the Limpopo Provincial Department of Co-operative Governance, Human Settlements and Traditional Affairs shall be understood as neither given nor endorsed by the said Department of Co-operative Governance, Human Settlements and Traditional Affairs.

19. AUTHORIZATION PROCEDURE

- 19.1. A user will be granted access to email facilities upon completing an application for network access or signing an undertaking in the format Annexure C, 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 filed 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 immediate revocation of access to all email facilities.

- 19.2. In addition to signing the undertaking, a network logon message will be presented through which an employee will further agree to abide by the provisions and aspects of this Electronic Mail Acceptable Use Policy and any other relevant policy. This logon message will clearly indicate where the user can locate the policies for review. At this point the user will also be presented with an option to either agree to the policies by clicking the OK button or disagree by clicking the cancel button. Email resources will not be available to any user who does not agree to abide by and be legally bound by this Policy.

20. EMAIL USER RESPONSIBILITY

All Email users are responsible, accountable and liable for all their activities while using the departmental email facilities. As such the email user has the following responsibilities:

- 20.1 Ensure that their usernames and passwords are kept secure and not shared;
- 20.2 Fully comply with all aspects of this policy;
- 20.3 Immediately alert GITO (Information Security/Incident Response) about any misuse and non-compliance;
- 20.4 Duty not to waste computer and network resources;
- 20.5 Continuously protect the integrity and public image of CoGHSTA.

21. GITO RESPONSIBILITY

GITO is responsible for the following:

- 21.1 Implement technical measures to ensure adequate Confidentiality, Availability and Integrity of CoGHSTA email facilities;
- 21.2 Monitor and enforce policy compliance;
- 21.3 Follow appropriate channels to resolve policy breaches and incidents;
- 21.4 Educate Emails users whenever possible about Email security best practices and this Electronic Mail Acceptable Use Policy.

22. CONSEQUENCES OF NON- COMPLIANCE





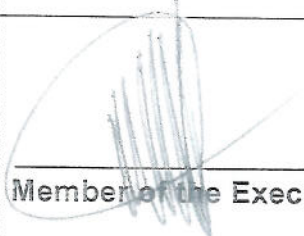
Non-compliance of this policy may lead to disciplinary actions, legal liability as well as Email privileges for the user in violation revoked.

23. INCEPTION DATE

This policy comes into effect from the date of approval.

24. POLICY REVIEW

This policy shall be reviewed annually.

Policy Title	Electronic Mail Acceptable Use Policy	
Compiled by :	 _____ Senior Manager (ICT Infrastructure and Systems)	<u>9/07/2013</u> Date
Acknowledge by :	 _____ General Manager (GITO)	<u>10/07/2013</u> Date
Acknowledge by :	 _____ Senior General Manager (Corporate Services)	<u>11/07/2013</u> Date
Adopted by:	 _____ Head of Department	<u>11/07/2013</u> Date
Approved by:	 _____ Member of the Executive Council	<u>02/08/2013</u> Date