

**POLICY: GPG EMAIL/ MESSAGING POLICY**

**APPROVED**

**NUMBER:** EP02/2005

**DISTRIBUTION:** ALL POLICY & PROCEDURE HOLDERS

**EFFECTIVE DATE:** August 2005

**REVISED DATE:** December 2005

**ALL RIGHTS RESERVED**

©Technical Support Services 2003

No part of this document may be photocopied, reproduced, translated or reduced to any electronic or machine readable form without the prior permission of the Gauteng Shared Services Centre.

**UNCONTROLLED DOCUMENT**

This document is uncontrolled unless viewed from a controlled area. Where this document is used in a printed format or viewed from an uncontrolled area it is the responsibility of the person using this document to ensure that it is the correct issue. If in doubt contact the document owner or the Quality Department.

---

Issue:.....**EP02/2005**

Owner: .....Information Security & Risk Manager

Amended By: .....Information Security & Risk  
Management

Status: .....Approved

---

**COMMERCIAL IN CONFIDENCE**

---

## DESCRIPTION

### Policy Purpose

The purpose of the Gauteng Provincial Government - now GPG - email and messaging policy is to ensure the appropriate use of the GPG email system and to make GPG employees and business partners aware of what GPG deems as acceptable and unacceptable use of its electronic messaging system.

### SCOPE

The GPG email and messaging policy applies to all GPG employees, contractors, temporaries, business partners e.g. SITA, operating on behalf of GPG.

### TABLE OF CONTENTS

1	DEFINITIONS .....	2
2	ACRONYMS.....	4
3	RESPONSIBILITY .....	4
4	INPUTS AND OUTPUTS POLICY AMENDMENTS .....	4
5	PUBLISHING THE EMAIL POLICY .....	4
6	MONITORING.....	5
7	POLICY VIOLATIONS.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
8	GPG USERS POLICY ACCEPTANCE.....	5
9	GPG EMAIL DISCLAIMER .....	5
	10.1 All outgoing e-mail shall be subject to the following disclaimer: .....	5
10	EMAIL POLICY STATEMENTS .....	5
11	POLICY ACCEPTANCE SIGN-OFF .....	7
12	APPENDICES .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>

## 1 DEFINITIONS

Authorisation	A person who has the power or right to make decisions or enforce obedience
Confidentiality Breaches	Unauthorised disclosure of confidential, proprietary or trade secret information such as when the employee secretly trade a product design specification, sales data and information of which departments are competing for, the sender and recipient may be charged for trade secret theft
Damage Reputations	Distortion, interruption or unwanted disclosure of messages such as badly written email or email containing unprofessional remarks will cause the recipient to have a bad impression of the employer the sender is representing.

Mailbox	Users that require email will be provided with a messaging mailbox that resides on the messaging server. The mailbox is the holding place for email that is received and transmitted
Email Attachment	A file attached to the email message
Email auditing	When GPG users email is scanned after the actual transmission
Email infrastructure	Is a computing facilities, services and network systems such as computers, computer data processing or storage functions service, servers, input/output and connecting devices related to computer records, programs, software and documentation to send email message
Distribution List	Distribution lists are created on the messaging infrastructure to group users together in a group that will receive common email information. Distribution groups are created to assist users in sending email messages to a large number of users.
Macro's	Macro's are used in documents and spreadsheet to perform predefined work statements and calculations. Viruses can also use Macro functionality to introduce malicious actions.
Out of Office Replies	Microsoft Outlook can be configured to automatically inform email users that the email recipient is not in the office.
Email SPAM	The word SPAM relates to information that is of no importance to email recipients. SPAM is an email intruder that will use the GPG email infrastructure to send non relevant business information to large number of users. SPAM is illegal and users must be aware of SPAM information such as non business related advertisements and non business related email messages.
RFC	A Request for Change is used by the GSSC to control changes to the operational IT environment. The RFC will be issued by the requestor and approved by the Change Control Manager
Email interception	Is where the email is intercepted and scanned during the transmission

Legal liability	These are legal costs and penalties incurred or paid by GPG when distribution of viruses or other harmful programs are sent through GPG email system as these harmful programs could threaten work environment for other employees
Letter –bomb	Is to resend the same email repeatedly to one or more recipient's which interferes with the recipient's use of mail
Lost of productivity	Is when inappropriate usage of email system is of a great concern where employees waste their productive time through reading or sending emails, which does not contain business related information.

## **2 ACRONYMS**

CIO	Chief Information Officer
GSSC	Gauteng Shared Services Centre
GPG	Gauteng Provincial Government
HOD	Head of Department
IT	Information Technology

## **3 RESPONSIBILITY**

The Head of Department will be responsible for the Department's overall email and messaging policy. GPG users will sign-off acceptance and adhere to the proposed GPG email and messaging policies.

The GPG messaging infrastructure and policies will be managed and controlled by the GSSC.

## **4 INPUTS AND OUTPUTS POLICY AMENDMENTS**

Any policy changes will be discussed between the GSSC and GPG. The policy outputs and changes will be added to the policy document for review. The policy outputs will be signed-off between the GSSC and GPG.

## **5 PUBLISHING THE EMAIL POLICY**

The policy shall be made available and accessible to all employees through intranet, website and manuals/hard copies

## 6 MONITORING

All messages distributed via GPG system are the property of the GPG. All GPG employees shall have no expectation of privacy in anything they store, send or receive on GPG's email system. GPG may monitor messages without prior notice or approval.

## 7 GPG USERS POLICY ACCEPTANCE

GPG users will sign-off acceptance of email policy in their employment contract so as to adhere to the proposed GPG email and messaging policies

## 8 GPG EMAIL DISCLAIMER

### 9.1 All outgoing e-mail shall be subject to the following disclaimer:

This message may contain confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. E-mail transmission cannot be guaranteed to be secured or error-free as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. The sender therefore does not accept liability for any errors or omissions in the content of this message, which arise as a result of e-mail transmission. The GPG does not take responsibility for GPG users personal views.

## 9 EMAIL POLICY STATEMENTS

- 1 Private use of the GPG email and messaging infrastructure is permitted but this is subject to strict control. Abuse of this privilege may be regarded as misconduct.
- 2 The GSSC will audit the GPG messaging infrastructure. The GPG messaging infrastructure audit will be triggered by the following events:
  - 2.1 GSSC suspects that the GPG messaging infrastructure is abused or over utilised by private email.
  - 2.2 Messaging irregularities are suspected.
  - 2.3 Messaging virus attacks are suspected.
  - 2.4 GPG email content-filtering rules are violated.
- 3 All emails created, sent, stored, forwarded, or printed are the property of GPG
- 4 Through using Email GPG users will have been deemed to have read, understood and agreed to the policies relating to GPG email systems
- 5 Employees shall not, as a matter of course, forward confidential, trade secret or proprietary information to third parties. Confidential information is deemed confidential or government proprietary information when the following headings or subtext are present:
  - 5.1 Confidential Information
  - 5.2 Proprietary Information
  - 5.3 GSSC or GPG Internal Information
  - 5.4 Each department must add the confidential, trade secrets and proprietary information to the documents

- 6 Employees shall only forward classified or confidential messages to other staff who are permitted / authorised to receive such information
- 7 Employees shall not send all messages as important as this negates the purpose and adds unnecessary overheads to the Email systems.
- 8 Adhere to messaging warnings regarding virus alerts from email systems administrators and help/ service desk.
- 9 Delete any Email enclosed viruses, BEFORE opening, particularly if documents containing executable programs are sent. If you open a message and are prompted to “Enable or Disable macros” you should select “Disable” and scan for viruses. If any viruses are found then notify the local system administrator and Help/ Service Desk (011 355 2222). If none are found you may utilise the attachment. (Review to address viruses in emails- communications)
- 10 If you get an attachment via Email which is unsolicited or of unknown origin, detach it and scan the file using your installed anti virus software. It is advisable to delete any unknown email and do not reply to the sender that the mail was deleted. For any assistance regarding attachment scanning please phone the GSSC Service Desk at (011 355 2222)
- 11 Avoid unnecessarily large distribution lists. GPG users must rather create smaller distribution lists.
  - 11.1 Distribution groups can be created for GPG per director in the departments using the proper RFC procedures
  - 11.2 Log a call with the GSSC Service desk to create the required distribution lists
  - 11.3 Grouping of Distribution lists can be requested by departments and user groups
- 12 Users must check their mailbox regularly for received mail.
- 13 Ensure that the content of your message is not ambiguous and that there is nothing unlawful about the transmission or content of your message.
  - 13.1 It is prohibited to display or transmit;
    - 13.1.1 Offensive, defamatory, discriminatory or harassing material;
    - 13.1.2 Sexually explicit or other offensive images or jokes;
    - 13.1.3 Unlicensed copyright material;
    - 13.1.4 Non- business related video and image files;
    - 13.1.5 Any message which would be deemed unlawful pursuant to the applicable law of any governing jurisdiction;
    - 13.1.6 Confidential, proprietary or trade secret information outside without authorisation;
    - 13.1.7 Private and personal advertisements;
    - 13.1.8 Chain letters.
    - 13.1.9 Do not send or forward Email notices concerning virus or harmful code warnings to other GPG employees.
    - 13.1.10 The GPG email and messaging infrastructure will not be used for Politically motivated e-mails
  - 13.2 When sending or forwarding Email to the Internet, do not include the system UserID’s of any GPG employees;
  - 13.3 Do not use auto-reply functions to respond to your Internet mail. If you use auto-reply functions such as Out of Office message option for your normal GPG internal mail when you are away, be sure to select the option that excludes sending the notices to Internet users;

- 14 Employees shall not use an electronic mail account assigned to another individuals to either send or receive messages. Individuals that require other users to use their messaging infrastructure must complete an RFC with the GSSC Service desk
- 15 Email accounts not used for 90 days will be deactivated. Email accounts not used for 100 days will be deleted. GPG users that will be offsite for a longer period than 100 days must inform the Help/ Service desk at (011 355 2222)
  - 15.1 Users will be contacted by the Help/ Service desk before the Email account is deleted
- 16 Employees should regularly move important information from electronic mail message files to word processing documents, databases, and other files, as Email messages and attachments may be erased periodically, either accidentally or as part of normal archiving and file maintenance functions.
- 17 If employees receive unwanted and unsolicited email (also known as SPAM), they shall refrain from responding directly to the sender. Instead, they should contact the system administrator and the Help/ Service Desk (011 355 2222).
- 18 It is the responsibility of individual employees to manage their own Email once they have downloaded it. It is suggested that unwanted Emails are regularly deleted and important Emails are moved to appropriate folders. Important attachments should be saved in an appropriate folder within the “My Documents” folder and saved to a network server for backup. Contact the Help/ Service Desk (011 355 2222) should further information regarding the management of Email be required.
- 19 When using GPG messaging systems, or when conducting GPG business over the internet, employees shall not deliberately conceal or misrepresent their identity.
- 20 Do not forward emails and attachments that were intended for the receiver only. The email sender will add the following line to the respective email “This email should not be forwarded or disseminated by the email recipient”.
- 21 GPG user that will not read or respond to received email messages within a period of 2 days must enable the Out of Office reply function. Contact the Help/ Service desk for assistance regarding the Out of Office setup.

## **10 ENFORCEMENT**

Any transgression of this policy shall be handled in accordance with the Public Service Disciplinary procedures and or other relevant labour legislation.

## **11 POLICY ACCEPTANCE SIGN-OFF**

The GPG Members of the Executive Committee accepts the GPG Email and Messaging Policy. The HOD will take overall responsibility for the GPG Email and Messaging policy.