

POLICY: GPG INTERNET POLICY

APPROVED

NUMBER: IP02/2005

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:.....**IP02/2005**

Owner:Information Security & Risk Manager

Amended By:Information Security & Risk
Management

Status:Approved

COMMERCIAL IN CONFIDENCE

POLICY DESCRIPTION

The Internet is used by GPG to connect to customers, suppliers and other organisations. It is important to remember the following points:

- The Internet is used by millions of people worldwide.
- Unprotected information sent across the Internet may well be read by any number of unknown people.

PURPOSE

The purpose of the GPG Internet policy is to ensure the appropriate use of GPG Internet access and to make GPG users aware of what GPG deems as acceptable and unacceptable use of the Internet infrastructure.

SCOPE

The GPG internet policy will apply to all GPG (Gauteng Provincial Government) employees using the GPG internet access infrastructure.

TABLE OF CONTENTS

1	DEFINITIONS.....	2
2	RESPONSIBILITY.....	3
3	INPUTS AND OUTPUTS POLICY AMENDMENTS	3
4	POLICIES.....	3
5	APPENDICES	5
6	POLICY ACCEPTANCE SIGN-OFF	5

1 DEFINITIONS

Firewall	Firewall technology is use to protect the GPG internal IT services from malicious activity on the internet
Audio Sessions	Internet technology can also allow users to receive audio feeds such as radio stations over the internet
Media Streaming	Media streaming is a technology that is used to provide media services via internet technology that provides video type services over the internet
Internet Infrastructure	The GSSC Internet servers provide internet access and services to GPG users. The GPG internet infrastructure is supported and monitored by the GSSC

Web Sites	Internet servers that provide brows able pages that provide information, data and services to user on the internet.
Viruses	Viruses are malicious programs created to disrupt computer services.
Internet Chat rooms	Internet chat rooms are created on the internet to provide a central point for users that communicate via text on different issues. Internet chat rooms are a security risk to the GPG internet
Security Testing Tools	Computer programs that provide information on the GPG IT infrastructures. Security tools and security scanning applications are not allowed on the GPG IT infrastructure
ISP	Internet Service Provider (ISP) is used to provide Internet connectivity to users all over the world. ISP's provide the interlinking services to create internet access

2 RESPONSIBILITY

The HOD's will be responsible for the Department's overall Internet policy. GPG users will sign-off acceptance and adhere to the proposed GPG internet policies.

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

3 INPUTS AND OUTPUTS POLICY AMENDMENTS

Any policy changes will be discussed between the GSSC and GPG. The policy outputs will be to create new policy or change current policies. The policy outputs will be signed-off between the GSSC and GPG.

4 INTERNET POLICY STATEMENTS

1. Only GPG employees who have received departmental management approval may access the Internet via the GPG internet facilities. Automatic access to the Internet is not a right, and access can be revoked if it is found that misuse of the facility is occurring.
2. Whenever an employee posts a message to an Internet discussion group, an electronic bulletin board, or another public information system, this message shall be accompanied by words clearly indicating that the comments do not necessarily represent the position or views of GPG.
3. Unless expressly authorised by the GPG, when using GPG internet systems, all employees are forbidden from participating in Internet chat rooms and non business related media streaming and audio sessions.

4. Although the Internet is an informal communication environment, the laws for copyrights, patents, trademarks etc. apply. GPG users using the GPG internet system shall:
 - 4.1 Repost material only after obtaining permission from the source;
 - 4.2 Quote material from other sources only if these other sources are identified;
 - 4.3 Reveal internal confidential, proprietary and trade secret GPG information on the Internet only if the information has been officially approved for public release by GPG.
5. Whenever an Internet user provides an affiliation with the GPG, whether implicitly or explicitly, care shall be taken not to make any political advocacy statements or product/service endorsements unless the permission from GPG has first been obtained.
6. GPG software, documentation and all other types of internal information shall not be sold or otherwise transferred to any party for any purposes other than the business purposes expressly authorised by GPG:
 - 6.1 Authorization must be obtained to transfer or post information on internet sites
7. GPG internet security access systems may routinely prevent users from connecting to certain non-business web sites directly. Users will be subjected to a warning message that will highlight the risk of visiting an unauthorised internet site. The ability to connect to a specific web site does not in itself imply that employees are permitted to visit the specific internet sites.
8. No employee or independent contractor to GPG may use the GPG Internet, Intranet or E-mail services to access newsgroups, Internet web sites and FTP sites for unauthorised and/or unacceptable purposes such as, but not limited to:
 - 8.1 The viewing and or downloading of pornographic or obscene material of any nature;
 - 8.2 The dissemination of material that advocates hatred and/or conflict or which causes discomfort or embarrassment to the organisation or their fellow colleagues by way of discrimination based on race, ethnicity, gender, religion, sexual orientation, age and/or material that propagates sexual harassment;
 - 8.3 The dissemination of any material supporting any petition, or advertising any services not specifically authorised in writing by GPG;
 - 8.4 The transmission of any message of an abusive or defamatory nature of anyone either internally or externally to GPG;
 - 8.5 The use of Internet, Intranet or E-mail facilities for any purpose whatsoever not connected to or forming an integral part of GPG customer operations or business;
 - 8.6 Web sites that advocate any illegal activity.
9. All information taken off the Internet should be considered suspect until confirmed by the Help/ Service Desk (011) 355 2222. Internet data and

- software downloads include any internet software or data moved from the internet to GPG users local workstations using GPG internet services.
10. Users shall not up-load software which has been licensed from a third party or software which has been developed by the GPG, to any computer via the Internet unless authorisation from GPG has been obtained.
 11. All users wishing to establish a connection with the GPG computers via the Internet shall authenticate themselves at a VPN and firewall before gaining access to GPG internal network. Contact the Help/ Service Desk (011) 355 2222 for further information.
 12. No systems shall be directly connected to the Internet; GPG users are prohibited from connecting any workstations or servers to the Internet.
 13. Internet access using computers in GPG offices is permissible only via the GPG firewall.
 14. Other ways to access the Internet, such as direct dial-up connections with an Internet Service Provider (ISP), are prohibited if GPG computers are connected to internal GPG networks. Non-GPG computers are prohibited from connecting to the GPG networks without specific permission from GPG.
 15. Do not run unauthorized security-testing tools or programs against any GPG Internet systems or servers.
 16. Dial up connections e.g. whilst travelling or from home based systems and laptop computers which are also utilised for GPG business must only be made via authorised dial up procedures which employ the use of GPG VPN and firewalls. Contact the Help/ Service Desk (011 355 2222) for further information.

5 ENFORCEMENT

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

6 APPENDICES

No Appendices

7 POLICY ACCEPTANCE SIGN-OFF

The GSSC Chief Information Officer (CIO) and the Head of Department (HOD) accepts the GPG Internet Policy. The HOD will take overall responsibility for the GPG Internet policy applied to the following Department: