E-Government Initiative

E-mail Usage Policy

Ministry of Information Technology and Telecommunications

E-Government Initiative

* * *

E-mail Usage Policy

* * *

Prepared by E-mail Usage Policy Committee

Date : March 2003

Table of Contents

1. Introduction

This document has been prepared at the request of the e-Government Task Force chaired by the Minister of Information Technology and Telecommunications. A committee under the chairmanship of the National Computer Board was set up with representatives from the Ministry of Information Technology and Telecommunications, the Ministry of Civil Service Affairs and Administrative Reforms, the Central Informatics Bureau and the Central Information Systems Division to prepare an e-mail usage policy document for the civil service.

The committee considered the existing e-mail usage policy document that was circulated to all Ministries/Departments with the introduction of the Government E-mail Services (GES) in May 2001.

This policy document is more comprehensive on e-mail usage policy in the civil service. It defines new policy and procedures where the existing policy did not address issues particular to the use of e-mail.

2. Purpose

The purpose of this e-mail usage policy is to ensure that :

(a) The Civil Service is informed about the applicability of policies to the use of e-mail;

(b) Electronic mail services are used in compliance with those policies;

(c) Users of electronic mail services are informed about how concepts of privacy and security apply to electronic mail; and

(d) Disruptions to GES are minimized.

3. Definitions

The terms "electronic mail" and "e-mail" are used interchangeably throughout this e-mail usage policy document. GES means the current mail.gov.mu services and any other e-mail service that may be used by government.

For a better understanding of the terms used in the document a glossary of terms is in the Appendix.

4. Scope

This e-mail usage policy applies to:

- All electronic mail systems and services provided to or owned by the government; and
- All users of the GES; and
- All e-mail records in the possession of Public Officers or other e-mail users of electronic mail services provided by the government.

This e-mail usage policy applies only to electronic mail in its electronic form. The policy does not apply to printed copies of electronic mail.

5. Provisions

A. Allowable Use

Purpose

To encourage the use of GES to share information, to improve communication, and to exchange ideas. GES is to be provided in support of public officers' daily duties and the administrative functions.

Users

GES are currently available to public officers of the rank of Higher Executive Officers and above.

Government Property

The government encourages the use of e-mail as a productivity tool. Unless third parties have clearly noted copyrights or some other rights on the messages handled by the GES, all messages generated on or handled by the GES are considered to be the property of the government.

Authorised Usage

The GES is generally restricted for official use. Incidental personal use is permissible as long as: (a) it does not consume more than a trivial amount of system resources, (b) does not interfere with public officer productivity, and (c) does not preempt any business activity.

Contents Of Messages

Public officers must not use profanity, obscenities, or derogatory remarks in electronic mail messages discussing employees, customers, competitors, or others. Such remarks may create legal problems. It is possible that such remarks would later be taken out of context and used against the Government. International communications are also problematic when humor is attempted but misunderstood; this is an increasingly serious problem with Internet electronic mail (avoid smiley faces, etc.). To prevent these and other problems, stick to business matters in the GES.

Service Restrictions

GES user should not use the facility for any unlawful purposes and agrees to abide by all applicable national laws and regulations.

Default privileges

GES must be established and maintained such that only the privileges necessary to perform a job are granted to a public officer. This approach is widely known as the concept of "least privilege". For example, when a public officer's relationship with the Civil Service comes to an end, all the public officer's privileges on the GES will also come to an immediate end.

Representation

GES users shall not make representations on behalf of the Government unless authorized.

False Identity

GES users shall not employ a false identity.

Interference

The use of GES shall not cause strain/interference with computing facilities.

Restriction on Access Without Consent

The government shall only permit the inspection, monitoring, or disclosure of electronic mail without the consent of the holder of such e-mail when required by and consistent with law.

Respecting Privacy Rights

Except as otherwise specifically approved by management, public officers may not intercept or disclose, or assist in intercepting or disclosing, e-mails. The government is committed to respecting the rights of its public officers, including their reasonable expectation of privacy. The government also is responsible for operating the GES. To accomplish these objectives, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, e-mails. To meet these objectives the government may employ content monitoring systems (which scan for certain key words) as well as other electronic system management tools.

No Guaranteed Message Privacy

E-mail can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, e-mail can be accessed by people other than the intended recipients in accordance with this policy. Because messages can be stored in backups, e-mail may actually be retrievable when a traditional paper letter would long since have been discarded or destroyed. Public officers should accordingly be careful about the topics covered in GES communications.

Statistical Data

Consistent with generally accepted business practice, the government collects statistical data about the GES. Using such information, technical support personnel monitor the use of GES to ensure the ongoing availability and reliability of the system. The government employs computer systems which analyze these types of statistical information to detect unauthorized usage, toll fraud, and other problems.

Misuse

This policy prohibits the theft or other abuse of computing resources and include (but are not limited to) unauthorized entry, use, transfer, and tampering with the accounts and files of others, and interference with the work of others and with other computing facilities.

B. Security and Confidentiality

The aspect of security of electronic mail should be in line with the ISO/IEC 17799 IT Security Standards which have been adopted by government and should include:

User Separation

Where GES provides the ability to separate the activities of different users, these facilities must be implemented. For example, electronic mail systems must employ personal user-ID's and associated passwords to isolate the communications of different users. If user separation has been established by the government, public officers must not employ the user-ID or identifier of any other user.

User Accountability

Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else. To give a password to someone else exposes the authorised user to responsibility for actions the other party takes with this password.

User Identity

Misrepresenting, obscuring, suppressing or replacing another user's identity on the GES is forbidden. The user name, electronic mail address, organisational affiliation, and related information included with electronic messages or postings must reflect the actual originator of the messages or postings. At a minimum, all public officers must provide their name, organisation and phone number in all e-mails. Electronic mail "signatures" indicating job title, company affiliation, address, and other particulars are strongly recommended for all electronic mail messages.

Use only GES System

Public officers must not use their personal electronic mail accounts with an Internet Service Provider (ISP) or any other third party for any government messages. To do so will circumvent logging and back-up controls that the

government has established. Likewise, public officers must not use the electronic mail features found in web browsers for any government business communications; they must instead use authorised GES software.

Use of Encryption Programs

Public officers are reminded that GES does not provide encryption features by default. If sensitive/confidential information must be sent by e-mail, encryption or similar technologies to protect the information must be employed.

Respecting Intellectual Property Rights

Although the Internet is an informal communications environment, the laws for copyrights and the like still apply. As there is no quality control process on the Internet, and a considerable amount of Internet information may be outdated, inaccurate, or misleading, such information should be taken with care.

Incidental Disclosure

It may be necessary for technical support personnel to review the content of a public officer's e-mail during the course of problem resolution (advanced approval by the head of Ministries/Departments is required for all such monitoring). Technical support personnel may not, however, review the content of a public officer's e-mail out of personal curiosity.

Handling Attachments

Attachments to electronic mail messages, may contain a virus or may in some other way damage a public officer's computer. Suspicious attachments should be viewed with care.

Message Forwarding

Government information must not be forwarded to any unauthorised party without the prior approval of the department head.

Handling Alerts About Security

Users must promptly report all information security alerts, warnings, spamming, vulnerabilities, and the like to the technical support personnel.

User Back-Up

Most electronic mail messages do not contain important reference information and accordingly can be erased after viewing. However important messages should be secured through back-up.

Purging Electronic Messages

Regular purging of unnecessary e-mails should be done to free storage space. After a certain period, messages stored on mail servers will automatically be deleted.

Archival Storage

All official GES messages, including those containing a formal management approval, authorization, delegation, or handing over of responsibility, or similar transactions, must be made on hard copy.

6. Policy Violations

Violations of policies governing the use of GES may result in restriction of access to Government information technology resources and in addition may lead to disciplinary action.

7. Responsibility for Policy

The Ministry of Information Technology and Telecommunications is responsible for development and maintenance of this Policy. The responsibility for ensuring compliance with this policy lies with the heads of the Ministries/ Departments.

8. Appendix : Glossary of Terms

Cryptography

The art of protecting information by transforming it (encrypting it) into an unreadable format called cyphertext. Only those who possess a secret key can decipher (or decrypt) the message into plaintext. Encrypted messages can sometimes be broken by cryptanalysis, also called codebreaking, although modern cryptography techniques are virtually unbreakable.

Download

To copy data from a main source to a peripheral device. The term is often used to describe the process of copying a file from an online to one's own computer. Downloading can also refer to copying a file from a network file server to a computer on the network

E-mail

Correspondence sent from one computer address to another computer address.

Internet

A network is a collection of computers that are connected together so they can exchange information, and the Internet is a network of networks. It allows individuals on one network to share information with users on another network that may be thousands of miles away. The shared information can take many forms. For example, the Internet can be used to send e-mail messages, to download files, to view video clips, listen to music, chat with people electronically and even for shopping.

Internet Service Provider

A company which provides its customers with a service whereby they can access the Internet. The user normally connects to the access provider's computer via a modem using a dial up connection.

Online

Service accessible via a computer, rather than on paper or other medium. Also describes a user who is actively using a computer system, especially the Internet. Users are considered online when they are connected to a computer service.

Server

A computer or series of computers that shares its resources with other computers. (i.e. An ISP, Internet Service Provider is a "Server" for other computers to the Internet.)

Spam

Unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups;

World Wide Web (WWW)

A collection of information located on many Internet servers that can be accessed with a browser or by navigating via hypertext links. On the WWW everything (documents, news and indices) is represented to the user as a hypertext object in HTML format. Hypertext links refer to other documents by their URLs.