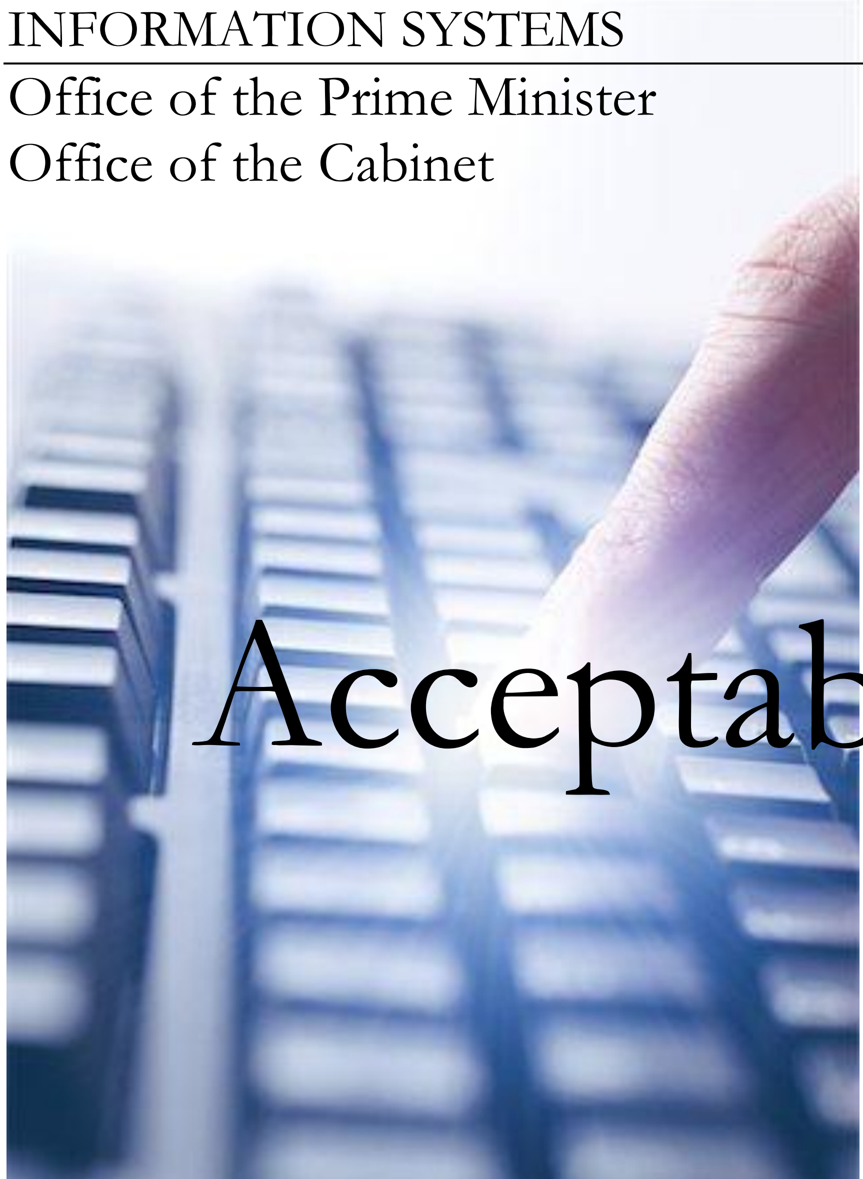
Version

2.3

INFORMATION SYSTEMS

Office of the Prime Minister
Office of the Cabinet



Acceptable Use Policy

INFORMATION SYSTEMS

Acceptable Use Policy

Version 2.3

1 Devon Road • Kingston 6
Extensions 2106 • 3443 • 2262 • 2213 • 3332 • 3121
E-mail techsupport@gov.lan • Fax 876.978.2158

Table of Contents

1.0 Overview

The intentions for publishing an Acceptable Use Policy (AUP) are not to impose restrictions that are contrary to the Office of the Prime Minister (OPM) and the Cabinet Office (CO) established culture. Rather the acceptable use policy is a commitment aimed at protecting OPM and CO employees, agencies and departments from illegal or damaging actions by individuals either knowingly or unknowingly.

Internet/Intranet-related systems, including but not limited to computer equipment, printers, software, operating systems, storage media, network accounts; domain user accounts, the provision of electronic mail (e-mail), world-wide-web (www) browsing, telephones, are the property of OPM and CO. These systems are to be used for business purposes in serving the interests of both organizations, and the interests of their clients and customers in the course of normal operations.

Please review the Government of Jamaica Staff Order relative to policies and for further details in the use of government resource and equipment. Effective security is a team effort involving the participation and support of every OPM and CO employee and affiliate who uses information and/or information systems owned by these organizations. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and network services provided at the Office of the Prime Minister and the Cabinet Office. These rules are in place to protect the employee and the OPM and CO. Inappropriate use exposes OPM and CO to risks including virus attacks, denial of service attacks, compromise of information systems, and services, legal and legislative issues including copyrights and intellectual property rights infringements.

3.0 Scope

This policy applies to all employees, contractors, consultants, temporaries, and other workers at OPM and CO, including all personnel affiliated with third parties. This policy applies to all equipment, services that are owned or leased and operated by OPM and CO or any third party duly contracted by the same and authorized so to do.

4.0 Policy

4.1 General Use and Ownership

4.1.1 **Intellectual Property**

While the Management and IT Staff of the OPM and CO desire to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of the OPM and CO. Because of systems abuse whether knowingly or unknowingly and the need to protect the OPM and CO networks, management cannot guarantee the confidentiality of personal information stored on any network device belonging to the OPM and CO. This is so because of the requirement to monitor and audit networks and systems on a periodic basis.

4.1.2 **Guideline Hierarchy**

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for enforcing guidelines concerning personal use of Internet/Intranet systems. In the absence of such policies, employees should be guided by the organizations' policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager or the MIS Unit.

4.1.3 **Storage / Retrieval of Confidential Data**

The OPM and CO recommends that for any information that users consider sensitive or vulnerable, special guidance should be sought on how to store and/or transmit the same. For guidelines on information classification, contact the Information Resources Unit (Registry).

4.1.4 **Auditing**

For security and network maintenance purposes, authorized individuals within the OPM and CO may and/or will need to monitor equipment, storage devices, systems, networks & internet traffic at any time, as per security requirements and audit policy.

The OPM and CO reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy (AUP). This may include macroscopic monitoring of general use or microscopic monitoring of end user workstations. These audits can be done at any time for any reason and without prior notification to end users. The audit process is usually seamless and will not intervene with a user's capacity to continue working.

4.2 Security and Proprietary Information

4.2.1 **Classify documents accordingly.**

The user interface for information contained on Internet/Intranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in the Access to Information policies.

Examples of confidential information include but are not limited to: minutes of meetings, confidential information, internal memoranda, corporate strategies, operational plans, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.

4.2.2 **Do not share user accounts.**

Keep passwords, access codes and other access devices secure; Authorized users are responsible for the security of their passwords, access codes, other access devices and accounts. System level passwords should be changed quarterly; user level passwords should be changed every thirty (30) days.

4.2.3 **Secure your workstation.**

All PCs, laptops and workstations shall be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes, or by logging-off (control-alt-delete for Windows users) or by locking the workstation (Windows + L) automatically when the host is unattended. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Tips".

4.2.4 Use disclaimers.

Postings by employees from an OPM and CO email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the OPM and CO, unless posting is in the course of business duties.

4.2.5 Anti-Virus Tools

All hosts (computers, handheld devices etc.) used by employees that are connected to the OPM and CO network, whether owned by the employee or by the OPM and CO, shall be continually executing approved virus-scanning software with a current virus database, unless overridden by departmental or group policy.

4.2.6 The Anti-Spam Service

While we have implemented a system to automate the filtration of unsolicited mail, the system is not perfect. Therefore, should such messages pass through our security system, employees must use extreme caution when opening e-mail attachments received from unknown senders, as they may contain malicious code.

Sometimes legitimate mail will be inadvertently blocked by the anti-spamming tool. Users may request the release of these messages by simply forwarding the blocked message notice to the Technical Support team at techsupport@gov.lan (or select Technical Support from your global address list). The message will be released at our discretion.

4.3 Unacceptable Use

Sections 4.4 and 4.5 in this document detail practices which are generally unacceptable. The details in these sections are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

Employees may be exempted from these restrictions with due authorization and reasonable notice during the course of executing their legitimate job responsibilities. For example, systems administration staff may have a need to disable the network access of a host (computer, handheld device etc…) if that host is disrupting normal production services.

4.4 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

4.4.1 Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the OPM and CO. Specifically:

4.4.2 The installation and / or use of any copyrighted software or media that has not been explicitly licensed by the organisation is **strictly prohibited**. Any software not purchased by the Office of the Cabinet / Office of the Prime Minister may not be installed on any machine belonging to either organization. Any such attempt is **illegal** and punishable by law.

4.4.3 The installation of any software licensed to an individual working within either organization for personal use, (whether purchased separately or acquired with a personal laptop or home PC). These are **not** to be installed on any machine belonging to either organization, even if for official use. Installing that software on any computer other than that which is privately owned by the individual is **illegal**. Software is protected by international copyright laws enforced in Jamaica. Most software licenses only permit the installation of that software on one computer, primarily that which is owned by the license holder.

4.4.4 Any breach of this policy is legally punishable by a fine and jail time should a network software audit by the relevant authorities reveal such. The Offices of the Cabinet and the Prime Minister will legally acquire any software that is needed.

4.4.5 Installation of free or open licensed software. Much of the free software available on the internet poses serious security risks to our networking infrastructure – that’s part of the reason why they’re free. As such, any request for the installation of free or open license software (such as instant messengers and media players) will be subject to the sole discretion of the

MIS team. Any free software not approved by the MIS team is strictly prohibited.

4.4.6 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources for which the OPM and CO or the end user does not have an active license is strictly prohibited. This includes audio, video, literature and other multimedia content representative of copyrighted work. Anyone found in the possession of such illegally acquired content could face disciplinary and possible legal action. Concordantly, if any member of the MIS team should discover such content on client workstations, we reserve the right to preemptively remove such software or media without prior notification or due explanation. Additionally, the infracting officer could face disciplinary action.

4.4.7 Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4.4.8 Introduction of malicious programs into the network environment (e.g., viruses, worms, Trojan horses, e-mail bombs, malware or spyware etc.).

4.4.9 Revealing your account password to others or allowing the use of your account by others. This includes family and other household members even when work is being done at home. Supervisory staff should not share their account passwords with their secretaries, colleagues or other supervisees. Each officer will be held liable for all activity that has been logged by our servers for their account, irrespective of whether they were actively using it or not. As such, each officer should guard the security of their user accounts assiduously.

4.4.10 Using an OPM and CO computing asset to actively engage in procuring, transmitting or downloading material that is sexually explicit (pornographic literature, pictures, video, streaming media etc…); in violation of sexual harassment or hostile workplace laws; infringes on copyright and intellectual property rights;

4.4.11 The creation or transmission or downloading of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;

4.4.12 Making fraudulent offers of products, items, or services originating from within OPM and CO using any account issued by same;

4.4.13 Making statements about warranty, expressly or implied, unless it is a part of normal job duties;

4.4.14 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to: accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access or utilize, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet or e-mail spoofing, denial of service, and forged routing information for malicious purposes;

4.4.15 Port scanning or security scanning is expressly prohibited unless prior notification is given;

4.4.16 Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job or duties;

4.4.17 Circumventing user authentication or security of any host, network or account;

4.4.18 Interfering with or denying service to any user other than the employee's host (for example, denial of service attack);

4.4.19 Use any programs/scripts/commands, or sending messages of any kind, intended to interfere with, or disable a user's working session, via any means, locally or via the Internet/Intranet;

4.4.20 Providing information about or providing lists of the OPM and CO employees to parties outside the OPM and CO without appropriate authorization.

4.4.21 Exercising the use of internet services provided without moderation and responsibility. Specifically:

4.4.22 Visiting websites which serve leisurely purposes. These websites oftentimes create considerable amounts of traffic on the network thus causing a noticeable deterioration in the performance of other business critical internet services at peak hours during the work day.

4.4.23 Visiting websites which serve sexually explicit purposes or any other purpose which may be construed as illegal, unacceptable or inappropriate. This includes but is not limited to pornographic websites, hacker "dens", "torrent" indexing sites or any others which may directly or indirectly support copyright infringement or feature lewd or unwholesome content. Some of these websites may pose a security risk – especially where they offer free content.

Internet usage is audited by our servers daily – inclusive of every website visited by users of the network. Every website visited by users is logged with their user name and the time of access. If the MIS team discovers the persistent, inappropriate use of the internet services for the consumption of the abovementioned online activities, individuals can be easily identified and may be reported to their supervisors for disciplinary action.

4.5 E-mail and Communications Activities

The following uses of the e-mail services are strictly prohibited:

4.5.1 Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam), especially if such material is unrelated to the business of the OPM or the CO;

4.5.2 Any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages;

4.5.3 Forging of e-mail header information (also known as "spoofing");

4.5.4 Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies;

4.5.5 Creating or forwarding "chain letters" of any type;

4.5.6 Creating or forwarding inappropriate humor, including content with multiple image attachments which may be considered inappropriate.

4.5.7 Using unsolicited e-mail originating from within the OPM and CO network for other Internet/Intranet service providers on behalf of, or to advertise, any service not hosted by the OPM or CO or connected via the OPM and CO network;

4.5.8 Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spamming).

4.5.9 Using your GOJ assigned e-mail address to sign up for goods, services, newsletters or to partake in e-Commerce transactions online which are not pertinent to the business of the Government of Jamaica.

Most websites have a Privacy Policy that allows them to use your e-mail for marketing purposes to third parties once you sign up with them. It is usually stipulated in the fine print that most website users tend to ignore. The websites are usually not responsible for the content of these third parties. Thus, this will expose your e-mail to abuse at the hands of spammers and hackers. Furthermore, these individuals usually harvest addresses at high traffic websites (e.g. Yahoo, Hi5, MySpace, Facebook, etc.). Using the GOJ assigned address at any such site is an implicit invitation for unsolicited e-mail (i.e. spam).

4.5.10 Using your GOJ assigned e-mail address as a personal contact for non GOJ business related communication or other personal purposes. There are a number of implications for this:

a. Personal contacts may forward mail to your address that could also be simultaneously routed to people on the forward list that you don't know. Some of these people are either spammers or hackers and they tend to harvest e-mail addresses this way.

b. Our servers are audited on a daily basis for security reasons and incoming e-mail may be included in this audit for content. We will not be held responsible if highly sensitive personal information becomes compromised as a result of your choice to use your GOJ assigned address as such. Instead, use your own personal e-mail address, preferably one of the free online services available (eg. Hotmail, Yahoo, G-Mail) for your personal mail.

c. Where solicited mail is inadvertently detained by our spam blocking service, it is subject to be opened; read and either released, quarantined or left for summary deletion by members the MIS team. We will not be held responsible for any personal information that may become compromised because of this normal activity. For your protection, keep all personal messages out of the system, as every single message is logged.

4.6 E-mail Best Practices

The following is an outline of a set of best practices that the MIS team *suggests* staff members adopt with respect to the use of Corporate E-mail. Please note that these are not *rules*. Rather, they are electronic communication standards that have been adopted by similar entities worldwide. These standards maximize the effectiveness of this medium, while minimizing the negative impact on technical and human resources:

4.6.1 **Use Meaningful Subject Titles**. The e-mail subject is designed to raise attention to your e-mail's content. Therefore, always include a Subject. Never leave it blank. When your message has been archived along with a large volume of other e-mails, the subject header is the fastest way for your recipients to find a message you had sent. As such, ensure that your subject is descriptive and meaningful. Avoid using cryptic, single word or similarly inexplicable expressions for your mail subject. As a general guideline, assume that the subject of your e-mail would be published in a local newspaper.

4.6.2 **Use Blind Carbon Copy (BCC) or Mail Groups.** When sending mail to a particularly large number of recipients, it is *never* wise to put all of their e-mail addresses in the **To:** column. Make use of the *Distribution Groups* available to you. Groups such as '*All Staff*' were created explicitly for this purpose. However, if you are sending to a large number of people that aren't already configured in any existing distribution group, use the Blind Carbon Copy field to add their e-mail addresses. This way you won't expose anyone's e-mail address to all recipients as well as e-mail harvesters lurking on the internet who scan e-mails like these for addresses to send unsolicited mail.

4.6.3 **Know when to use Carbon Copy**. Messages directed at individuals in the **To…** column are those for whom it is directly relevant (or from whom action is required). Reserve Carbon Copy (i.e. Cc…) for individuals to whom a Copy of the message would be useful, but from whom a direct action is *not* required. Lumping all recipients in the "To…" column is bad practice for this reason and is the primary source of the "Reply-To-All…" mistake users regularly make.

4.6.4 **Use 'Reply-To-All' discriminately.** Do not use this feature unless your message is pertinent to all recipients of the message you are replying to. Otherwise you may be simply filling users' inboxes with irrelevant messages – much to their annoyance. If you *must* use the feature, double check to ensure that you remove those recipients to whom your response is not directed (especially if this contains any distribution groups). Indiscriminate use of this feature may inadvertently forward confidential portions of an e-mail conversation to users for whom such content is either above their clearance level or not at all pertinent.

4.6.5 **Use Distribution Groups Wisely**. Do not send a message to the entire membership of the "*Cabinet Office Staff*" or "*OPM Staff"* when you only meant to direct your message at a subset of people who fall under both organisations. If you need to regularly send messages to large teams of people on <u>this</u> network, simply send a request to the technical support team to have a distribution list created for you and the names of all the members. This would be especially useful for staff members from both organisations that sit on a committee. However, The Technical Support team will *not* create distribution lists for off-site contacts. Use your Outlook Contacts list to do that.

4.6.6 **Only attach Substantial Documents**. Do not send document attachments that are only a page or less in length. Simply create a new e-mail message with the content that would have been put in that document. This is especially pertinent to users who insist on creating a one page memo, then attaching that memo to an e-mail message. This practice consumes four times as much space in the e-mail database to communicate the same message as using just an e-mail message. The obvious exception of course, is where the attachment is scanned.

4.6.7 **Avoid attaching large files**. Avoid sending exceptionally large files (such as music, video, large PDF files, etc.) especially when sending a message to a large number of recipients. While the document size limit is 10 megabytes, large documents clog up e-mail inboxes, bringing them to their storage limit faster than usual. Rather, use a file host (e.g. www.yousendit.com) to upload the file. You will then be provided with a download link you can send via e-mail. You can optionally host the file on the organisation's website and hotlink to it from there. If you need assistance, contact technical support.

4.6.8 **Memo format is irrelevant in an E-mail**. It is unnecessary to re-create memo headings (To:, From:, Subject:, etc.) in your e-mail messages as the system automatically records and uses this information every time you create a new e-mail.

4.6.9 **Use the Out of Office Auto-Responder during extensive official absence.** This is a way of showing professional courtesy. If you are going to be out of office for an extended period of time, activate the out of office auto-responder from your mail client before you go on leave. Indicate how long you will be out of office, when you will return and to whom messages are to be directed. Failure to do so may incite one to be established for you by a member of the MIS team upon request from an authorized divisional officer.

4.6.10 **Avoid typing out e-mail addresses**. Use the global address list to access the addresses of all members of staff (click **To…** near the top of a new message) or use your Outlook contacts to store the addresses of offsite contacts. Typing an e-mail address in the To: box exponentially increases the risk of a typing error. This is the cause for over 80% of all returned (aka "bounced") messages, as users often type e-mail addresses incorrectly. When in doubt, you may consult the online staff directory at http://directory/.

4.6.11 **Use Mail Signatures**. Create a mail signature for your e-mail profile. This is basically a block of text that automatically appears at the bottom of every e-mail that you create. This block identifies yourself, your Post Title, your department or organisation and any relevant contact information. It adds a professional touch to your e-mail messages and automatically provides a way for your contacts to get in touch with you by other means. To do this:

a. From your Outlook main window, select **Tools → Options**

b. Go to the **Mail Format** tab.

c. Click the **Signatures…** button.

d. Click **New** and ensure that **Start with a Blank Signature** is selected. Type in a name for the signature. Click **Next**.

e. Fill in your signature. You can change the font and style of the text.

f. Click **Finish** when done. You can either create a new signature for Forwards and Replies, or use the same one that you just created.

g. Select the signature you just created by clicking on the appropriate drown down lists, (either **'Signature for new messages'** or **'Signature of replies and forwards'** then click **Ok**.

4.6.12 **Restrict the use of the High Priority flag.** If you constantly flag an e-mail message as “Urgent”, “High Priority”, “For Follow-Up” or use such prefixes in your subject header, messages from your Outbox will be treated with the same priority as those from the boy who cried wolf.

4.6.13 **Avoid the unnecessary use of Highlighted Text**. Unnecessarily **bolding**, colouring, underlining, using ALL CAPS or **ALL OF THE ABOVE** will not communicate a message any more clearly than being clear and concise. In fact, unnecessarily highlighting text in e-mails can be interpreted as shouting.

4.6.14 **WORM: Write Once, Read Many**. At the risk of stating the obvious, please *read* your messages several times *before* you hit the send button. Ensure that spelling and grammar check out before responding. Check the tone of the messages you write. Remember that body language and voice are missing from written words. Ensure that the message is being sent to the *right* individual(s). Failure to do this may invite a poor reflection on the sender or the organisation. While the MIS team can possibly retrieve messages that have been inadvertently sent, this is limited to messages sent on *this* domain. Messages sent external to this network *cannot* be retrieved. When in doubt, ask for a second opinion. These are basic tenets that must be met with every message.

4.6.15 **Be cautious about Background Patterns**. A number of staff members have taken to the use of Background Patterns and other decorative styles for their e-mail messages. This is generally unacceptable in a corporate environment. Background patterns (if used) can seriously inhibit the readability of your message. Please remember that Stationery (as they’re called in Outlook) was designed for home use. Also, they only work with very specific font patterns and colours in mind. The best practice is to avoid the use of these patterns altogether as where readability suffers for most users, it becomes impossible to users who may be colour blind. The default plain white backgrounds and dark coloured text are the recommended configuration.

4.6.16 **Do not forward Virus Warnings**. Our network is protected by a Corporate Antivirus mechanism that *automatically* updates itself to protect the network against all of the latest viral threats. Forwarding an e-mail about a virus warning is the *least* efficient way to warn anyone of such threats. Therefore, any warning you are tempted to forward will likely either be outdated or a hoax. This is exactly why anti-virus programs have an auto-update feature. Chances are that forwarding such messages will only irritate recipients.

4.7 Laptop Security Tips

Some officers will be required to use mobile computers in the performance of their duties. The onus lies upon those officers to ensure the security of these machines. Failure to do so will require the immediate re-imbursement of the Government of Jamaica for cost of the machines. To help secure your mobile computers:

4.7.1 While on the compound, ensure that the machine is locked in your office, in a safe, or a similarly secure location while away from your workstation. If you will be away from the machine for an extended period of time, close the lid. The machine will automatically lock the workstation and require a password for access.

4.7.2 Always carry the device in the cases provided. Most laptops were not designed to sustain concussive forces in excess of 1 g.

4.7.3 Never leave the machine in your car or other mode of transportation. Vehicles parked in a sunlit area often generate extreme temperatures sufficient enough to permanently damage the liquid crystal display.

4.7.4 Always remove the machine from your car once parked in an area for an extended period of time. Even if your vehicle is tinted, a visible laptop sitting in your vehicle will significantly increase the likelihood of theft.

4.7.5 Never loan your laptop to members of your household, friends or family. You will still need to authenticate on our network once the machine is returned to the compound. Thus any inappropriate activity will likewise be logged by our servers once the machine is reconnected to our domain.

4.7.6 Refrain from the using the device for personal purposes. All laptops remain the property of the Government of Jamaica. Laptops may be re-assigned without prior notice. We cannot guarantee the safety of any personal information found on the machines once re-assigned. Officers granted the use of a laptop should instead seek to procure a personal home computer for such purposes.

4.7.7 Officers who are required to use laptops must be aware of special arrangements with the Ministry of Finance (and other external Government auditing bodies) with respect to these machines. The Government does not insure against accidental or loss of laptop computers. Thus, any officer who is required to use a laptop in his / her service to the Government will be liable for replacing it in the event of theft, fatal damage or other loss while in possession of the laptop in any environment external to the premises of the Offices of the Cabinet and Prime Minister, irrespective of the conditions under which it was damaged or lost. Therefore, laptop users are required to utilize special care and caution when handling this or any other piece of equipment whenever they are being removed from the premises.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action where necessary, which may include termination of employment in compliance with procedures contained in the Government of Jamaica Staff Orders.

6.0 Terms of Use Agreement

Once you have exercised your privilege to access the ICT resources of the OPM and CO it indicates your full agreement with the terms and conditions of use and agree to be legally bound to the terms and conditions contained herein.

7.0 Definition of Terms

Ad-ware – A program that hides inside a computer system (usually through hijacking a web browser or hiding inside some other free software) and then using that computer to deliver direct, unsolicited marketing via random pop up messages and unsolicited mail.

Denial of Service attack – A hacking technique that overwhelms an internet server such that users connected to it will no longer be able to access the service.

e-Commerce – Any internet based monetary transaction, usually involving a credit card, electronic funds transfer or electronic banking.

Hacker – An individual whose primary intent includes surreptitiously gaining access to computer systems or inflicting damage to those systems usually by bypassing computer security protocols through the use of malicious code, viruses, Trojans, or other types of attack which could cripple these systems.

Hosts – Any device that accesses the network. This includes computers, printers, handheld devices (PDA's, smart phones, etc…).

Mail Bomb – A computer virus or a direct hacking technique which exploits the mailing system to clog user inboxes with several hundred (or thousands) of junk messages, thus overwhelming the system.

Piracy – Any media, including video, audio, pictures, literature or any other copyrighted work which was acquired without a license or proof of ownership, by breaching a copyright distribution requirement or through a peer to peer network.

Social Networking – A popular trend in internet pop culture where users share personal and contact information on the internet for collaborative purposes.

Spam – Unauthorized and/or unsolicited electronic mail.

Spoofing – An internet jargon which means to deliberately falsify the source of a piece of communication, usually the original address of an e-mail message, or data packet.

Spyware – A special type of computer virus that hides itself in a computer system and focuses on data mining a user's computer for personal information (such as bank account numbers, credit card information, login names and passwords) that is then relayed to hackers or spammers.

Trojan – A special type of computer virus that opens otherwise secure gateways on a computer system thus allowing hackers to gain access to the system.

Virus – A malicious piece of code which causes considerable harm to computer systems by interfering with the normal operation of that system, including data loss. Computer viruses typically use simple artificial intelligence to propagate within that computer system.

8.0 Revision History

The OPM and CO reserves the right to revise and update this Policy at any time without notice. We will attempt to notify our employees, clients and customer of any such modifications electronically and by other means where possible.