FACT SHEET – SECURE USAGE OF EMAIL IN THE CIVIL SERVICE

Email Usage

Electronic mail (email) is the transmission of messages over computer networks. Officers in the Civil Service readily make use of the Government Email Service (GES) for official purposes. GES is provided in support of public officers' daily duties and administrative functions. GES can be accessed through a Web browser or via an email client such as Microsoft Outlook.

Use of email via GES is governed by the Email Usage Policy which had previously been circulated to all Ministries and Departments. Users of GES should comply to provisions of the Email Usage Policy which can also be accessed at the G2G section of the Government Web Portal[1].

Security Threats for Email

- **Spam**: Spam emails are unsolicited electronic messages usually transmitted to a large number of recipients. Spam emails usually have a commercial focus, promoting/selling products or services. Spammers collect email addresses from the Internet. Do not respond to spam emails. *(For more information, refer to the Spam Fact Sheet)*

- **Viruses/Worms within Email**: A virus is a program that is loaded into your computer and runs without your knowledge. Viruses can have harmful effects ranging from displaying annoying messages to stealing data or giving a hacker control over your computer. A worm is a type of virus that creates exact copies of itself on its own and use computer networks to spread itself. *(For more information, refer to the Computer Virus Fact Sheet)*

- **Phishing**: Phishing emails contain links which look legitimate but they direct the recipient to a lookalike site set up to collect login and password information. E.g. for credit cards and/or bank account details. *(For more information, refer to the Phishing Fact Sheet)*

- **Identity Theft**: If someone obtains your email account details (username and password), he or she can log in as you and send messages making as if the message is being sent by you. Your email identity can thus be stolen and you may be held accountable for the emails sent from your account. To protect access to your email account, you should adopt good password management practices. *(For more information, refer to the Effective Password Management Fact Sheet)*

- **Forging of Emails**: An email can be forged which makes it appear as if it originates from a credible or known user other than the actual fraudulent source. Such an email is sent to users in an attempt to entice the receiver to open and respond to the message which can have malicious content. Verify the origin of any suspicious emails.

- **Disclosure of Information**: When emails are used to transmit sensitive confidential information from an organisation to a third party, adequate security measures must be taken to prevent unauthorised disclosure of information. Users should adopt additional security measures such as password protecting the attachment and should ensure that the email address of the right recipient(s) is correctly typed.

Managing Government Email Accounts

The GES, hosted at the Government Online Centre, is protected by antivirus software and an anti-spam appliance. GES emails are thus scanned for viruses and majority of spam emails are blocked. Administration of GES is effected by the Postmaster of CISD and end user support is provided by CISD Help Desk (211-2480). At the individual level, additional simple measures can be taken for a safer usage of email as follows:

Good housekeeping

Properly managing your email account goes a long way towards safe email usage.

- **Good Password Selection**: Passwords are an important aspect of email security. A poorly chosen password may result in the compromise of your email account. *(For more information, refer to the Effective Password Management Fact Sheet)*

- **Email Quota**: When you access your email via a Web browser, all your email data resides on the email server. Your email account has a fixed storage size (quota) and when your quota is full, you will not be able to receive new emails.

[1] The G2G section of the Government Web Portal (www.gov.mu) contains the Email Usage Policy and Fact Sheets circulated previously.

Regularly remove unnecessary emails by deleting them and then empty the "Deleted Items" or "Trash" folder to free storage space.

- **Suspicious Emails from Unknown Sender**: When you receive unknown emails from senders that are not familiar to you, verify that any attachments included are not infected with viruses or worms. Do not respond to such email, if possible.

- **Dealing with Spam**: The total amount of spam received can be cut down drastically by blocking the sender of spam emails. This can be done by enabling the spam filters if you are using an email client such as Microsoft Outlook or by informing the GES Postmaster for blocking at GES level.

- **Backup**: Ensure that you keep a copy of important emails and attachments on a removable media such as a CD or a pen drive. If you are using an email client such as Microsoft Outlook, it is important that you regularly back up your email data file so that you may recover in the event of a computer failure. You may contact your IT support to assist you on backing up your email data.

- **Heavy Attachments**: If the attachment is a large file, sending it may use up the receiver's email disk space quota thus preventing the receiver from using his/her email facility. Avoid sending unnecessary large files as attachments.

Additional measures for using email on public/shared PCs

When checking your email on a computer used by several persons or in a public place like a cyber café, some additional measures to adopt are:

- **Delete Browser Cache and History**: Most browsers automatically keep track of all the Web pages that have been visited, and some may keep track of passwords and personal information that could have been entered. After using a public PC, it is important to delete the browser cache and history.

- **Closing the Browser**: After checking your email on a public or shared PC, log out of your email account and ensure the closing of the browser window completely.

DOs

- ✓ Respect email laws and regulations
- ✓ Use meaningful subject lines in your email messages. Do not leave it empty as it may be rejected by certain spam filters
- ✓ Change your password frequently and choose a strong password
- ✓ Regularly purge unnecessary emails to free storage space
- ✓ Make use of email signatures indicating job title, Ministry/Department affiliation, address, and other particulars
- ✓ Be suspicious of any email with urgent requests for personal, financial or password information
- ✓ If sensitive information must be sent by email, added security features must be employed
- ✓ Emails from unsolicited senders should be viewed with care. Use caution when opening attachments
- ✓ Back up your email at regular intervals
- ✓ When not in office for many days, configure an *"on leave"* message so that senders are informed and do not send more emails - hence reducing the probability of exceeding your email quota

DON'Ts

- ✘ Never share or reveal individual passwords for your email account
- ✘ Do not let others access your account
- ✘ Avoid giving out your official email account unnecessarily
- ✘ Do not send bulk emails such as chain letters or jokes with heavy attachments (images) to colleagues and friends
- ✘ Avoid filling out forms in emails that ask for personal, financial or password information
- ✘ Do not readily click on suspicious attachments coming from unsolicited sources
- ✘ Do not include your email address in any transaction that does not explicitly require it

Assistance

For issues regarding email (spam, phishing etc.), inform the Postmaster at *postmaster@mail.gov.mu*. Should you require any technical assistance at your premises, contact your Database Administrator or IT Technical Support (211-2480). For further advice, you may contact the IT Security Unit, Ministry of ICT (210-0201) or email *itsecurity@mail.gov.mu*.