**E-Mail Usage Policy**

Prepared By

**IT Security**

**VERSION: 1.0**

All rights reserved. This document is a proprietary product of IT Security and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission from IT Security, is strictly prohibited. Any printed copy of this document is uncontrolled

**CHANGE HISTORY**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Date** | **Summary of changes** | **Author** | **Pages affected** | **Remark** |
| 1.0 |  |  |  |  |  |
|  |  |  |  |  |  |

Table of Contents

***GENERAL EMAIL USAGE POLICY 4***

**USER IDENTITY & EXTERNAL REPRESENTATIONS 4**

**PRINCIPLES ON EXPECTATION OF PRIVACY 5**

**GUIDELINES ON USAGE ACCOUNTABILITY 5**

**GUIDELINES AGAINTS PROHIBITIVE USAGE** **5**

**NON-REPUDIATION & DATA INTEGRITY REQUIREMENT 6**

**RETENTION OF E-MAILS FOR LEGAL DISCOVERY 6**

**E-MAIL ADMINISTRATORS POLICY SPECIFICS 6**

**E-MAIL GATEWAY AND SERVERS SECURITY 7**

***REMOTE EMAIL ACCESS POLICY 7***

***ENFORCEMENT 7***

## *GENERAL EMAIL USAGE POLICY*

* 1. ***Email messages should only be accessed by parties they are intended for.***
  2. ***Staff should be cautious when opening emails received from unknown senders as these emails may contain viruses, email bombs, or Trojan horse codes.***
  3. Staff should adopt good emailing practices, such as: -
     + 1. Do not send cc or bcc unnecessary.
       2. Use ‘Reply All’ only when you need to disseminate to all parties from the previous mail
       3. Avoid attaching graphics files, e.g. BMP, JPEG, TIG, GIF
       4. When forwarding/replying emails, do delete the previous mail or attachment unless you need it for reference
       5. Keep the size of the email small, as big emails may jam up the receiving parties’ accounts
  4. Staff should not send the following types of information over unknown or uncertain email locations or broadcast channels: -
     + 1. Information pertaining to questionable survey on Organization’s practices
       2. Any Organization data or sensitive information such as strategic plans, personnel matters or finances, etc.
       3. Information of userid and/or password that would allow third party to breach security of a given account.

1. **USER IDENTITY & EXTERNAL REPRESENTATIONS**
   1. E-mail systems must employ personal user-IDs and associated passwords to identify the users. Users must not use an e-mail account assigned to another individual to either send or receive messages. In addition, user must not allow anyone else to send e-mail using his or her accounts.
   2. Misrepresenting, obscuring, suppressing, or replacing a user's identity (spoofing) on an electronic communications system is forbidden.
   3. The user name, e-mail address, organizational affiliation, and related information included with messages or postings must reflect the actual originator of the messages or postings.
   4. Users using corporate resources to access the Internet shall conduct themselves with the view of their affiliation with the company. Users should therefore: -
      * 1. Be aware that disclaiming one’s opinion as not reflecting that of the company in the messages posted in public or private discussion does not absolve their liability
        2. Refer to the Public Affairs Department all questions and queries from the public or outside organizations on matters relating to the company and not communicate on behalf of the company unless prior authorization is received from the Management
        3. Comply with the company’s Data Classification Policy on matters pertaining to releasing of internal information to the outside.
   5. Employees should not use own private e-mail (e.g. privately subscribed web mail at free public-domain service or e-mail service that comes with one’s private Internet Service Provider- ISP account) for official business communication purposes.

## PRINCIPLES ON EXPECTATION OF PRIVACY

* 1. E-mails sent or received using the Company’s resources and/or sent from the Company’s e-mail account, including back-up copies, are considered to be the property of the company.
  2. Although it is the policy not to regularly monitor the content of electronic communications, users expressly waive any right of privacy in anything they create, store, send, or receive on the computer or through the Internet or through any other computer network.
  3. The company has the right, but not the duty, to monitor any/all aspects of its computer system, including, but not limited to, monitoring sites visited by users on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded or uploaded by users to the Internet, and reviewing e-mail sent and received by users.
  4. It may be necessary for authorised personnel to review the content of an individual employee's communications during the course of problem resolution or in an investigation. The access privilege to perform such review should be authorised by the proper approval channels as decided by the Management.
  5. Except as otherwise specifically provided, users may not intercept or disclose, or assist in intercepting or disclosing, e-mail communications. The Company is committed to respecting the rights of its employees, including their reasonable expectation of privacy.

1. **GUIDELINES ON USAGE ACCOUNTABILITY**
   1. E-mail generally must be used only for business activities. Incidental personal use is permissible so long as: -
      * 1. It does not consume more than a trivial amount of resources
        2. Does not interfere with user productivity
        3. Does not pre-empt any business activity

## GUIDELINES AGAINTS PROHIBITIVE USAGE

## Users should not send e-mails containing profanity, with seditious content, of defamatory nature or other unlawful or inappropriate remarks.

* 1. Users should not send unsolicited commercial (junk-) e-mail to anyone, whether directly from their corporate e-mail account, through a third-party spammer, through a spam relay, or in any way using forged headers.
  2. Users should not use e-mail to harass anyone, specifically, it is forbidden to: -
     + 1. Send large numbers of messages to an individual or a group (mail-bombing),
       2. Attempt to subscribe anyone else to mailing lists.
  3. Users should not send e-mails with virus, Trojan Horse or worm to anyone.
  4. Users are forbidden from using electronic communication systems for charitable endeavours, private commercial activities, or amusement/entertainment purposes.
  5. ***Users must not use e-mails to conduct financial transactions on behalf of the Organization unless explicit permission has been obtained from management and the necessary security controls is in place.***

## NON-REPUDIATION & DATA INTEGRITY REQUIREMENT

* 1. E-mail messages that have non-repudiation requirement for authenticity purposes (e.g. e-mails that carry authorisation) should be supplemented with additional controls, e.g. digital signatures, public-key-infrastructure (PKI) arrangement or a manual confirmation process put in place.
  2. E-mail messages that have higher data integrity requirement (e.g. e-mails with attachment documents) should be supplemented with additional control such as checksum, hashing or message-digest mechanism, and the subsequent process for counter-confirmation, or an alternative manual process.

## RETENTION OF E-MAILS FOR LEGAL DISCOVERY

* 1. Systems administrators must establish and maintain a systematic process for the recording, retention, and destruction of e-mail messages and the accompanying logs. The destruction of both logs and the reference e-mail messages must be postponed whenever a subpoena, discovery motion or other legal notice is received. Such destruction should also be postponed if the material might be needed for an imminent legal action.

## E-MAIL ADMINISTRATORS POLICY SPECIFICS

* 1. E-mail administrators must ensure all incoming e-mails be scanned by default for viruses and other malign content on the user desktop.
  2. E-mail administrators must ensure that accounts are properly maintained. Procedures must be documented and in place for handling activation, de-activation, and removal of e-mail accounts.
  3. Email accounts for individuals no longer requiring access, or no longer with the company must be promptly disabled immediately and permanently removed.
  4. Explicit management consent is required before an e-mail or system administrator may access e-mail messages that are not his/her own.
  5. E-mail administrators must establish and maintain a systematic process for the recording, backup, retention, disaster recover procedures and destruction of e-mail messages and accompanying logs.

##### E-MAIL GATEWAY AND SERVERS SECURITY

* 1. Each production e-mail server and gateway must have identified a primary and secondary e-mail administrator, who is responsible for the account administration, maintenance, and backup of the system.
  2. E-mail gateways are visible to the Internet and therefore vulnerable to external attacks. Therefore, they should generally be implemented as single purpose machines and never shared with other internal servers. They should also be secured in a protected area.
  3. Anti-virus filtering mechanisms must be installed on the e-mail gateway.
  4. All e-mail sent through the mail server is archived and subject to review by people other than the recipient and sender.

1. ***REMOTE EMAIL ACCESS POLICY***
   1. ***Staffs are given Remote Access for the sole purpose of conducting official business.***
   2. ***The use of remote email service is governed by the established requirements stated in the Organization’s Email Usage Policy.***
   3. ***The Organization reserves the right, at its sole discretion, with and without notice, to remove the given account if the staffs are found to misuse the facility.***
   4. ***It is strongly advised that remote email access should not be done at unsecured locations, such as Cyber Café (as Trojan programs and Viruses are commonly found at those desktops). If the remote access is needed and unavoidable, staff must ensure that the accessed desktop is switched off / rebooted after use.***
   5. ***Staff must inform the IT Security Department immediately if the remote access is found to be compromised (such as Token’s PIN password is changed without notice, Sign-on password is rejected by the system, etc).***
2. ***ENFORCEMENT***

# *All staffs are required to comply with this security policy and its appendices. Disciplinary actions including termination may be taken against any Organization staffs who fail to comply with the Organization’s security policies, or circumvent/violate any security systems and/or protection mechanisms.*

# *Staff having knowledge of personal misuse or malpractice of IT Systems must report immediately to management and IT Security.*

* 1. ***Organization’s staff must ensure that Organization’s contractors and others parties authorized by the Organization using its internal computer systems, comply with this policy.***
  2. ***Where the role of the service provider is outsourced to a vendor, the outsourced vendor should ensure compliance with this policy.***