Policy:Email and Internet

CLASSIFICATION	**PUBLIC**
Attention	The information is intended for the private use of Capillary. By viewing this document, you agree to keep the contents in confidence and not copy, disclose, or distribute this without written request to and written confirmation from Capillary. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of the contents of this document is prohibited.
Copyrights	Capillary Technologies Pvt Ltd The controlled master of this document is on the Capillary's Computer network. Printed copies are not controlled. If you are working from a printed copy, please verify the document version to ensure it is the latest revision.

Document Management Information

Document	Email and Internet
Document ID	Email_and_Internet_Policy
Version	2.0
Document Creation Date	22-Jan-2011
Classification	PUBLIC

Scope

This document lists out the policy for proper email and Internet related mechanisms to be followed by the IT team to ensure information security at Capillary.

Policy Statement

Policy states all the rules that are to be followed to safeguard and increase the security of all the information assets of Capillary, contained in the emails, taken care by the IT team of Capillary. It also pertains to have in place the necessary security mechanisms to prevent risks faced by Capillary form improper internet security controls and their awareness.

Purpose

Purpose of this policy is to provide useful guidelines to help IT Team maximize the security posture to defend Capillary from all the security risked faced by it from improper email and internet configurations, practices and controls.

Policy Sections and Clauses

Email Types Under Consideration

- Business emails are those used during the day-to-day operations within your department or with other departments within Capillary or with organizations outside Capillary for a business-related issue.

- Personal emails are those, which have no relationship to Capillary's operations and are usually correspondence with friends or family, responses to advertisements, purchase of personal goods, etc. Capillary email account is strictly for business purposes except in situations of hardship or duress.

- Spam or unsolicited email is advertisements about products or services, which you have not requested for. This is usually sent if your email address has been published somewhere on the Internet, or if you filled up an online form and did not specifically request for emails NOT to be sent. So it has to be ensured that email address, phone numbers or other contact details are not disclosed freely & without need. Spam emails consume resources such as bandwidth of the network, and reduce the speed of network. At the same time they utilize the space allotted for saving legitimate Capillary's business related mails.

Making Users Aware

IT team has to make people aware of the following points:

Personal Usage

If personal communication using Capillary's network need to be sent, then they should be done so only in situations of hardships or duress, and as long as they do not:

- Interfere with the operation of Capillary's computing facilities by wasting computer resources or unfairly monopolizing them to the exclusion of others. Computer based resources - such as network bandwidth and storage capacity - are not unlimited;
- Diminish the User's productivity in terms of work-related obligations; and
- Violate the rules contained in this or any other applicable policy.

Prohibited Use

Emails should not be sent for:

- Pornographic texts or images
- Material promoting sexual exploitation or discrimination, racism or violence
- Messages that are derogatory or inflammatory regarding race, age, disability,
- Commercial advertisements
- Taking part in competitions
- Conducting activities, which are in violation of any of the applicable laws

- For registering to any web-sites or seeking information from any web-site unless required by business.

Sending And Receiving Sensitive Emails

- Messages sent/received to/from e-mail accounts outside Capillary e-mail system over the public Internet are not protected by Capillary security & can be easily read, changed and forwarded without any permission.
- To limit the dissemination of restricted information, forwarding of e-mail to addresses outside Capillary is not permitted without a copy being saved in Capillary's system.
- Users must not send any sensitive information or parameters (such as fixed passwords or account numbers) through e-mail unless the message has been suitably protected.
- When sending sensitive information, the use of the Return Receipt function is recommended.
- Email clients should not have password saved. The User must enter his login credentials each time he opens the email client.

Email Communication With Client

- All business email should only come from e-mail addresses that are official and not personal. Users should not solicit or send business emails to customers or others to or form personal email addresses such as yahoo, gmail, and so on, except in cases where there is no better alternative and then also only on infrequent occasions.
- All business mails that are of importance - whether sent or received must be retained and stored on the PC and appropriate back up can be taken of all important correspondence.

Internet Usage

- All Users who have been given access to emails and Internet have the responsibility to use Capillary's computer resources and Internet in a professional, lawful and ethical manner.
- Since computer-based resources - such as network and storage capacity - are not unlimited, all Users connected to the Capillary's Computer Network are responsible for conserving these resources.
- Staff members must not perform deliberate acts to waste computer resources or unfairly monopolize resources to the exclusion of others, or participate in any activities, which are in violation of applicable laws.
- All Users should make utmost effort to safeguard business documents like tenders, reports, training materials, citizen information and other confidential information. They should be sent either by encrypting it or password protected.
- The Internet is provided also for business purposes only. Internet should not be used for:
    - Visiting pornographic websites or downloading images or files of a sexual content
    - Downloading music files and videos of any type
    - Software for which licenses have not been purchased, or which is not for business use. If you feel there is a software that you would like to use for business use, then you should email the Administrator requesting it, and they will obtain the necessary authorization
    - Material promoting sexual exploitation or discrimination, racism and violence
    - Information concerning drugs or weapons
    - Destructive codes (e.g. viruses, self-replicating programs) and material concerning 'hacking'
    - Mass mail or chain letters
    - Personal solicitations and promotions
    - Commercial advertisements any other unauthorized material

- Sending security parameters: Users must not send any sensitive parameters, such as telephone calling card numbers, fixed passwords or account numbers, through Internet unless the connection has been encrypted.

Frivolous Use

- Frivolous use of the Computer Network and Internet Services is discouraged because it wastes computer resources or unfairly monopolizes these resources to the detriment of others.
- Frivolous use includes, but is not limited to:
  - Spending an excessive amount of time on Internet web sites
  - Downloading games or entertainment software
  - Playing on-line games
  - Engaging in on-line personal chats or chat groups.
  - Uploading or downloading large files
  - Excessive access to streaming audio and/or video files
  - Creation of unnecessary loads associated with non-organization-related use of Internet.

Configuration And Application Of Security Controls

- IT team has to ensure that the email server and server-client communication channels have to be configured taking into consideration the criticality of the information assets being protected and security requirements for those.
- Usage of defaults (default configurations, assignment of default passwords, etc) should be avoided.
- Proper practices for the following good security practices, but not limited to, are to be devised and communicated to all Users:
  - Changing the first time logon password given by IT Team
  - Incident response plan
  - Procedure for changing passwords of email clients in Capillary
  - Downloading, browsing and using Internet resource as stated by Acceptable Usage of Information Assets Policy and related procedures
- IT team has to also ensure that the email server/s and network security devices are patched at regular intervals to prevent any vulnerability, if any, from being exploited.
- Various devices and channels to facilitate Internet usage are aptly configured (content filters, firewalls, routers and switches, etc).
- Backup of configurations are maintained and tested.
- Capacity planning has to be done and the devices, communication channels and other resources facilitating emails and Internet usage are to be monitored for their health regularly; and fault if any is to be tackled as per the Incidence Response Plan devised.

Monitoring Email And Internet Use

Capillary reserves the right to monitor and log any and all aspects of its computer system, including, but not limited to monitoring:

- The content of End-User systems and personal computers (if used to access or act on assets of Capillary)
- Chat groups, newsgroups and other Internet sites visited

- Files downloaded
- All communications sent and received electronically
- Firewall and other network devices logs
- Content filter/proxies logs

Enforcement

Necessary disciplinary action will be taken against any Employee not following the Policies and Procedures laid down by Capillary.

Similarly, action will be taken against those Employees encouraging/observing such an activity and not reporting the same to the concerned authority.

Any Employee found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.

Special Situations and Exceptions

If Capillary's Management, Indian Government, or any other Regulatory Body's/Bodies' norms overwrites Capillary's Acceptable Usage of Information Assets Policy at a particular point in time.

Procedures

Capillary maintains internal procedures for ensuring effective IT related Housekeeping.

- This page was last modified on 2011 March 29, at 18:21.