



Smartlink Network Systems Ltd.	
<i>Document Title</i>	Email Use Policy
<i>Document Version</i>	1.6
<i>Document Approval Date</i>	19th November 2010
<i>Document Effective Date</i>	31st December 2010
<i>Document Last Updated Date</i>	16th May 2012

Email Use Policy

1.0 Purpose

To prevent tarnishing the public image of Smartlink, whenever email goes out from Smartlink the general public will tend to view that message as an official policy statement from the Smartlink.

2.0 Scope

This policy covers appropriate use of any email sent from a Smartlink email address and applies to all employees, vendors, and agents operating on behalf of Smartlink. It is the responsibility of each such person to strictly follow these guidelines.

3.0 Policy

3.1 Email Usage. Smartlink email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Smartlink employee should report the matter to their supervisor/IT dept immediately. IT dept recommends employees to avoid preserving emails on server beyond 400MB of storage capacity, as the same can be downloaded on client PCs.

a) Backup of Emails on Server –

- ❖ Daily full Backups (daily full backups rotated on one disk for a period of one month.)
- ❖ Monthly Backups (contains month-end backup - taken on first day of next month - total 6 disks, rotated twice a year.)
- ❖ Off-site Mail archiving – (Last six month-end backups are preserved.)

b) Maximum mail size to be received & sent outside Smartlink Network is 8MB.

c) Backup of Emails on client PCs -

1. IT dept does not maintain client-side mail backups.
2. Employees if required can archive “Client-side emails” from their PCs to CD/DVDs at regular intervals. IT dept will assist those employees one time on the archiving process, further to this they can refer to the archiving procedure notified by IT dept. Employees with PCs without CDROMs can put in temporary accessory request for CDROM drives to IT dept as and when required.

3.2 Personal Use.

Using a reasonable amount of Smartlink resources for personal emails is acceptable. Sending chain letters or joke emails from a Smartlink email account is prohibited. Virus or other malware warnings and mass mailings from Smartlink shall be approved by authorized VP before sending. These restrictions also apply to the forwarding of mail received by a Smartlink employee.

3.3 Monitoring

Smartlink employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. Smartlink may monitor messages without prior notice. Smartlink is not obliged to monitor email messages.

3.4 Email Usage

Employees must exercise utmost caution and are responsible when sending any Smartlink email to recipients either internal or external. Smartlink emails should not be automatically forwarded to external destination. Sensitive information should not be forwarded, unless that email is critical to business and is encrypted/content-secured with password protection.

4.0 Enforcement

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

5.0 Definitions

Term	Definition
Email	The electronic transmission of information through a mail protocol such as SMTP or IMAP or NRPC or POP. Typical email clients include Mozilla Thunderbird, Evolution, Outlook Express, Windows Mail and Microsoft Outlook or Mobile mail application.
Forwarded email	Email resent from an internal network to an outside point.
Chain email or letter	Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.
Sensitive information	Information is considered sensitive if it can be damaging to Smartlink or its customers' reputation or market standing.
Virus warning	Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people, both inside and outside Smartlink, who do not have a need to know that information.
Daily Backups	Backups scheduled on daily basis either as Full backup or Incremental backups.
Rotate backups	Backups which are overwritten on previous backup.

6.0 Revision History

Version	Date	Author	Remarks
1.0	14 th October 2009	Kiran Gole	Document created
1.0	15 th October 2009	Sandeep S	Discussed with Security Committee / Head
1.1	15 th October 2009	Kiran Gole	Document updated.
1.1	15 th October 2009	Sandeep S	Approved by Security Committee / Head
1.2	11 th November 2009	Kiran Gole	Document updated – added 3.1 (a) & (b).
1.2	11 th November 2009	Sandeep S	Approved by Security Committee / Head
1.3	12 th November 2009	Kiran Gole	Document updated – modified 3.1 (a).
1.3	12 th November 2009	Sandeep S	Approved by Security Committee / Head
1.4	13 th November 2009	Kiran Gole	Document updated.
1.4	13 th November 2009	Sandeep S	Approved by Security Committee / Head
1.5	26 th October 2010	Kiran Gole	Document updated.
1.5	19 th November 2010	Shridhar K	Approved by Security Committee / CTO

1.6	16 th May 2012	Mayur Gujar	Name & Logo updated
-----	---------------------------	-------------	---------------------