Smartlink Network Systems Ltd.	
Document Title	Antivirus Policy
Document Version	1.5
Document Approval Date	19th November 2010
Document Effective Date	31st December 2010
Document Last Updated Date	16th May 2012

Anti-virus Policy

1.0 Recommended processes to prevent virus problems:

This policy is to be read in conjunction with the Acceptable use Policy. It provides guidelines for all employees to follow in relation to protecting Smartlink network, from virus attacks. It is the responsibility of all Smartlink employees to strictly follow these guidelines.

- IT Dept shall install standard corporate antivirus software with latest definitions & anti-virus updates set to auto-daily/weekly when the PCs are allotted to the employees. Software virus definitions are updated automatically through antivirus server/Internet in most cases with exception to roaming clients at branch/remote locations. However in cases where employees have received PCs earlier and/ or the software is older/ auto-updates are non-functional, employees should contact IT Dept.
- Always run the corporate standard, supported anti-virus software. Follow any special IT instructions during virus outbreaks.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then “double delete” them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding, as per *Acceptable Use Policy*.
- Never download files from unknown or suspicious sources.
- IT Dept does not recommend direct disk sharing (e.g Windows Sharing with read/write access). It is not recommended to utilize USB drives/memory cards for data sharing, instead utilize on-site file servers. In remote locations where file servers are in-accessible, it is user responsibility to always scan a USB flash drive / USB Hard Disk drive / floppy diskette from a known/unknown source for viruses before using it.
- Lab tests should not be performed in production network in any circumstances, unless approved in written from IT Dept for specific period & unless there is absolutely a business requirement. It is recommended that if lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, and then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing by use of any communication medium.

2.0 Revision History

Version	Date	Author	Remarks
1.0	23rd September 2009	Kiran Gole	Document created
1.0	15th October 2009	Sandeep S	Discussed with Security Committee / Head
1.1	15th October 2009	Kiran Gole	Document updated.
1.1	15th October 2009	Sandeep S	Approved by Security Committee / Head

1.2	11 th November 2009	Kiran Gole	Document updated – 1.0 Antivirus software signatures updated automatically.
1.2	11 th November 2009	Sandeep S	Approved by Security Committee / Head
1.3	13th November 2009	Kiran Gole	Document updated.
1.3	13th November 2009	Sandeep S	Approved by Security Committee / Head
1.4	26th October 2010	Kiran Gole	Document updated.
1.4	9th November 2010	Kiran Gole	Document updated.
1.4	19th November 2010	Shridhar K	Approved by Security Committee / CTO
1.5	16th May 2012	Mayur Gujar	Name & Logo updated.