Smartlink Network Systems Ltd.	
Document Title	Acceptable Use Policy
Document Version	1.4
Document Approval Date	19th November 2010
Document Effective Date	31st December 2010
Document Last Updated Date	16th May 2012

Acceptable Use Policy

1.0 Overview
Intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Smartlink's established culture of openness, trust and integrity. The IT Dept is committed to protecting Smartlink's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Smartlink. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Smartlink employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose
The purpose of this policy is to outline the acceptable use of computer equipment at Smartlink. These rules are in place to protect the employee and Smartlink. Inappropriate use exposes Smartlink to risks including virus attacks, compromise of network systems and services, and legal issues. It is the responsibility of each Smartlink employee to strictly follow the acceptable use policy.

3.0 Scope
This policy applies to employees, contractors, consultants, temporaries, and other workers at Smartlink, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Smartlink.

4.0 Policy
4.1 General Use and Ownership

1. While Smartlink's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Smartlink. Because of the need to protect Smartlink's network, management cannot guarantee the confidentiality of information stored on any network device belonging to Smartlink.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. If there is any uncertainty, employees should consult the IT Dept.
3. The IT Dept recommends that any information that users consider sensitive or vulnerable be either password protected or encrypted.

4. For security and network maintenance purposes, authorized IT individuals within Smartlink may monitor equipment, systems and network traffic at any time.
5. Smartlink reserves the right to audit networks and systems on a periodic basis or whenever required to ensure compliance with the IT Policies.
6. IT dept is not responsible for configuring Mobile devices or installation/configuration of Mail access on Mobile devices. However the Internet wireless access settings on Mobile device can be assisted by IT dept.
7. Internet access is limited between 10:00am to 6:00pm on weekdays. (Sites those consume bandwidth & Social networking sites are restricted for above mentioned duration. e.g YouTube, Orkut, Facebook etc.)
8. Internet downloads are limited (e.g. 15MB download limit per user per day) to optimize & maintain IT operated services. In case of business requirements, where large downloads are required, employees can request IT dept for larger capacity downloads; the downloaded content can then be provided to the users.
9. To minimize power consumption, IT Dept recommends employees to switch their PCs to standby/hibernate power-saving mode, when left unattended for 30mins.
10. Software licensing is managed by IT dept. Users should not install any software's without approvals from IT dept.
11. Any 'software' required as per business need has to be notified to IT dept, only after approvals (licensing) from IT dept, requisite software's shall be installed by IT dept for users, wherever possible.
12. IT dept is not responsible for training users on installed software's.
13. Any physical damage to the IT assets (e.g. PC – Desktop/Laptop, Mouse, Keyboard, LCD screens, etc) will be accounted to end users. IT is authorized to deduct charges accordingly.
14. Loss or Theft of IT assigned computer (Laptop/ Desktop) - If your computer is lost or stolen, you must notify Information Technology department & Administration department immediately by sending email. Legal documentation/ Police station report shall be provided in case of lost/stolen issues to Administration department. Information Technology department shall also be kept informed.
15. The new mail ID requests will be entertained via HR department (when "New Joinee form" is submitted by HR to IT dept) and few authorized users identified by IT.
16. The mail ID format is standardized and user cannot request for format. The mandatory format for mail ID is "firstname.lastname@company-domain-name.com"

4.2 Security and Proprietary Information

1. The information contained on Intranet/Extranet/Internet-related systems is classified as either confidential or not confidential in the "Acceptable Use Policy – Information Classification document" (recommended to be presented/ signed by employees during joining). Employees should take all necessary steps to prevent unauthorized access to all such business purpose information.
2. With reference to Password policy, User level passwords (end-user PC) should be changed every four months and IT System level passwords (Server software/applications/Server OS) should be changed every quarter by respective owners/functional/operational teams.
   Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
3. IT shall setup PCs, laptops & workstations with a password-protected screensaver with automatic activation feature set to 10mins & Account lockout for 10mins for 3 invalid password attempts. All employees should comply to these settings, in cases where these settings are observed to be missing, employees should contact IT dept to secure their PCs. Whenever the hosts will be left unattended, employees should ensure PC access in locked state [locking too password prompt or logging-off or control-alt-delete for Win2K/XP/7/Linux users].
4. Use encryption/password protection for sensitive information wherever feasible.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised.

6. As a guideline, postings by employees from a Smartlink email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Smartlink, unless posting is in the course of business duties.
7. It is recommended all the computers connecting to Smartlink Networks, used by employee (whether employee owned or Smartlink owned) shall be continually executing approved virus-scanning software (with latest antivirus updates) with prior notification & approval from IT dept on IT Helpdesk.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Smartlink authorized to engage in any activity that is illegal under local, state government or international law while utilizing Smartlink-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are not recommended /prohibited:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Smartlink.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Smartlink or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a Smartlink computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any Smartlink account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to IT Dept is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.

13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, Smartlink employees to parties outside Smartlink.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Smartlink's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Smartlink or connected via Smartlink's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.4. Blogging / Chatting

1. It is recommended to utilize corporate chat/messenger “Microsoft Lync” for internal communication. However as per business requirement other permitted messengers are GTalk, Skype, MSN/Hotmail.
2. Blogging /Chatting by employees, whether using Smartlink’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Smartlink’s systems to engage in Blogging /Chatting is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Smartlink’s policy, is not detrimental to Smartlink’s best interests, and does not interfere with an employee's regular work duties. Blogging /Chatting from Smartlink’s systems are also subject to monitoring.
3. Smartlink’s employees should not reveal any Smartlink confidential or proprietary information, trade secrets or any other material when engaged in Blogging /Chatting**.**
4. Employees shall not engage in any Blogging /Chatting that may harm or tarnish the image, reputation and/or goodwill of Smartlink and/or any of its employees. Smartlink does not recommend employees from making any discriminatory, disparaging, defamatory or harassing comments when Blogging /Chatting.
5. Employees may also not attribute personal statements, opinions or beliefs to Smartlink when engaged in Blogging /Chatting**.** If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Smartlink. Employees assume any and all risk associated with Blogging /Chatting.
6. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Smartlink’s trademarks, logos and any other Smartlink intellectual property may also not be used in connection with any Blogging /Chatting activity

5.0 Enforcement

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

6.0 Definitions

Term	**Definition**
Blogging	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
Chatting	Using online or software based Instant Messengers for text / voice communication.

Spam Unauthorized and/or unsolicited electronic mass mailings.

7.0 Revision History

Version	Date	Author	Remarks
1.0	22nd 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	13th November 2009	Kiran Gole	Document updated.
1.2	13th November 2009	Sandeep S	Approved by Security Committee / Head
1.3	18th October 2010	Kiran Gole	Document updated – 4.1 (6,7,8,9); 4.4 (1)
1.3	19th November 2010	Kiran Gole	Document updated.
1.3	19th November 2010	Shridhar K	Approved by Security Committee / CTO
1.4	16th May 2012	Mayur Gujar	Name & Logo updated.