

		Sharp Business Systems (India) Pvt. Ltd.	SHARP Be Original.
Rev:00	Date:	<u>Policy – Information Technology</u>	

Prepared By:	Checked & Approved By:	Approved By:
		
Deputy Manager - IT	Head- HR & IT	Managing Director

Sharp Business Systems (India) Pvt. Ltd.

Information Technology Policy & Procedure

**3rd Floor, Add India Centre,
Plot No.:9, Sec:125, Noida (UP) – 201301**

		Sharp Business Systems (India) Pvt. Ltd.	SHARP Be Original.
Rev:00	Date:	<u>Policy – Information Technology</u>	

Prepared By:	Checked & Approved By:	Approved By:
		
Deputy Manager - IT	Head- HR & IT	Managing Director

Contents

1	Purpose:	3
2	Scope & Application	3
2.1	Information Technology Resources:	4
2.2	User:	4
2.3	Policy:	4
3	Policy:	4
4	General standards for acceptable use of SBSI Information Technology resources require:	4
5	General Information Technology Usage	4
5.1	Passwords	4
5.2	Access Control	5
5.3	Managing System Privileges.....	6
5.4	Changes to Systems	6
5.5	Security (Access Control)	6
6	Software Licensing	6
7	Internet and Intranet Usage	7
8	Email Usage	7
9	Data Backup	8

		Sharp Business Systems (India) Pvt. Ltd.	SHARP Be Original.
Rev:00	Date:	<u>Policy – Information Technology</u>	

1 Purpose:

To provide a secured IT environment that ensures the usability and availability of IT resources to all users of Sharp Business Systems (India) Pvt. Ltd. (also known as SBSI) is the primary intent of this Policy. The Policy also lays down privacy and usage guidelines for those who access Information Technology of Sharp Business Systems (India) Pvt. Ltd.

SBSI recognizes the vital role of Information Technology in affecting the Company's business as well as the importance of protecting information in all forms. As more and more information is being used and shared in digital formats across different platforms, it becomes imperative to protect the information and the technology resources that support us.

2 Scope & Application

This policy applies to **everyone (Employees/consultants/vendors/suppliers) who has access to SBSI's Information Technology Resources**, and it shall be the responsibility of all the Functional Heads across all locations and the IT team to ensure that the policy is clearly communicated, understood and followed by all users.

Departmental Heads who contract our services shall be responsible to provide the contractor/vendor/supplier with a copy of this Policy before any access is given to them.

The IT policy covers the usage of all Company's Information Technology and communication resources, whether they are owned or leased by the company or are under the company's possession, custody or control, including but not limited to:

- ❖ All computer-related equipment/company's IT assets, including desktop, Laptop, Data-card, iPad, personal computers (PCs), portable PCs, terminals, workstations, PDAs, wireless computing devices, telecom equipment, networks, databases, printers, servers and shared computers and all networks and hardware to which these equipment are connected.
- ❖ All electronic communications equipment including telephones, radio communicators, voice-mail, e-mail, fax machines, PDAs, wired or wireless communications devices and services, Internet and other on-line services.
- ❖ All software including purchased or licensed business software applications, SBSI written applications, employee or vendor/supplier-written applications, computer operating systems, firmware and any other software residing on SBSI owned equipment.
- ❖ All intellectual property and other data stored on SBSI's Information Technology equipment.
- ❖ This policy is also applicable to all users, whether on Company property or otherwise, connected from remote connections via any networked connection or using Company equipment.

Rishi Sethi

		Sharp Business Systems (India) Pvt. Ltd.	SHARP Be Original.
Rev:00	Date:	<u>Policy – Information Technology</u>	

2.1 Information Technology Resources:

It includes, but not limited to, SBSI owned or those used under license or contract or those devices that are not owned by SBSI but intentionally connected to SBSI-owned Information Technology Resources such as computer hardware, printers, fax machines, Data Card, voice-mail, software, e-mail and Internet and intranet access.

2.2 User:

Anyone who has access to SBSI's Information Technology Resources, including but not limited to, all employees, temporary employees, probationers, contractors, vendors and suppliers.

2.3 Policy:

This Policy includes within its purview the following referred Points.

- ❖ The General Information Technology Usage
- ❖ The Software Licensing
- ❖ The Internet and Intranet Usage
- ❖ The E-mail Usage
- ❖ Data Backup

3 Policy:

The use of the SBSI's Information Technology resources in connection with SBSI's business and limited personal use is a privilege but not a right, extended to various users. The privilege carries with it and the responsibility of using the Users of SBSI's Information Technology resources efficiently and responsibly.

By accessing SBSI's Information Technology Resources, the user agrees to comply with this Policy. Users also agree to comply with the applicable laws and all governing contracts and licenses and to refrain from engaging in any activity that would subject SBSI to any liability. SBSI reserves the right to amend these policies and practices at any time without prior notice.

Any action that may expose SBSI to risks of unauthorized access to data, disclosure of information, legal liability or other potential system failure is prohibited and may result in disciplinary action up to and including termination of employment and/or criminal prosecution.

4 General standards for acceptable use of SBSI Information Technology resources require:

- ❖ Responsible behavior with respect to the electronic information environment at all times.
- ❖ Compliance with all applicable laws, regulations and SBSI's policies.
- ❖ Respect for the rights and property of others including intellectual property rights.
- ❖ Behavior consistent with the privacy and integrity of electronic networks, electronic data and information and electronic infrastructure and systems.

5 General Information Technology Usage

5.1 Passwords

- ❖ Individual password security is the responsibility of each user.
(iPAD password to be managed by SBSI IT Team Only).

Priya Sethi

		Sharp Business Systems (India) Pvt. Ltd.	SHARP
Rev:00	Date:	<u>Policy – Information Technology</u>	Be Original.

- ❖ Passwords are an essential component of SBSI's computer and network security systems. To ensure that these systems perform effectively, the users must choose passwords that are difficult to guess. This also means passwords should not be a single word (weak security) found in the dictionary or some other part of speech.
- ❖ Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control systems or in other locations where unauthorized persons might discover them. Passwords must not be written down and left in a place where unauthorized persons might discover them. Immediately upon assignment of the initial password and in all cases of password "reset" situations, the password must be immediately changed by the user to ensure confidentiality of all information.
- ❖ Under no circumstances, a user shall use another user's account or password without proper authorization.
- ❖ Under no circumstances, the user must share his/her password(s) with other user(s), unless the said user has obtained from the concerned Functional Head the necessary approval in this regard. In cases where the password(s) is/are shared in accordance with the above, the user shall be responsible for changing the said password(s) immediately upon the completion of the task for which the password(s) was shared.
- ❖ In cases where no prior approval had been obtained for sharing of password(s) with other user(s), such user shall be completely responsible for all consequences that shall follow in respect of breach of this Policy and SBSI shall initiate appropriate disciplinary proceedings against the said user.

5.2 Access Control

- ❖ All SBSI computers that are either permanently or temporarily connected to the internal computer networks must have a password-based access control system. Regardless of the network connections, all computers handling confidential information must also employ appropriate password-based access control systems.
- ❖ All in-bound connections to SBSI computers from external networks must be protected with an approved password or ID access control system.
- ❖ All access control systems must utilize user-IDs, passwords and privilege restrictions unique to each user. Users are prohibited from logging into any SBSI system anonymously. To prevent unauthorized access all vendor-supplied default passwords must be changed before SBSI's use.
- ❖ Access to the server room is restricted and only authorized-recognized IT staff or someone with due authorization from IT Head is permitted to enter the room.
- ❖ Users shall not make copies of system configuration files (e.g. Passwords, etc) for their own, unauthorized personal use or to provide to other users for unauthorized uses.

5.3 Managing System Privileges

- ❖ Requests for new user-IDs and changes in privileges must be made to the IT Department in prescribed User Right Request Form. Users must clearly state why the changes in privileges are necessary.

Rishi Sethi

Policy – Information Technology

- ❖ In response to feedback from the Human Resources Department, the IT Department will revoke any privileges no longer needed by users. After receiving information from HR / Admin Department all system access privileges will be terminated within 24 hours when a user leaves SBSI.
- ❖ SBSI Management reserves the right to revoke the system privileges of any user at any time. Conduct that interferes with the normal and proper operation of SBSI information systems, which adversely affects the ability of others to use these information systems or which is harmful or offensive to others will not be permitted.

5.4 Changes to Systems

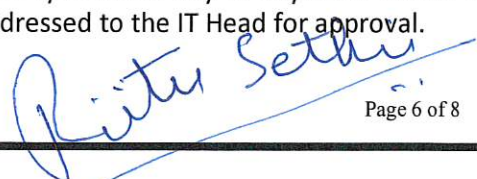
- ❖ No user must physically connect or disconnect any equipment including SBSI-owned computers and printers, to or from any SBSI network except Internet connections (Wi-Fi & LAN)

5.5 Security (Access Control)

- ❖ Users are forbidden from circumventing security measures.
- ❖ Users are strictly prohibited from establishing dial-up connections, using modems or other such apparatus, from within any SBSI's premises.
- ❖ Users who have been given mobile/portable laptop /I-PAD or any other device and duly authorized for such remote access, which connects to SBSI's mail system on a real-time basis, can do so through the Internet.
- ❖ Unless the prior approval of the IT Head has been obtained, users shall not establish Internet or other external network connections that could allow non-authorized users to gain access to SBSI systems and information. These connections include the establishment of multi-computer file systems, Internet web pages & FTP servers.
- ❖ Users must not test or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the IT Head. Incidents involving unapproved system cracking (hacking), password cracking (guessing), file decryption, software copying, computer configuration changing or similar unauthorized attempts to compromise security measures will be considered serious violations of the SBSI policy. Likewise, short-cuts bypassing system security measures is absolutely prohibited.

6 Software Licensing

- ❖ For all software including purchased or licensed business software applications, SBSI written applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on SBSI-owned equipment, all users must comply with the software licensing policy and must not use/install/download any software for their individual use or even for business purpose without prior approval of the IT Head. In case any such software is found on any SBSI system which is not allocated to the individual user, it shall be the responsibility of the user to inform the same to the IT Department. In case the same is not installed by the said user, SBSI shall initiate appropriate disciplinary proceedings against the said user.
- ❖ All necessary software(s) are pre-installed on all SBSI systems for day-to-day office needs. The request for any additional need will have to be addressed to the IT Head for approval.



		Sharp Business Systems (India) Pvt. Ltd.	SHARP Be Original.
Rev:00	Date:	<u>Policy – Information Technology</u>	

- ❖ Use of SBSI network resources to illegally distribute or duplicate unauthorized copyrighted or licensed material is prohibited. Users shall not make unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright.

7 Internet and Intranet Usage

- ❖ Internet software may only be installed / used by or with the approval of the IT Head. Software patches or updates may only be downloaded, subject to approval and ensuring strict adherence to the vendor's security and usage guidelines.
- ❖ Access to the Internet and its resources is provided for the purposes of conducting business on behalf of SBSI. Reasonable personal use of the Internet is permitted, according to constraints and conditions set out by the Sophos Firewall.
- ❖ The IT Department reserves the right to block access to any Internet resource without any prior notice. In case anyone is required access to restricted site, the same may be dealt as special case provided the same is identified as use strictly for official purpose and conducting SBSI business. The approval for the same needs to be obtained by the Department Head from the Management.
- ❖ Similarly, to protect SBSI's IT Systems from imported viruses, downloading or exchanging screensavers, games, entertainment software or other inappropriate files (for example, video or audio materials for personal use), playing games against opponents or gambling over the internet is not permitted.
- ❖ Furthermore, users may not conduct any form of 'hacking' or use malicious code to penetrate or attempt to penetrate other computers or to deliberately release viruses or other harmful programs within either the SBSI network or the Internet or bypass security features.

8 Email Usage

- ❖ All authorized users of SBSI are provided with an E-mail account, which is either individual to the specific user or generic E-mail ID and the same is protected with a password which is provided to the individual user. The use of E-mail should be restricted only for the business purpose. In case any individual is found using E-mail service, which is objectionable by any means, the access can be terminated by IT Department without any prior information. However, the same may be re-instated with the approval from the Managing Director and Functional Head.
- ❖ E-mail users should be aware that exchange of information with external sites may not be secured with high risks of spam, Trojans, malicious codes etc. Hence exchange of information should be limited to reliable sites. Users are prohibited to use their names/E-mail ids/mail domain in public domain without prior authorization from the IT Head.
- ❖ Information must not be transmitted internally or externally which is beyond the bounds of generally accepted standards, values and ethics of the company. This includes, for example, material which could be considered offensive or discriminatory, pornographic or obscene, defamatory or any other material which is otherwise abusive or contains illegal content prohibited by law or regulations of the country or which brings the organization into disrepute. Information is understood to include text & images and is understood to include printed information and sending information via E-mail.

Preeti Sethi

		Sharp Business Systems (India) Pvt. Ltd.	SHARP
Rev:00	Date:	<u>Policy – Information Technology</u>	Be Original.

- ❖ All material contained on the E-mail system belongs to the SBSI and users should consider messages produced/received by them on SBSI account to be secure. The confidentiality of E-mail data should be maintained by the individual user.
- ❖ Security regarding access to the E-mail system is of paramount importance. User identities and personal passwords must not be shared with others. Users should be cautious of providing their email addresses to external parties, especially mailing lists.
- ❖ Users transferring or receiving files or attachments from external sources should note that the SBSI system automatically checks downloaded material for viruses. However, in the event that a virus is suspected, the file or attachment must not be opened and the matter must be reported to the IT Department immediately for inspection and action.
- ❖ SBSI E-mail users are required to use this communication tool in a responsible fashion and to observe the related guidelines. SBSI provides the email system for the purposes of conducting official business and it may not be used for personal gain or business activities unrelated to SBSI's operations. Users must not use the system to promote an external cause without prior permission from the IT Head.
- ❖ In case of a breach of this policy by a user, the services of the user will be terminated without any prior information.

9 Data Backup

- ❖ Company has provided One-Drive access to all the users for keeping their data and users are responsible for the same.

Riiter Sethi