Shilpa Pharma Lifesciences Ltd

IT Usage Policy

IT USAGE POLICY

	Author	Reviewed By	Approved By
Name	Alkesh Kashte	M.P. Naidu	K.H. Hameshaid
Designation	System Administrator	GM- QA	Head operation
Signature	Akashte		
Date	05/01/23	05/01/23	05/01/23

IT USAGE POLICY

Table of Contents

IT USAGE POLICY

1.0 Purpose

The purpose of this policy is to establish the appropriate use of Computing, Telecommunication networks, Computing equipment, and Technology for information security protection for Shilpa Pharma Life Sciences Ltd. These resources are owned/leased/ rented by the company and are provided primarily to enable/ facilitate the official duties and responsibilities of the intended users. This policy sets out the responsibilities and limitations on the use of the Company's computer systems and the intention is to avoid any unauthorized use which may cause damage to the system, loss of data, or criminal/ civil liability for you and the Company.

Shilpa Pharma Life Sciences Ltd.'s intentions for publishing, an IT Accepted Use Policy are not to impose restrictions that are contrary to the organization's established culture of openness, trust, and integrity. The company is committed to protecting its employees, partners, clients, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Hence it is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

2.0 Scope

This policy applies to all associated unit employees, contractors, consultants, trainees, other workers, and who's having access to the systems at Shilpa Pharma Life Sciences Ltd, including all personnel affiliated with third parties.

3.0 Enforcement

All Shilpa Medicare employees and IT resources user(s) need to adhere to this policy. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or contract or agreement as the case may be. Violation of this policy may also invite legal implication/solicitation under applicable law.

4.0 Policy

4.1 General Use and Ownership

4.1.1 All users are responsible for the appropriate use of IT resources per company policies, standards, and guidelines. Company resources must not be used for any illegal or prohibited purpose.

4.1.2 All users are responsible for ensuring the protection of assigned information and information processing facilities

4.1.3 Use of facilities and services for personal and commercial purposes is prohibited.

4.1.4 User must switch off computer system before leaving the office every day (unless required otherwise for official reasons)

4.1.5 Do not send any official data/information to internal/external users for non-business-related purposes/persons. If it is necessary then next-level permission is required from the Management.

4.1.6 Unauthorized data access is strictly prohibited for all users.

4.1.7 Business-critical data should be on the network file server for data protection.

4.1.8 The physical movement of the PC or any other hardware equipment should be done by IT department only.

4.1.8 Any changes to the hardware configuration of the allotted PC/ Laptop are strictly prohibited and any changes noticed must be reported immediately to the IT department.

4.1.9 Printers must be used only for printing necessary documents and use duplex printing (printing on both sides of the paper) for any bulk printing like manuals, e- books except GMP documents, etc.

4.1.10 All workstations, printers, and other desks must be cleared of all redundant and non-usable documents before leaving for the day.

4.1.11 Do not leave your computer's system logged in and unattended for long durations. Ideally whenever you are leaving your PC unattended then either it must be logged off or it must be locked (Ctrl+Alt+Del). Automatic log-off is enabled for 5 minutes.

4.1.12 Providing information about, or lists of, SML employees to parties outside SML is strictly prohibited.

4.1.13 Transportation of Media (USB, Drives) should be done with prior approval from the respective HOD. The user should get the media full scan by the IT dept.

4.1.14 Sharing of information/ data through the mobile device to an unauthorized person is strictly prohibited.

4.1.15 Users are not to carry any official document e.g. Xerox outside of the office premises without prior approval from the management.

4.1.16 The usage of personnel smartphones for data capture by using mobile cameras is strictly prohibited.

4.4.I 7 Authorized mobile phones shall be allowed in office premises as per the P&A approved list.
Note: P&A department shall prepare and circulate the list of approved list of authorized mobile user

4.4.18 P&A shall allow the Mobile and Laptop devices to the visitor with prior approval from Department Head and Unit /Site Head temporarily.

4.2 User Access Management of Domain Controller

4.2.1 The user raises a request to be granted access to any hardware through e-mail, which has to be approved by his/her respective department head and further sent to the IT department for action.

4.2.2 Unique user ids are issued to each user.

4.2.3 Sharing a User ID, and Password is strictly prohibited.

4.2.4 The user is solely responsible for all actions conducted by using that user id. Thus it is expected to take all necessary steps to protect against misuse of user id, which is not limited to periodically changing quality passwords, etc.

Users are precluded from installing, removing, or editing scripts that affect system configuration.

4.2.6 Any unauthorized deliberate action that causes a system to malfunction or disrupts the normal performance of the system and /or the connection terminals is a security violation, irrespective of the system location or time duration.

4.2.7 Users should not make any attempt to gain unauthorized access to restricted files or networks or damage or modify computer equipment or software.

4.2.8 Users will respect the privacy of other users and will refrain from attempting to view or read material being used by others.

4.2.9 Users are responsible for the security of data, accounts, and systems under their control along with the IT Department. (Except for the failure of the hardware itself.)

4.3 E-Security

4.3.1 Change temporary passwords at the first log-on.

4.3.2 Select quality passwords with a minimum of 8 characters which are:

4.3.2.1 Password should be alphanumeric with a special character.

4.3.2.2 Not based on anything somebody else could easily guess or obtain using person-related information, e.g. names, telephone numbers, date of birth, etc.

4.3.2.3 Free of consecutive identical characters

4.3.2.4 Passwords used in 3 previous cases should not be used again.

4.3.2.5 Avoid keeping a paper record of passwords and users should not divulge passwords to other users. Authorized users are responsible for the security of their passwords.

4.3.2.6 Change passwords at regular intervals maximum password age is 30 Days and also do it whenever there is any indication of possible system or password compromise.

4.3.2.7 Don't include passwords in the automated log-on process, e.g. stored in a macro or function key

4.3.2.8 The user account will be locked out automatically after 5 wrong password attempts.

4.3.2.9 To enhance security password complexity has been enabled.

4.3.2.10 The password should not contain the information of your name.

4.3.3 IT Department should keep auto scanning enabled for all the systems.

4.3.4 Port scanning or security scanning is strictly prohibited

4.3.5 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 is prohibited.

4.3.6 Personal chatting on the internet is strictly prohibited. In special cases, where chatting with the external client is required, authorization should be taken from the

4.3.7 Access to a USB mass drive is strictly prohibited.

4.3.8 Access to a USB mass drive shall be provided in special cases after the senior management approves over the mail.

4.3.9 Temporary approved USB access shall be revoked after completion of user activity or within 24 hours

4.3.10 Authorized CD media, data cards, and USB, where required, should be scanned and cleaned before use.

4.3.11 The Company's computer network must not be used to disseminate, view, or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, self-replicating programs, etc.), illegal material, pornographic text or images, or any other unauthorized materials.

4.3.12 The user is responsible for the security and appropriate use of the company's network resources under their control. Using company resources for the following is strictly prohibited:

4.3.12.1 Causing a security breach to network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniffing network traffic.

4.3.12.2 Transmitting on or through any of our services, any material and/or message that is illegal, false, obscene, threatening, sexual or obscene, defamatory, offensive, abusive, hateful, or encourages conduct that could constitute a criminal offense, give rise to civil liability, or otherwise violate any local, national or international law.

4.3.12.3 Indulging in any illegal activity and/or crime such as breach of confidentiality and leakage of data, video voyeurism, e-commerce frauds like phishing, identity theft, etc.

4.3.13 USB access is kept open only for the dedicated system with reading or download access to the images from the camera.

4.4 IT/ Software Compliances

4.4.1 Downloading and installing any unauthorized software or mobile app extension on the company Computer *I* Laptop without prior approval from the IT department /Site Head. This includes software like MS Office, VB, Screensavers, Games (except for default games loaded with the windows operating system), etc.

4.4.2 Use of pirated software is prohibited on any computer system of the company and also the media containing such software should not be brought into the organization's premises.

4.4.3 Downloading software from the Internet without prior IT permission is prohibited.
Employees are prohibited from bringing software from outside and installing it into the computer system or Laptop.

4.4.5 Approved inventory for Hardware/Software/Licenses shall be maintained at each respective site.

4.4.6 The system owner i.e. user, site IT Administrator, and Site Head shall be accountable for the installed software on each computer system.

4.4.7 The internal audit shall be performed for the License and software usage at each respective site and the report shall be shared with Senior Management.

4.5 E-Mail

4.5.1 When communicating on the official email system, the utmost care has to be taken as well as high professional standards must be followed because you are representing the organization while sending or replying to an official mail id.

4.5.2 No personal email id must be used to interact for official reasons with (including but not limited to) vendors, customers, service providers, or partners. Only an official email id must be used to do any official email correspondence.

4.5.3 Personnel use of official e-mail id is strictly prohibited.

4.5.4 The best effort must be made to restrict the size of the email to a minimum. Tools like WinRAR must be used to reduce the size of email attachments.

4.5.5 Employees must use extreme caution when opening e-mails and specifically attachments received from unknown senders, which may contain viruses, worms, or Trojan horse code.

4.5.6 Sensitive attachment types like PIF & SCR (more extensions might be added from time to time) are blocked at the gateway level, hence no mail must be sent with these extensions.

4.5.7 Forging email headers is prohibited. Similarly sending emails from someone else PC without the prior approval of that user is not allowed.

4.5.8 Company policy strictly prohibits creating, circulating, distributing, storing, and/or downloading (internally or externally) any:

4.4.8.1 Chain letters, Religious, political, or business solicitations that do not relate to your duties as an employee of the Company

4.4.8.2 Any files (including games, screen savers, .jpg or .wav or .mp3 or .scr or .bin or .zip files or other software and shareware) which are not Business related.

4.5.9 All the time users are responsible for the professional, ethical and lawful use of email and other network systems

4.5.10 Named e-mail id shall be provided to Assistant Manager and the above category. In case of any exception then prior approval has to be taken from the reporting manager and Management

4.6 Internet

4.6.1 Different level of Internet access is provided to employees depending on the job's responsibility and other parameters. Using someone else password to gain a different level of access is prohibited and users must stick to the level of access allowed to them.

4.6.2 Internet will not be used for illegal activity, to access illegal materials, or to access/publish materials that are obscene /pornographic/ sexually explicit material.

4.6.3 No online storage accounts like yahoo or another briefcase must be accessed to store official or personal information.

4.6.4 Use of an Internet Proxy Server other than that provided by the company is prohibited.

4.6.5 Use of personal external devices, such as Internet Data Cards/USB, to establish Internet or external connection(s) is strictly prohibited.

4.7 Remote/ Teleworking

4.7.1 Listed below are the security measures, which should be taken when working from home or offsite.

4.7.2 The local Administrator password for the laptop user should be assigned by the IT administrator (do not keep the password blank) to avoid unauthorized access to admin share like C$ on the network.

4.7.3 Treat company property and data as you would in the office, according to company information security procedures.

4.7.4 IT administrator is to ensure that adequate and up-to-date virus protection software is installed on the official Laptop / Desktop. Also same applies to any personal computer being used to connect to the official network.

4.7.5 Do not allow a laptop issued for business purposes to be used by family or friends.

4.7.6 Specifically, protect all sensitive business documents stored on laptops by using password protection.

4.7.7 Use a password- protected screensaver to lock it during the period of inactivity.

4.7.8 Where appropriate use a BIOS password to restrict authorized users only to starting the system.

4.7.9 Tum your system off when it is not being used. If the Laptop is to be used frequently then even hibernate can be done, to ensure faster boot-up time.

4.8 Laptop Usage

4.8.1 Backup of business-critical data shall be taken by IT Administrator while working **at the** office or traveling.
Note: The user has to give advance intimation to the IT department to take the data back

4.8.2 Protect individual files from unauthorized access by password protection.

4.8.3 Regularly update the virus scan definitions.

4.8.4 Tum off or shut down the laptop, ensure that all lights are out, all external cables are unplugged, and no removable media is inside then place it in the laptop case.

4.8.5 Never check in a laptop as luggage.

4.8.6 Always carry software authorization and virus certificates from IT while traveling overseas.

4.8.7 If the laptop is lost or stolen, it should be reported immediately to IT and necessary action to be initiated like FIR or so.

4.8.8 Do not place heavy objects on the laptop. Handle the laptop with care.

4.8.9 Do not have liquids or other eatables near a laptop to prevent damage from spilling or dropping.

4.8.10 Do not hit or push the screen display of a laptop to its extremes.

4.8.11 Do not move the laptop when it is running and do not remove the power connector by pulling out the cord, rather grasp the plug itself when removing.

4.8.12 Do not expose the laptop to extreme temperatures. Extreme cold can cause the screen to crack and condensation to form when returning to a warm room. Extreme heat can melt important components of the laptop. Laptops should also be kept away from other sources of heat such as radiators.

4.8.13 Ensure that laptops are kept secure at all times.

4.8.14 The company shall issue laptops to the employee based on their work profile and not necessarily based on seniority. IT department shall ensure that such laptops shall be loaded with all required security software at the time of handing over the laptop to the employee.

4.8.15 Laptops shall be issued to employees based on mail confirmation from the site head and shall be approved by Management.

4.8.16 The laptop shall be retrieved from the employee after their resignation as per the HR Policy.

5.0 Privacy

Shilpa Pharma Life Sciences Ltd has full respect for individual privacy and rights. However, users should not have any expectation of privacy in respect of their usage of company IT resources. The Company's IT resources are the backbone for running the organization's business and nothing must be done to compromise this in any way even if this is unintentional. Please note that the Company may/will monitor or keep a record of communications (at any time with or without notice) either directly or via an external agency and/or record your use of the IT Resources to (including, but not limited to):

5.1 To detect/investigate any unwanted elements like viruses etc. which might be destructive

5.2 Detect and/or prevent crime

5.3 Ascertain and/or demonstrate whether you and/or the Company are complying with the Company's rules and policies (including, but not limited to, this policy) and also with legal and/or regulatory obligations which you and/or are subject to Company

Ascertain whether communications are relevant to the Company's Business the Company while conducting such monitoring activities, will use all reasonable.

endeavors to comply with regulatory guidelines and to respect your privacy and that of third parties using the IT Resources.

6.0 Acceptance

All users further agree, acknowledge and confirm that:

5.5 The company reserves the right to revise, amend, or modify this policy at any time and in any manner. However, a notice of any revision, amendment, or modification will be notified to all Shilpa personnel via email.

5.6 Reading and practicing any future release(s) of this policy, periodically, is solely the user's responsibility; however, understanding of any part of this policy shall be provided on written request to the quality assurance department.

5.7 The provision(s) and obligation(s) of this policy, and its future release(s), shall apply and continue in effect for a period of their employment from the date hereof.

7.0 Classification of Information / Data

All the information and data must be classified according to an appropriate level of Confidentiality, Integrity, and Availability.

5.8 Classifying The Information.

The information shall be classified into one of the following categories:

Sensitive / Restricted: This classification applies to strategic business information, which is most critical and intended strictly for use within a closed group of Shilpa Pharma Life Sciences Ltd. Any unauthorized disclosure could seriously and adversely impact Shilpa Medicare and its stakeholders, business partners, and customers leading to legal and financial repercussions and adverse public opinion (Example: business plans, trade secrets, information security data customer data, pricing strategy, etc.).

Confidential: This classification applies to less sensitive business information, which is intended for use within the Shilpa Pharma Life Sciences Ltd group. Its unauthorized disclosure could adversely impact Shilpa Medicare employees, customers, stakeholders, and business partners (For example employee performance evaluation, CTC details, internal audit report, marketing plans, analysis of competitive products/services, etc.).

Internal Use: This classification applies to all other information, which is supposed to be shared only within Shilpa Pharma Life Sciences Ltd which does not fit into the above categories. Its unauthorized disclosure against the policy is not expected to have a serious or adverse impact on Shilpa Medicare employees, customers, stakeholders, and business partners (Example: information posted related to employee usage, HR policies, administrative circulars, training materials, manuals, etc.).

Public: This classification applies to information, which has been explicitly approved by Shilpa Medicare management for release to the public and disseminated without potential harm (Example: information posted on internet portals, product brochures, advertisements, job opening announcements, published press releases, etc.).

8.0 Ownership of the Information.

All critical applications and information shall have designated owners. The files created by individuals shall be owned and classified by them. The data owners shall also define access rules and retention periods. IT department takes responsibility for the security of the information/data based on the definition provided by the owner.

9.0 e-Waste Management:

IT assets (including but not limited to desktops, Laptops, servers, projectors, printers, etc) shall be disposed of safely when the asset is obsolete either by usability or age. Such identified assets shall be disposed of through authorized/certified e-waste partners. The information of disposed of assets shall be informed to Finance/Account for necessary treatment in books. The "Certificate of e-waste recycling" shall be documented for reference.

The provision hereof shall be governed and construed by Shilpa Pharma Life Sciences Ltd, and by your acceptance hereof you agree that you have understood this policy to your satisfaction. Please indicate your acceptance of the above by signing and returning the enclosed copy of this policy.

Name:
Employee ID:
Signature with Date: