Policy for

INFORMATION TECHNOLOGY (IT)
SIDDHARTH UNIVERSITY, KAPILVASTU

SIDDHARTH UNIVERSITY, KAPILVASTU,
SIDDHARTHNAGAR, UTTAR PRADESH, 272202

Information Technology (IT) Policy
(Manual of Procedures, Regulations & Guidelines)

1. Introduction

1.1. Information Technology (IT) Policy is required for Smooth & Secure running of All the Computers and Data related Business and Functions. This IT Policy intends the same within the Siddharth University.

1.2. Information Technology (IT) Policy provides the policies, procedures, regulations and guidelines for selection and use of Information Technology (infrastructure and system) within the workflow which must be followed by all Users (#5). It also provides guidelines Siddharth University will use to administer these policies, with the correct procedure to follow.

1.3. Siddharth University will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures. (#8) Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.

2. Objectives

2.1. This policy provides guidelines for the purchase of hardware for the business to ensure that all hardware technology for the business is appropriate, value for money, and where applicable, integrates with other technology for the business.

2.2. The objective of the IT Policy is to devise, catalyze, support and sustain IT and IT enabled activities and processes in order to improve access, quality and efficiency in the education system of the University.

2.3. The IT Policy aims at preparing adult learners to participate creatively in the establishment, sustenance and growth of a knowledge society leading to all round socio- economic development of the nation and global competitiveness.

3. IT Principles

Certain core principles have been identified which should work as meta-paradigm in formulation of IT policy. These are:

3.1. Confidentiality and Integrity Principles: Only authorized individuals have access to information - reliable and accurate – and the same must be available when needed.

3.2. Accountability, Awareness and Ethics Principles: Accountability and responsibility for the security and privacy of information must be clearly defined and acknowledged; the users must be aware of principles, standards, conventions, or mechanisms for maintaining the security and privacy of information; and the same is to be used ethically.

3.3. Multidisciplinary, Proportionality and Integration Principles: Security and privacy governance must address the considerations and viewpoints of all interested parties; safeguards are to be proportionate to the risks and design and implementations are to be coordinated and integrated within the system of safeguards and the life of the information asset.

3.4. Timeliness, Assessment Principles: Parties will act in a timely and coordinated manner; Risks to information are to be assessed initially, and reassessed periodically.

3.5. Equity Principle: The rights and dignity of individuals are to be respected while carrying out security and privacy goals.

3.6. Notice Principle: Informs the individual about privacy policies and procedures and identifies the purposes for which the individual's information is collected, used, disclosed and retained.

3.7. Choice & Consent Principle: Obtains implicit or explicit consent from the individual with respect to the collection, use, disclosure, and retention of the individual's information, particularly if that information is to be used for a secondary purpose or disclosed to a third party.

3.8. Collection Limitation Principle: Collects only the information needed to achieve the purposes identified by the business unit in support of the university's mission, and as outlined in the notice.

3.9. Use & Retention Principle: Uses the individual's information only as outlined in the notice, and keeps the information only as long as necessary to fulfil the stated purposes.

3.10. Disclosure Limitation Principle: Discloses the information to third parties only as outlined in the notice and as consented to by the individual, either implicitly or explicitly.

3.11. Access Principle: Provides access to the individual to review and update or correct his or her information.

3.12. Monitoring & Enforcement Principle: Monitors compliance and has procedures to address complaints and disputes.

4. IT Resources

4.1. IT infrastructure of the Siddharth University is made up of all the usual hardware and software components: facilities, data centre, servers, networking hardware desktop computers and enterprise application software solutions.

4.2. IT Resources include all the IT infrastructure as well as full range of specialized staff and personnel who are responsible for the proper functioning of the Information technology related all the business of the University.

5. Scope of the policy

5.1. A **User**: is an individual using IT infrastructure/system of the University. This includes – All the Administrative/management staff, Faculty members, Guest faculty members, Research fellows, Students, Invited guests and other individuals visiting university.

5.2. **Primary user:** is an individual in whose room/chamber/assigned office space the computer system is installed and is primarily used by him/her shall be considered the ‘primary’ user.

5.3. If a computer system has multiple users, and none of them is considered to be the 'primary' user, in that case, the Head/In-charge of the concerned department/facility should make due arrangements to make a person responsible for compliance and the same would be considered 'primary' user.

5.4. All such aforesaid users SHALL be required to abide to this policy and to sign an undertaking placed as Annexure – I, at the end of this document.

6. The IT Cell

6.1. The University shall constitute an IT Cell per requirements of this policy and to enforce and disseminate this policy.

6.2. The competent authority shall decide the constitution of the Cell. The cell shall be headed by the HoD/Professor of the relevant department of the University.

6.3. The members of the IT Cell shall be nominated by the Head of the cell and the competent authority may approve accordingly.

6.4. The IT Cell shall:

6.4.1. Review and approve plans for major IT projects and decisions.

6.4.2. Prepare the Annual IT Budget of the institution and place it for approval before the Principal and Management to ensure that baby steps are taken towards technology advancements.

6.4.3. Plan at the end of each academic year for the upgradation of IT infrastructure for the next academic year, to support evolving requirements of the learner and educator communities of the institution.

6.4.4. Progress action plans to respond quickly and appropriately to IT maintenance issues and difficulties.

6.4.5. Administer all IT related work and conduct annual stock taking of IT hardware and assets used for academic and administrative purpose.

6.4.6. Educate all teaching staff, non-teaching staff and students on the importance of sensitive and purposeful usage of computers and other IT related equipment on campus. Conduct frequent awareness drives for the same.

6.4.7. Do regular checks of the computer stock registers maintained in all the department/laboratories/facilities.

7. The Policies

7.1. Hardware, Software and Peripherals

7.1.1. Procurement/Purchase

7.1.1.1. The purchase of all business desktops, laptops, mobile devices, servers, network, and computer peripherals must adhere to this policy. All computer hardware, software, and mobile device related purchases MUST be approved by or done through IT Cell. (#6)

7.1.1.2. Approved requisitions shall be deemed to be justified even in case further purchase procedure may find it not feasible.

7.1.1.3. IT Cell may formulate basic standard requirements for the Hardware along with basic minimum specifications (also categorically for the specific purpose of the Hardware use).

7.1.1.4. This policy provides guidelines for the purchase of software for the University to ensure that all software used by the University is appropriate, value for money, and where applicable, integrates with other technology for the business. This policy applies to software obtained as part of hardware bundle or pre-loaded software.

7.1.1.5. All software, including types of non-commercial software such as open source, freeware, etc. here must be approved by the IT Cell prior to the use or download of such software. The Cell may provide list of such software and upgrade the same time-to-time.

7.1.2. Open source software

7.1.2.1. This policy intends to encourage the use of Open source Software within the University's IT Framework.

7.1.2.2. Provided that the business as usual does not get hampered or quality of performance compromised, the University shall attempt to encourage all the users to shift to Open Source Software in place of commercial software (even if they are part of the hardware bundle or pre-loaded software).

7.1.2.3. In the event that open source is required, approval from the IT Cell must be obtained prior to the download or use of such software.

7.1.2.4. All open source software must be compatible with the business's hardware and software systems.

7.1.2.5. Any change from the above requirements must be authorised by the IT Cell or competent authority which may enlist the software and keep such list up-to-date.

7.2. IT Resource Management

7.2.1. Management and operation of IT resource is the responsibility of concerned head of respective subdivision to which that IT resource belongs. In Siddharth University, it could be the Dean, Head of Department, Coordinator of School, Principal Investigator, Coordinator of certain facility or any other competent authority with whom such IT resource has been associated. Compliance of the Institute's Computer Assets and IT (usage) Policy shall be the sole responsibility of the aforesaid officials for the IT resources of their concern. For convenience, aforesaid officials may designate another person to manage and operate respective IT resource (designated as "system administrator") but responsibility for policy compliance on respective IT resources shall still remain with the concerned official only.

7.2.2. The system administrator will manage and operate IT resources as per the policies of the Institute and of the concerned sub-division. He/ she will also refer to the Information Security Office, any matter, which is beyond maintenance and operation of such IT resource.

7.2.3. System Administrator should:

7.2.3.1. Educate users regarding various nuances of Institute's Computer Assets and IT (usage) policy and other prevailing national and international policies and developments.

7.2.3.2. Help users implement and comply with the Institute policies and help users execute and maintain faithfully all licenses on their IT resource.

7.2.3.3. Secure and protect IT resources by taking befitting actions.

7.2.3.4. Prevent and protect IT resources from damage or theft.

7.2.3.5. Coordinate with the Chief Information Security Officer to seek recommendations and guidelines for implementation, and to find and correct problems associated with the systems and network under their control.

7.3. Acceptable use

7.3.1. An acceptable use policy outlines what an organization determines as acceptable use of its assets and data, and even behaviour as it relates to, affects, and reflects the organization.

7.3.2. Such a policy provides a baseline that all users must follow as part of their employment/admission.

7.3.3. By providing end users with guidance for what to do and limitations on how to do things, an organization reduces risk by way of the user's actions.

7.3.4. The University prohibits use of its IT resources for any commercial purpose except when permitted by appropriate authority.

7.3.5. The University may encourage participation of users in Open source knowledge development with the consideration that any such activity does not interfere with/compromise the primary academic/administrative/management business of the University. In that case, use of the University IT resources for such Open knowledge activities may be deemed to be justifiable to the extent they do not hamper the routine business.

7.3.6. General Guidelines

7.3.6.1. Administrative/management staff, Faculty members, Guest faculty members, Research fellows, Students, Invited guests and other individuals visiting university are authorized to use the IT infrastructure of the university – for academic, official university business, and personal purposes – as long as they do not violate any Law (Indian and/or International) and University policies.

7.3.6.2. Any contribution towards the destruction or distortion of congenial academic or work environment is prohibited and shall be considered violation of this policy, in general. No user should attempt to vandalize, damage, or change any data inappropriately, whether by accident or deliberately.

7.3.6.3. Gaining or enabling unauthorized access to forbidden IT resource of the University is totally prohibited. The basic notion of trustworthiness of information resources must be preserved by all of its users. Any interference, disruption or encroachment in the University IT resources shall be a clear violation of this policy.

7.3.6.4. Sending, viewing or downloading fraudulent, harassing, obscene, threatening, or other messages or material that are a violation of applicable laws (Indian and/or International) or University policy, are prohibited. Therefore, user's inhibitive discretion is solicited where category of certain content could be doubtful.

7.3.6.5. Users must respect IPR and copyright law(s), and licensing policies. Any unlawful file- sharing, use of any form of illegal or pirated or un-licensed software, on the University's IT resources (including individually owned IT resources being used under Institutional IT privileges) shall constitute a violation of this policy.

7.3.6.6. Users are expected to take proper care of equipment, and are expected to report any malfunction to the staff on duty or to the in-charge of the facility. Users should not attempt to move, repair, reconfigure, modify, or attach unauthorized external devices to the systems.

7.3.6.7. Laboratories/facilities using IT resources of the University should formulate and disseminate their own detailed manuals/guidelines within the framework of, and in accordance with, this policy to better orient their best practices and ensure the abidance to the policy within their perimeter and in their functions.

7.4. Personal Devices

7.4.1. The University does not require or recommend use of individually owned IT resources to conduct institutional tasks. However, individual units may allow its users to use such IT resource within the unit only and any such user may choose to use his/her own IT resources and abide by respective terms and conditions.

7.4.2. Employees/students/guests using Personal devices and related software to connect to technology infrastructure of the University will, without exception, use secure remote access procedures.

7.4.3. The University reserves the right to require students and employees to shut down any form of personally owned technology that has been identified to cause interference with the proper functioning of the University wireless/Wi-Fi network.

7.4.4. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain University data.

7.4.5. If a user accesses University related data on his/her personal device, the user shall be required to follow all enterprise-sanctioned data removal (sanitisation) procedures to permanently erase University-specific data from such devices once their use is no longer required.

7.4.6. Following the Data classification and security concerns, the head/in-charge of the department/facility may enact and enforce rules/regulations for the attachment, data transfer and communication with the University IT infrastructure, of individually owned devices.

7.5. Electronic communication policy

7.5.1. The purpose of this policy is to identify electronic communication as an official means of communication within The Siddharth University and to define the responsibilities of students, faculty and staff related to electronic communication.

7.5.2. In an effort to increase the authorized/authentic/efficient distribution of critical information to all faculties, staff and students, and the University's administrators, it is recommended to utilize the university's e-mail services for formal University communication and for academic & other official purposes.

7.5.3. All other electronic means i.e. IRC's, WhatsApp Groups, other kind of electronic communication user groups, Social media platforms etc. may be used as additional/supplementary means (solely for the ease) of communication. However, any communication made on such subsidiary/alternative channels may not be considered formal/authentic/official and the same is discouraged by this policy.

7.5.4. Formal University communications are official notices from the University to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general University messages, official announcements, etc.

7.5.5. This University email service shall be the official electronic communication channel and all users are expected to use their official email for any official/business correspondence. Users may however relay (forward) communications from their official email accounts to their personal email but Siddharth University network services does not guarantee the reliability of this relay.

7.5.6. Shared email accounts are not allowed. In exceptional cases, where such accounts are required (such as those for specific events such as the Science Conclave or other conferences), they will be created with a SINGLE designated faculty/officer user. However, in case of any unwanted, objectionable or harassing content being distributed using a shared email account, the principal account holder will be held liable.

7.5.7. User of such official University e-mail ID should be aware that by using this they abide to the following:

7.5.7.1. The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.

7.5.7.2. Using the facility for illegal/commercial purposes is a direct violation of this policy and the facility may be withdrawn. Such inappropriate activities include, but not limited to, unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages; generation of threatening, harassing, abusive, obscene or fraudulent messages/images.

7.5.7.3. User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, user should get confirmation from the sender about its authenticity before opening it.

7.5.7.4. User must not share password of this mail ID to anyone in any case. Must create strong password and frequently change the same to ensure maximum security.

7.5.8 Social media can be defined as any web or mobile based platform that enables an individual or agency to communicate interactively and enables exchange of user generated content. These generally include – Social networking sites, microblogging sites, blogs, video sharing platforms and wikis.

7.5.8.1 The University may maintain its presence over social media for the sake of Enhanced Outreach, Real Time engagement, Individual Interaction Managing Perceptions.

7.5.8.2 Only authorised individuals should engage in social media presence/activities on behalf of the University/departments/facilities.

7.5.8.3 Individuals, even in their personal capacity, should abide to certain things and be aware that their views/activities may be associated with the University even if they clearly state their actions are performed in personal capacity.

7.5.8.4 All the Users (#5) should abide to certain best practices. They should: clearly disclose their identity and role, not comment and respond unless authorized to do so, Be Polite, Be Discrete and Be Respectful to all and do not make personal comments for or against any individuals or agencies, professional discussions should not be politicized, Be open to comments, Be compliant to relevant rules and regulations, and maintain privacy; Do not reveal personal information about other individuals as well as do not publish their own private and personal details unless they wish for them to be made public to be used by others.

7.5.8.5 Social media use shouldn't interfere with employee's responsibilities at the University.

7.6. Data Classification and Database management

7.6.1. Data classification and database management policy ensures guidance on how to make informed risk decisions when transacting, sharing, and using sensitive data.

7.6.2. To provide that, security and risk management authorities would benefit from the creation of a data classification policy and accompanying standards or guidelines.

7.7. Network policy

7.7.1. Network Infrastructure Liability: The University holds responsibility of managing and protecting the University network(s) against electronic forms of attack or abuse. It is the sole prerogative of the Institute to terminate network connections to computers within its domain due to suspected or actual abuse of the network and/or its components.

7.7.2. Termination of Connection to an Offending Computer: The network connection to an offending computer may be terminated by disabling the port of that particular switch which connects the offending computer to communicate with the Internet

and further traffic to and from that computer will be stopped. Local applications on the computer, however, will remain unaffected after such termination.

7.7.3. Terminating a Connection with warning: Depending upon the urgency of taking preventing action(s), concerned Users will be informed regarding their machines which are causing disturbances and an action from the user end will be solicited within a specified time-frame beyond which action can be taken from the System Administrator's side.

7.7.4. Any attempt to bypass the security and authentication measures by way of obfuscation, flooding etc., or use of unauthorized VPN services is absolutely not allowed. Users found in violation will have their network access privileges revoked immediately, along with further administrative action.

7.8. Website policy

7.8.1. The university website is an online gateway to the various kinds of Information, and channel/portal/medium to the various administrative/management/academic functions. It, being an IT resource and functioning system, comes under this policy. However, the IT Cell or the competent authority may devise and enforce a separate Website Policy within the framework of this policy.

7.8.2. It is recommended by this policy that the University website should be designed and developed in such a way to make it user friendly and easy to navigate through, up to the maximum possibilities.

7.8.3. To ensure the maximum possible user friendliness and usability, it is advised that the website interface and information displayed on/delivered through the website should be bilingual i.e. in English primarily and in Hindi wherever possible.

7.8.4. The Hindi version of such website content shall use easily comprehensible terminology, i.e. common terms of English or other foreign origin shall be used in *Devanagari* script if they are widely used and understood by the common Hindi speakers. Comprehensibility is paramount, nothing else.

7.8.5. Website should be designed with special considerations in order to ensure the maximum possible user friendliness to visually challenged users. It is advised that the links to some open source/freeware screen readers may be provided on the main page of the website.

7.8.6. There shall be a Website updating and monitoring team, constituted by the competent authority to help the IT department (i.e. coding cell) to keep website up-to-date and to suggest means to better design and functioning.

7.8.7. For the security purposes, it is advised to have minimum possible personnel involved in actual updation (those having access to password and the updation mechanism).

7.8.8. Subdomains may be created to separate/classify different areas/departments/facilities and functions. However, they shall be kept minimal as security related risk may increase with an increased number of them. Subdomain policy (within Website policy or separate) may be devised within the framework of this policy.

7.8.9. Security issues and considerations shall have precedence over the ease of updation and design considerations.

7.9. Security policy

7.9.1. Security concerns are of paramount importance and shall be dealt according the core principles mentioned in section #3.

7.9.2. Proper data classification, access limitations and password protection shall be applied.

7.9.3. Users shall create strong passwords, must not share their own created or provided passwords in any case (unless multiple users are authorised by the competent authority).

7.9.4. All the remote access to the University IT resources shall be protected by firewall.

7.9.5. Further security measures can be taken by the head/in-charge of the facility/department/division with appropriate discretion.

7.9.6. Separate IT Security policy can be devised within the framework of this policy.

7.10. Incident Response

7.10.1. How should our organization respond to an incident such as a data breach, hack, malware attack, or other activity that presents risk? The answer could mean the difference between experiencing a minor event and suffering a catastrophic blow to the functioning of the University IT system.

7.10.2. It SHALL be the duty of users to report policy violation(s) before appropriate authority or a concerned official, especially when issues are related with accounts, system security, or when they have information about unlawful or suspected abuse of IT resources, through e-mail or in person, during normal office hours.

8. Upgradation & Revision

8.1. This very policy – i.e. "IT Policy (Manual of Procedures, Regulations & Guidelines)" – shall be subject to revision by the IT Cell and/or any competent authority to ensure it being state-of-the-art in order to address situations/incidents and proper functioning of the IT Resources and established System.

8.2. The IT Cell shall be responsible for, time-to-time, inviting the expression of concerns/issues/incidents faced and suggestions to maintain this policy up-to-date.

8.3. The competent authority shall have power to summon/convene meeting of the IT Cell with due procedure to revise and upgrade this policy per need.

8.4. In case of any difficulty in implementing this policy, the competent authority can take appropriate decision to remove the same.

8.5. Any changes per Upgradation/revision in policy will take effect immediately after a brief announcement by any means, e-mail, printed notices, or through the news groups.

9. Dissemination & Enforcement

9.1. For **dissemination**, following measures shall be adopted:

9.1.1. Disclosure of this policy on the university website shall be mandatory.

9.1.2. Orientation sessions at the time of joining of employees/staff/faculty and admission of students to the university should be carried out to ensure their familiarity with this policy.

9.1.3. A due undertaking (Annexure – I) shall be taken by the employees/staff/faculty at the time of joining.

9.2. In general, the **enforcement** of this policy is a collective responsibility of all the stakeholders (#5) – i.e. all the users are expected not just only to abide to this policy but also ensure, as a best practice, that the other users also abide to the same. For this, users may help each-other to better understand the policy provisions and in case of its breach it shall be their duty to report the incident to the appropriate authority, if any such breach comes to the knowledge of the user.

9.3. Within the administrative and academic and associated domains, it shall be responsibility of the department/division/facility head/in-charge/responsible individual to ensure the enforcement of this policy within that particular domain.

9.4. **Violations** of this policy will be treated as academic misconduct, misdemeanour, or indiscipline as appropriate/applicable and depending upon the nature and graveness of the violation may attract disciplinary/punitive action from the competent authority or even legal action if applicable.

Annexure - I

I, ... , Employee ID/ Enrolment No:..... ,

do hereby declare that as an employee / student in Siddharth University, have carefully read and understand the provisions of the IT policy and will abide by the same. I accept that any act of mine that can be considered to be the violation of the policy will be dealt with as mentioned in section #9.4.

Date: Signature: