IT Policy

1. Introduction

Panjab University (PU) provides IT resources to support the educational, instructional, research, and administrative activities of the University and to enhance the efficiency and productivity of the faculty, staff and students. These resources are meant to be used as tools to access and process information related to their areas of work. These resources help them to remain well informed and carry out their functions in an efficient and effective manner.

2. Scope

This policy establishes University-wide strategies and responsibilities for governing the usage of IT resources from an end user's perspective and is applicable to all the users of computing resources owned or managed by University. Individuals covered by the policy include (but are not limited to) faculty and visiting faculty, staff, students, alumni, guests, departments, offices, affiliated colleges and any other entity which fall under the management of Panjab University accessing network services via PU's computing facilities. For the purpose of this policy, the term 'IT Resources' includes all university owned, licensed, or managed hardware and software, and use of the university network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network. Misuse of these resources can result in unwanted risk and liabilities for the University. It is, therefore, expected that these resources are used judiciously and in a lawful and ethical way. Use of resources provided by PU implies the user's agreement to be governed by this policy.

3. Objectives:

The objectives of this policy are:

- To ensure proper access to and usage of PU's IT resources and prevent their misuse by the users.
- To maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the University on the campus.
- To protect the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the University.

4. General Rules and Responsibilities

4.1 Computer Centre shall be the primary agency to implement appropriate controls to ensure compliance with this policy by their users and shall provide necessary support in this regard.

4.2 Computer Centre shall ensure resolution of all incidents related to the security aspects of this policy by their users and shall provide the requisite support in this regard.

4.3 All the users shall use PU's IT resources for those activities that are consistent with the academic, research andpublic service mission of the University and are not "Prohibited Activities".

4.4 All the users shall comply to existing national, state and other applicable laws.

4.5 All the users shall abide by existing telecommunications and networking laws and regulations.

4.6 All the users shall follow copyright laws regarding protected commercial software.

4.7 The users of PU shall not install any network/security device on the network without requisite permission.

4.8 It is responsibility of the users to know the regulations and policies of theUniversity that apply to appropriate use of the University's technologies and resources.

4.9 As a representative of the PU community, each individual is expected to respect and uphold the University's good name and reputation in activities related to use of ICT communications within and outside the university.

4.10 Competent Authority of PU should ensure proper dissemination of this policy.

4.11 An authorized user may use only the IT resources he/she has authorization.

4.12 No user should use another individual's account or attempt to capture or guess other users' passwords.

4.13 A user is individually responsible for appropriate use of all resources assigned to him/her, including the computer, the network address or port, software and hardware. Therefore, he/she is accountable to the University for the use of such resources. As an authorized user, he/she should not engage in or enable unauthorized users to access the network by using IT resources of PU or a personal computer that is connected to the PU campus wide Local Area Network (LAN).

4.14 The university is bound by its End User License Agreement (EULA), respecting certain third-party resources; a user is expected to comply with all such agreements when using such resources.

4.15 Users should make reasonable efforts to protect their passwords and to secure resources against unauthorized use or access.

4.16 No user should attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.

4.17 Users must comply with the policies and guidelines for any specific set of resources to which they have been granted access.

4.18 While the University does not generally monitor or limit content of information transmitted on the campus wide LAN, it reserves the right to access and review such information under certain conditions after due approval of the competent authority.

4.19 Computer Centre may block content over the Internet which is in contravention of the relevant provisions of The Information Technology Act, 2000 and other applicable laws or which may pose a security threat to the network.

4.20 Computer Centre may also block content which, in the opinion of the university, is inappropriate or may adversely affect the productivity of the users.

4.21 Computer Centre shall have the right to audit networks and systems at regular intervals, from the point of compliance to this policy. For security related reasons or for compliance with applicable laws, Computer Centre may access, review, copy or delete any kind of electronic communication or files stored on University provided devices under intimation to the user. This includes items such as files, e-mails, posts on any electronic media, Internet history etc. Centre may monitor user's online activities on University network, subject to related Standard Operating Procedures of GoI norms.

5. Email Account Use Policy

In an effort to increase the efficient distribution of day-to-day information to faculty, 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. E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. 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. To receive these notices, it is essential that the e-mail address be kept active by using it regularly.

Staff and faculty may use the email facility by logging with their User ID and password. For obtaining the university's email account, user may contact Computer Centre for email account and default password by submitting an application in a prescribed proforma. Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

5.1 The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes. Using the facility for illegal/commercial purposes is a direct violation of the university's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk email messages; generation of threatening, harassing, abusive, obscene or fraudulent messages/images.

5.2 Users 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. This is very much essential from the point of security of the user's computer, as such messages may contain viruses that have potential to damage the valuable information on the computer.

5.3 Users should not share email account with others, as the individual account holder ispersonally held accountable, in case of any misuse of that email account.

5.4 User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.

5.5 While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its

contents, by the user who has occupied that computer for its use.

5.6 Impersonating email account of others will be taken as a serious offence under the university IT policy.

5.7 It is ultimately each individual's responsibility to keep their e-mail account free from violations of university's email usage policy.

6. Internet and Wi-Fi Access Policy

6.1 A user shall register the client system and obtain one-time approval from the competent authority before connecting the client system to the University Campus wide LAN.

6.2 Users shall not undertake any activity through any website or application to bypass filtering of the network or perform unlawful acts which may harm the network's performance or security.

6.3 For connecting to PU's wireless network, a user shall register the access device and obtain one-time approval from the competent authority before connecting the access device to the PU's wireless network. Wireless client systems and wireless devices shall not be allowed to connect to the PU's wireless access points without due authentication.

6.4 To ensure information security, users should not connect their devices to unsecured wireless networks.

A meeting of Committee duly constituted by Dean of University Instructions to prepare IT policy document held on 25-03-2022 (Friday) at 2 p.m. in the office of Director, Computer Centre. Following members attended the meeting:

Prof. Savita Gupta (UIET) ..... Chairperson

Prof. Sukhwinder Singh, Director, Computer Centre

Professor Sonal Chawla (DCSA)

Dr. Nidhi Gautam (UIAMS)

Dr. DeepakSalunke (Chemistry)

Dr. Tejinder Singh (UBS)

Prof. Anu Gupta (DCSA) ..... Convener

Mr. Guldeep Singh, System Administrator, Computer Centre (Special Invitee)

The members deliberated upon various aspects related to usage of computer and network resources of Panjab University. The proposed IT policy comprising broad guidelines regarding usage of computer and network resources is attached herewith. The committee unanimously recommended that the IT policy need to be reviewed and updated at least once in a year to keep pace with technological advancements in the field of IT.

Prof. Savita Gupta

Prof. Sukhwinder Singh

Professor Sonal Chawla

Dr. Nidhi Gautam

Dr. DeepakSalunke

Dr. Tejinder Singh

Prof. Anu Gupta