IT POLICY

Pandit Deendayal Energy University

Information Technology (IT) Policy

1. Preamble

The Information Technology (IT) infrastructure at Pandit Deendayal Energy University (PDEU) endeavors to facilitate faculty members, staff, students, and visitors with modern computing, networking, and IT facilities that lead to effective daily service operations. PDEU shall implement policies to conserve the functionality of the IT system and safeguard the privacy of work of all stakeholders, keeping the right of usage of networks. This IT Policy shall help set the direction toward acceptable and prohibited actions for policy violations. All the IT infrastructure users abide by this Policy.

2. Applicability

The present Policy is valid for all the IT infrastructure users, such as teaching and non-teaching staff, students, visitors, etc. The Policy is equally applicable to all those who utilize the IT infrastructure/facilities of the University, within and outside the campus.

3. Infrastructure and Information

The IT infrastructure includes all the hardware, devices/technology, network, and software the University facilitates to execute, store, or transfer various technical/non-technical/personal or professional information. These also include the IT resources bought by the individual users and utilized within the premises of the University.

4. IT Service Management

4.1 Primary Users

The primary users of the IT infrastructure/facilities are defined as:

- The person who has been issued a laptop/desktop by the University.
- The person whose cabin/lab/room contains IT infrastructure.

In the case of a facility being used by multiple users, the Registrar/Director/Dean/HoD should assign the responsibility to a specific person.

4.2 End User Computer System

Apart from the IT systems, the University shall consider servers not directly administered by the IT Department as end-user computers. If no primary user can be identified, the concerned department must assume the responsibilities of such end-user computers.

4.3 Entitlements

Teaching and non-teaching staff of the University shall be issued a desktop computer with the approval of reporting/reviewing/superior officer through the IT Department. Employees at the level of Director or above shall be issued computing equipment after approval of the Director General of the University. In case where there is a need to issue a laptop and/or additional computers and other hardware to teaching or non-teaching staff, this may be done with the prior approval of the

		concerned authorities. Removable storage devices, such as USB drives, portable hard drives, etc., shall not be issued to the faculty/staff members. Any deviation from this Policy, such as the issue of additional devices, the issue of laptops/desktops, and devices for internet connectivity, etc., may be done after proper justification and approval from the reporting and reviewing officer of the employee.
	4.4	**Hardware** The University network user community needs to observe certain precautions while getting their computers or peripherals installed so that he/she may not face any inconvenience due to interruption of services or hardware failures. The IT Department should maintain a proper record of all the hardware installations.
	4.5	**Procurement of Hardware and Maintenance Contracts** IT assets like computers, laptops, networking equipment, peripherals, and other hardware are to be procured through the IT Department of the University. The concerned individual should take the approval of the reporting and reviewing officer after proper justification and checking the availability of adequate budget under the category of specific head proposed for the financial budget under consideration. The indent copy should be submitted to the IT Department for further procurement. The IT Department shall first review the availability of indented required assets in the PDEU infrastructure inventory and provide the same to the user if it satisfies the requirements. In case of non-availability of required assets, the IT Department shall communicate with the vendor for procurement after approval of appropriate authorities. The procurement shall only be executed after considering all the requirements of the individual who has raised the requirement/indent. The requirement of assets such as network cables, batteries, damages to desktop/laptop, etc., that are directly handled by the primary user should also be submitted to the IT Department after approval of reporting and reviewing officer. The IT Department should have required budgetary provisions for such assets. The IT Department should execute the annual maintenance contract (AMC) only after evaluating the importance of any asset. Yearly maintenance contracts and/or extended warranties should preferably be with on-site service. Such AMCs may be reviewed periodically, and the IT Department may decide whether to continue with it. The IT Department should regularly communicate information about such contracts/ warranties to primary users.

	4.6	**Maintenance of Computer Systems provided by the University** For all computers purchased by the University and issued to the users, the IT Department shall carry out maintenance work and address any complaints as and when informed by the user. The IT Department shall not be responsible for performing maintenance work on user-owned devices.
	4.7	**Network Cable Connection** While connecting the computer to the network, the connecting network cable should be kept away from any electrical/electronic equipment, as they interfere with the network communication. Further, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.
	4.8	**File and Print Sharing Facilities** The users should not share, distribute, and/or use any illegal or unauthorized copies of the software, music, video, or other digital or non-digital piracy forms. Transferring large movie or music files may overload the network and degrade services that, in turn, slow down the network, making it less responsive to the users. This excessive network traffic can adversely affect the system performance used by other users. Interfering with the ability of others to use the network services violates the university policy and may result in the termination of access to the university network services. The IT Department of the University should routinely monitor network usage patterns. File and print-sharing facilities on the computer over the network should be installed only when required. When shared through the network, the files should be protected with a password and a read-only access rule.
5	**Software** Computer and software purchases for the University should be made through the IT Department. The IT Department should routinely check the expiry of software or license requirements and update the same to the primary user/ department. The installation request should be generated well in advance so that the IT Department can execute the task on time without disturbing academic/teaching work. The request for purchasing software should also be raised in advance after checking budgetary provisions and approval of the reporting and reviewing officer. In the case of software shared by multiple departments, the concerned School Director should assign custody of such software to a specific individual. The individual shall ask for the requirement of such software to all departments and later raise a request for purchasing through the school director. Every department should assign one individual	

	responsible for activities of requirement/installation/renewal of teaching-related software installed in various departmental labs. The IT Department shall ensure the installation of licensed software, operating systems, antivirus software, etc., to all computer systems provided by the University. Alternatively, the use of open-source software should be promoted. University IT policy does not allow pirated/unauthorized software installation on university-owned computers and the computers connected to the university campus network. In such instances, the University shall hold the individual having custody of the computer responsible for any pirated software installed.	
	5.1	**Open Source Software** The University encourages the user community to go for open-source software.
	5.2	**Software Asset Management** The University uses an RF base chip for software asset management.
	5.3	**Operating System (OS) Update** Individual users should ensure that their respective computer systems have the OS updated in respective service packs/patches. The IT Department shall assist users in configuring automatic updates if needed. This is particularly important for all MS Windows-based computers (both PCs and Servers).
	5.4	**Antivirus Software** Computer systems used in the University should have antivirus software installed and always be active. The IT Department shall install appropriate computer antivirus software and configure antivirus signature updates. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy. Individuals should ensure that the updates run regularly. In case of problems with software updates, individual users may ask the IT Department for assistance. The user should not attempt to turn off antivirus updates under any circumstances.
6.	**IT Services**	
	6.1	**Campus Network Operations** The campus network and its active components shall be administered, maintained, and controlled by the IT Department. Service levels shall be maintained as required by the University, School, Departments, and divisions shared by the campus network within operating constraints.

	6.2	**Connection to Network** The IT Department shall be responsible for the smooth functioning of physical connectivity through the campus network backbone of all buildings on the university campus. The IT Department shall choose the best connectivity network backbone that shall suffice the requirements of all users.
	6.3	**Monitoring and Electronic Logs** The University may, at its discretion, monitor Internet and Email activity on the network. Electronic logs that are created as a result of monitoring the internal network or internet usage or Email usage need only be retained until the need for their ends, or for one month, at which time they may be destroyed.
	6.4	**Network Expansion and Upgradation** The IT Department may, at regular intervals, review existing network facilities and the need for possible expansion and upgradation. The IT Department should generate such expansion and upgrade requests and forward them to the university official for budgetary provision in advance.
7.	**Risk Management**	
	7.1	**Backup of Data** In case of information stored on desktop/laptop computers in the custody of individual users, he/she should perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible. The IT Department shall provide additional support in case of need of the user. Preferably, at the time of Operating System installation, one can have the computer's hard disk partitioned into two volumes. The operating system and other software should be on one drive, and the user's data files should be on the other. In the event of virus infection or corruption of the operating system, formatting only one volume shall protect the user against data loss. The IT Department shall take appropriate backups and retain them if data is on servers. Users wishing to have regular data backups should store it on the servers maintained/backed up by the IT Department. The user should contact the IT Department to obtain space on the server.
	7.2	**CCTV Surveillance** The University campus (including boys and girls hostels) shall be monitored using CCTV cameras. The Aminity Department shall decide the locations that need to be monitored in consultation with the IT Department of the University. The CCTV recordings shall be retained for 30 days.

		The purpose/objectives of this system are to monitor all areas to assist with the following: • To assist in the prevention and detection of crime. • To facilitate identifying, apprehending, and prosecuting individuals who perpetrate crime and public order offenses. • To provide the opportunity for monitoring individuals breaching the University regulations and staff conditions of service.
8.	**Information and Network Security**	
	8.1	**IP Address Allocation** Computers attached to the PDEU network may be given static IP addresses or dynamically assigned (through DHCP) addresses at the discretion of the IT Department. Only authorized users shall be allowed to connect to the PDEU network. The users must not change the IP address allotted to their device without the permission of the IT Department. The users who do not comply with the addressing scheme risk disconnection from the PDEU network.
	8.2	**Internet Access** The Internet access provided by PDEU, including the use of the wireless network, shall be intended for education-related activities, whether for college-owned equipment or personal device(s). The internet is encouraged for research, education, and communications for PDEU-related activities. The University may block access to certain websites/content categories that it deems inappropriate for access through the University network. In order to obtain access to websites/content that has been blocked (or sometimes misclassified), proper justification by the user and reporting officer is to be provided. The content may then be unblocked after obtaining the permission of the Director General/Registrar/Director. The University shall maintain the records of websites accessed by the users. Abuse or misuse of Internet access provided by PDEU shall be treated as violating University norms. It may result in disciplinary action, up to and including termination of employment in the case of employees or up to and including expulsion in the case of students. Use of the Internet (wired or wireless) is not intended for the following: • Operation of a business or other commercial use, • Solicitation for personal gain, • Sending chain letters or spamming, • Gambling, • Malicious actions, such as denial of service attacks, • Harassment of other computer users, • Accessing and/or distribution of pornographic materials,

		• Copyright violations, • Bit-torrents, file-sharing, or other bandwidth-intensive applications that may degrade quality of service, • Wireless spectrum interference or disruption of other authorized communications, • Engaging in any other activity in violation of law. • Any other activity leading to violation of rules and guidelines notified by the Government of India or the Government of Gujarat. **Prohibited Downloads** • Any peer-to-peer file-sharing application: Such applications may be used to utilize bandwidth inappropriately. Further, these applications contain third-party applications – called adware or spyware, that collect information about a user's Web surfing habits, change system settings, or place unwanted advertising on the local computer. • Any third-party personal antivirus or firewall: Since adequate security has already been provided on all machines via pre-defined firewall rules, third-party firewalls may interfere with these rules, thus endangering the network. • Any Proxy servers, private firewall, tunneling software, connectivity sharing software. • Hacking tools of any sort: The use of any such tools on the college network is strictly prohibited. • Any other copyrighted content/materials/software which are not appropriate to the user.
	8.3	**Wireless Local Area Networks** Wi-Fi facility is provided across the entire campus of PDEU. In some locations where access through Fiber Optic/UTP cables is not practical/ feasible, wireless communication may be considered. Such connectivity should make use of unlicensed bands of the RF spectrum. The IT Department may restrict access to the wireless local area networks via authentication or MAC/IP address restrictions. Unauthorized Wireless Access Points (APs not installed, maintained, and managed by the IT Department) shall be prohibited at the University. If any unauthorized APs are identified (usually by their interference with other services), the owners of the offending APs shall be asked to remove them from the network, and the devices shall be blocked from the network.

		The users can inform the IT Department if he/she feels that the Wi-Fi signal in a particular location is inadequate for their use. After checking all aspects, the IT Department can add additional Wi-Fi access points. PDEU IT may ask users for the MAC address of their device if required. IP addresses may then be bound to specific MAC addresses. Spoofing of IP and/or MAC addresses is not permitted. Users indulging in such activity may be disconnected from the campus network.
	8.4	**Password Policy** Passwords are an essential aspect of computer security. All University employees shall be responsible for taking the appropriate steps to select and secure their passwords. All system-level passwords must be changed on at least a quarterly basis. All user-level passwords (e.g. Email, web, desktop computer, etc.) must be changed at least every six months. Passwords should never be inserted into email messages or other forms of electronic communication. All user-level and system-level passwords must conform to the guidelines the IT Department provides from time to time. If an account or password is suspected of having been compromised, report the incident to the IT Department and change all passwords.
	8.5	**Removable Media Policy** Removable media refers to any computer storage that is not physically fixed inside a computer. This includes, but is not limited to: • USB flash drives (aka USB sticks, USB pens, memory sticks) • External hard disk drives, including "internal" drives used via a "dock." • Mobile devices used as external storage (e.g., smartphones) • Optical media (e.g., DVD, CD) The use of removable media within the University is not prohibited but should only be used in cases where no suitable alternative exists. The users shall ensure that the use of removable media is suitably controlled within their area of responsibility in line with the objectives of this Policy. • To facilitate the transfer of official data, it is imperative to exclusively employ the official Removable Disk (Pen Drive/Memory Stick) available with the Registrar, Director, Dean, or Head of Department (HoD). The use of personal Removable Disks on official computers, desktops, or laptops is strictly prohibited.

		• University staff members within professional services electing to use removable media shall be responsible for ensuring they are authorized to do so within their area. • Any removable media used to transport or store university data should be purchased via IT Department. • Personally owned removable media shall not be used to transport or store University data. • When the removable media has reached the end of its useful life, it should be submitted for secure destruction to the IT Department.
9	**Social Media Usage** Social media are websites and applications that enable users to create and share content or to participate in social networking. Examples of popular social media sites include but are not limited to LinkedIn, Twitter, Facebook, YouTube, Instagram, Snapchat, Yahoo/MSN messenger, Wikis, and blogs, WeChat, WhatsApp, etc.	
	9.1	**Social Media Post** The messages posted on the official social media handles of the University/School shall be carefully drafted before uploading. Any message shall not damage the reputation of the University or otherwise bring it into disrepute. Safeguards should be implemented to minimize the risk of communication errors via social media, including checking content before publishing. Those posting content on corporate social media accounts must not: • post or promote content that harasses, bullies, or otherwise intimidates, • post or promote content that instructs, causes, or coerces others to harass, bully, or otherwise intimidate, • post or promote content intended to incite violence or hatred, • post or promote abusive content relating to an individual's age, disability, gender reassignment, marriage/civil partnership, pregnancy/maternity, race, religion or belief, sex, or sexual orientation. Content posted or promoted on corporate accounts must be respectful of others and courteous. Corporate accounts must not be used to criticize or argue with colleagues, students, customers, partners, or competitors. Communications through social media must not • include confidential information about an individual or organization,

- discuss the University's internal workings or reveal plans that have not been communicated to the public,
- reveal intellectual property,
- use someone else's images or written content without permission and/or without acknowledgment.

It is also important that content should be accurate and not commit to something that the University does not intend to deliver. If a mistake is made, it is important to be transparent and update the page with a correction.

9.2 **Social Media Account Security**

Social media accounts are at risk of hacking, which can cause significant reputational damage and potentially severe misinformation for stakeholders.

There must be an agreed-upon account manager where several members of staff require access to the same social media account. He/She is responsible for choosing strong and secure passwords, which should be in line with password policy.

9.3 **Individual's Personal and Professional Accounts**

Social media can be an essential tool for individual professional activity and provide a helpful platform for profile-raising and enhancing networks. It is recommended that individuals using social media for both professional and personal reasons maintain separate accounts for these purposes, as the audiences for each activity are often distinct.

10 **Digital Campus**

The University has implemented the TCSiON Digital Campus Solution. The TCSiON Digital Campus Solution comprises a suite of distinct yet cohesive offerings catering to seasonal academic events and mapped to specific departments of an institution. It facilitates the entire student lifecycle management from inquiry to alumni and allows the selection of specific offerings to meet your current requirements. The faculty, staff members, and students should take the maximum benefit of the features of the TCSiON.

11. **Email Account Usage**

The University shall provide email accounts to all faculty, staff members, students, and administrators to communicate information efficiently.

This email service is expected to be used for formal academic or official communications. Use of University email for personal and other frivolous use is not recommended.

All the users shall abide by the following norms while using the email facility provided by the University:

- The facility should be used primarily for academic and official purposes.
- Use of the facility for illegal/commercial purposes is a direct violation of the University IT policy and may entail the withdrawal of the facility. The illegal use includes but is not limited to the unlicensed and illegal copying or distribution of software, sending unsolicited bulk email messages, and generating threatening, harassing, abusive, obscene, or fraudulent messages/images.
- While sending large attachments to others, the user should ensure that the recipient has an email facility that allows him to receive such large attachments.
- DG/Registrar/Director may approve the email storage limit time to time on need basis to various stakeholders.
- The user should keep the allotted storage space of the mailbox within the 80% usage threshold, as the 'mailbox full' or 'mailbox almost full' situation shall result in bouncing off the mail, mainly when the incoming mail contains large attachments.
- The user should not open any mail or attachment from an unknown and suspicious source. Even if it is from a known source and contains any suspicious attachments or looks dubious, the user should get confirmation from the sender about its authenticity before opening it.
- The users should configure messaging software on the computer that they use on a permanent basis, so that periodically they can download the mails in the mailbox onto their computer, thereby releasing the disk space on the server. The user is responsible for keeping a backup of their account's incoming and outgoing emails. The IT Department can be consulted in case of an issue with the configuration of messaging software.
- The users should not share his/her email account with others, as the individual account holder is personally held accountable in case of any misuse of that email account.
- The users should refrain from intercepting or trying to break into others' email accounts, as it is considered illegal and infringes other users' privacy.
- While using the computers shared by other users, any email accounts 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.
- Impersonating the email account of others shall be taken as a serious offense.
- The user, when sending an email from the official mail ID, assumes full responsibility for the email's content.
- While sending any email, the use of carbon copy (cc) to the senior officials of the University is to be done judiciously.

	• The University email account registered under an individual employee's name is to be deactivated immediately upon their departure due to retirement, superannuation, contract completion, or being relieved from their position. In exceptional circumstances, the account may be kept active for a maximum of 15 days with approval from the University Registrar.
12.	**Green Computing** In keeping with the concept of Green Computing, PDEU shall stress energy-saving technologies such as virtualization. This technology allows the conversion of multiple physical servers into virtual servers, which can then be hosted on a single physical server. This leads to lower power consumption by the servers. Since the single physical server generates less heat, additional savings in electricity are seen through a reduction in the air-conditioning load.
13	**Policy Compliance** The Dean-IT Infrastructure shall verify the compliance of this Policy at regular intervals through various methods. The employee/students violating this Policy may be subjected to disciplinary action per the University norms.
14.	**Revision and Deviation in the Policy** PDEU may revise this Policy from time to time as and when required. The modification of this Policy may be possible upon the approval of the Director General of the University.

01/3

Registrar
Pandit Deendayal Energy University
Formerly
Pandit Deendayal Petroleum University
. Gandhinagar, Gujarat - India.