Islamic University of Science & Technology- IUST
Awantipora, Pulwama -192122

Information Technology Policy

Version 1.0

Directorate of Information Technology & Support Services – DIT&SS

1. Introduction

The Islamic University of Science and Technology (IUST) IT policy document sets forth the central policies that govern the responsible usage of the University's Information and Communication Technology (ICT) resources by its authorized users. This IT Policy document covers the IT facilities and services provided either centrally by the University or by the individual departments of the University. Every member of the University is expected to be familiar with the IT policy and adhere to It. Users of the IUST campus network and other computational resources shall be responsible for proper usage and safeguard of the information resources while respecting the rights of other authorized users.

2. Scope of IT Policy

The IT Policy of IUST comes into force to govern the appropriate usage of IT infrastructure established by the University through the Directorate of IT&SS on the Campus (Details of Directorate are given as Annexure I). The broad scope of the IUST IT policy will be as under:

- This policy shall determine strategies to safeguard both data and IT assets in terms of **Confidentiality, Integrity, and Availability** accessed, created, managed, and controlled by the University.
- The policy shall spell out the usage and protection of information assets in data, information systems, servers, computers, network devices and other ICT infrastructure.
- The policy shall ensure high integrity, reliability and availability of information technology assets to all the stakeholders of the University on the Campus.
- Faculty, staff, and students with authorized accounts shall be allowed to use the computing and IT facilities for academic purposes, official University business, and for personal purposes so long as such usage:
    - ✓ It does not violate any Indian laws, university policies, or the Information Technology Act of the Government of India.
    - ✓ It does not interfere with the performance of university duties or the completion of academic work of any kind.
    - ✓ It does not result in commercial gain or private profit other than that which the University permits.

3. Applicability

This policy shall apply to all the stakeholders of the University, including faculty, staff and students using information assets of the University or their resources on the Campus while transmitting, accessing or storing various types of data and information.

4. Areas

The IT Policy shall apply to the areas as specified hereunder:

4.1 Internet Use Policy

Through its Directorate of Information Technology and Support Services, the Islamic University of Science and Technology provides access to a wide range of services through a robust network to support its educational, management, and operational requirements. The Network Support Service section of the Directorate of Information Technology and Support Service is responsible for the ongoing maintenance and support of the network infrastructure. Any problems related to network service within the University should be

reported to the Network Support Services section through a technical help desk that can be accessed through users' accounts or email : nss@islamicuniversity.edu.in.Those who use the computing, networking, and information technology (IT) resources available at the Islamic University of Science and Technology are expected to adhere to the following rules, which are intended to protect the utility and flexibility of the system, the privacy and work of students and faculty, as well as our right to access the international networks to which the system is connected.

a) To use internet services, students and employees are provided user id, and passwords by the Network Support Services section of DIT&SS. Users are expected to respect the privacy of their fellow users and may not permit anyone else to use their password or share their account with them.
b) The users 'responsibility is to protect their accounts from unauthorised use by changing passwords periodically and using passwords that are not easily guessed. The password needs to be at least 8 characters long with at least one special character and one uppercase. The sharing of passwords, for any reason, is strictly against the rules.
c) The use of any method to circumvent system security, guess other people's passwords, or in any way gain unauthorised access to local or network resources is strictly prohibited. User accounts may not be used to access another person's computing account, nor may users attempt to forge an account identity or use a fictitious email address.
d) Using the internet services provided by the University inappropriately or illegally by any user (whether a student or an employee) will subject the user to disciplinary action as determined appropriate by the competent authorities (including suspension or termination of Internet Services, imposition of an Internet Services fine, legal action, and other repercussions).
e) All Internet services provided by the University will be subject to periodic monitoring and surveillance to ensure that they are operating under university policies and procedures.
f) The Directorate of Information Technology and Systems Security (IT&SS) reserves the right, on behalf of the University, to terminate the internet user id of any user who is deemed to be using excessive amounts of storage space or whose actions otherwise restrict the use of computing resources by other users.

4.2 Policy Regarding the Use of Email Accounts

To increase the efficient distribution of critical information to all faculty, staff and students, and the University's administrators, it is recommended to utilize the University's email services, for formal University communication and for academic & other official purposes. Staff, faculty and research scholars duly recommended by their HoD's/Supervisors may avail the email facility by applying to NSS of DIT &SS in prescribed Performa duly forwarded by their respective HoD's. Users should be aware that by using the email facility, they agree to abide by the policies listed below:

a) Employees and students have access to email to assist with the University's day-to-day operations, particularly for educational, research, and administrative purposes.
b) Email should not be used for any unlawful or immoral purposes, nor should it be used for extensive personal use.
c) Using facilities for incidental personal use is permitted as long as it does not consume more than a trivial amount of resources, does not interfere with staff productivity, is not used for

private business activities, does not prevent others who have legitimate University-related needs from using the facilities, and does not involve any illegal or unethical activities.

d) Each user is solely responsible for the content and use of his or her own account. Passwords should not be shared with anyone else and should be changed on a regular basis.
e) Under the University's information technology security policy, impersonating another's email account will be treated as a serious offence.
f) It is primarily the individual's responsibility to keep their email account free of violations of the University's email usage policy.
g) Any email account that is inactive for more than three months will be deleted automatically.

4.3 IT Hardware/Software Installation Policy

4.3.1 IT Hardware Installation Policy

Users of university networks must take certain precautions when having their computers or peripherals installed to experience the least inconvenience if services are interrupted due to hardware failures.

a) All hardware devices acquired by the University shall be considered to be institutional property at all times. All such hardware devices must be used following the terms of any applicable licenses, notices, contracts, or other agreements that may be in effect.
b) Every purchase involving information and communications technology (ICT) must be subjected to technical inspection by DIT&SS and certified following specifications specified in the purchase order.
c) If a Section/Department/Project purchases computers, it is preferable that they come with a 3-year on-site comprehensive warranty. An annual maintenance contract should cover computers after the warranty has expired. This type of maintenance should also include reinstalling the operating system and checking for viruses.
d) UPS should be used to connect all computers and peripherals to the electrical point. Since the UPS requires a continuous power supply to recharge its batteries, it is never recommended to turn off the UPS's power supply. These uninterruptible power systems (UPS) should also be connected to electrical points properly earthed and properly laid electrical wiring, among other requirements.
e) Hardware systems may be moved from one location to another with prior written notification to the NSS unit of DIT&SS, which keeps a record of the move to keep up with the latest inventory.
f) If IUST faculty, staff, and students fail to adhere to this computer hardware installation policy, they may expose themselves and others to the risk of network-related problems, which may result in damaged or lost files, as well as inoperable computers, which may result in a reduction in productivity. Other individuals, groups, departments, and even the University can be adversely affected by a non-compliant computer that belongs to one individual. Thus, it is critical to bring all computers into compliance as soon as they are identified

4.3.2 Software Installation Policy

a) It is the responsibility of individual departments/projects to ensure that any computer systems purchased by them have all licensed software (including the operating

system, antivirus software, and any other necessary application software) installed on them before deploying them. Following the anti-piracy legislation in the country, the information technology policy of the University prohibits the installation of pirated or unlicensed software on university-owned computers or computers connected to the University's campus computer network. A department or individual will be personally liable for any pirated software installed on computers in their department or room if the University determines that the software is obtained illegally.

b) Any new software must only be downloaded and installed with the explicit permission of the administrators of the facility in which it is being used. IUST facilities and individual machines connected to the IUST network are strictly prohibited from installing unlicensed software.

c) Users should ensure that their operating systems, service packs/patches, and other software are up to date by downloading and installing them from the Internet. For all computers that run Microsoft Windows, this is especially important to remember (both PCs and Servers). Users who regularly update their operating systems assist their computers in repairing bugs and vulnerabilities in the operating system discovered by Microsoft regularly. The company releases patches and service packs to correct the problem. It is recommended that at least once a week, checking for and updating the operating system should be performed.

d) Antivirus software should be installed on all computer systems used by the University, and it should be kept up to date and active at all times. Individual users should ensure that their computer systems are protected against viruses by using virus protection software that has been installed and maintained by DIT&SS.

e) Customers, clients, contractors, and other third parties should not be given access to licensed or copyrighted software unless they have been expressly authorized to do so under the terms of the prevailing software agreement.

f) Users shall only use the software in compliance with the terms of the general software license agreement on local area networks, licensing servers, or multiple PCs.

g) The Directorate of IT&SS is not responsible for data loss or corruption on a user's computer due to improper use of computing resources (hardware or software) or damage caused by the advice or actions of an IT&SS staff member assisting the user in resolving network/computer-related issues. The Directorate of IT&SS also makes no guarantees about the security or privacy of electronic messages.

5. Network Security Policy

All users of university information assets must follow the Information Security Policy and any additional rules, processes, protocols, procedures, or guidelines, as well as stay informed about policy changes. Failure to follow the Information Security Policy and any other rules, procedures, or standards in compliance with the University's disciplinary policies and rules, appropriate disciplinary steps will be taken.

a) Those who are authorized to connect network-capable devices of a type that has been approved to the University's network include students, instructors, researchers, and other university community members. The Directorate of Information Technology and Support Services (DIT&SS) is responsible for maintaining and providing configuration requirements for approved devices. Equipment that does not comply with these requirements should not be permitted to connect to the Network in any way whatsoever. Exceptions to these requirements may be made to meet the academic needs of the University.

b) Any Department/Centre/Unit desiring to establish Wi-Fi at their respective departments must take technical specifications along with approved

configuration/make from the Directorate and devices purchased be informed and get configured from Directorate of IT&SS to ensure security on Wi-Fi devices.

c) Activities that can jeopardise the reliable operation of the Network are strictly barred. Some examples of this include, but are not limited to, the operation of network-capable devices that launch attacks against other network-capable devices, network users, and the Network itself; the operation of wireless access points, cordless phones, and other devices that operate in the unlicensed radio communications spectrum; and the impersonation or interference with Network equipment or Network services. Those devices that are interfering with the Network should be disconnected and/or removed from service.

d) Monitoring network traffic and scanning and mapping the network are prohibited unless specifically authorized by the Directorate of Information Technology and Support Services(DIT&SS).

e) The Directorate of Information Technology and Support Services (DIT&SS) will scan all devices connected to the network for security issues and vulnerabilities. Network traffic is monitored to aid in providing a reliable and consistent Network service and the protection of Network users. Network connectivity will be terminated for any devices suspected of violating this policy.

6. Social Networking

All Social networking sites are generally barred in the Campus. Accessing such site through PROXY or by using special browsers will result in the deactivation of their network user Id. Also, legal and disciplinary action will be taken against the rule violator.

7. Directorate of Information Technology & Support Services Responsibilities

In addition to developing e-Governence for IUST, the DIT&SS is responsible for architecting, designing, engineering, configuring, managing, securing, supporting, maintaining, and monitoring the University's wired and wireless network environments, as well as the server infrastructure, which spans over 1000+ nodes distributed throughout the campus. The following are some of the Directorate's primary responsibilities:

a) **Maintenance of Computer Hardware and Networks**

Specifically, Network Support Services, DIT &SS, is responsible for the upkeep of university-owned computer hardware systems and peripherals covered by a warranty or an annual maintenance contract and for which DIT&SS has been officially designated as the primary contact.

b) **Addressing Complaints**

If any of the specific computer systems are causing Network-related problems, DIT&SS may receive complaints about them. User complaints are received by the designated person in DIT&SS, who then works with the service engineers of the respective brands in the case of computer systems under warranty to resolve the issue in a reasonable amount of time.

c) **Scope of Service**

In addition to resolving hardware-related issues, DIT&SS will also be responsible for resolving problems with the operating system or any other application software legally purchased by the University and loaded by a third-party vendor.

d) **Installation of Un-authorised Software**

ACCORDING TO THE GUIDELINES, the DIT&SS Technical team should not encourage users to install any unapproved software on their computer systems. They should strictly refrain from complying with such requests.

e) **Reporting IT Policy Violation Incidents**

f) Any applications that interfere with network operations or with the University's information technology policies must be brought to the attention of the appropriate university officials if they are discovered by DIT&SS or by its technical team.

g) **Reporting incidents related to Network Operations**
The Network Support Services, DIT&SS will be notified when a network port on a specific computer system is turned off due to a virus or other related behaviour that is interfering with network performance.

Director
Directorate of IT & SS IUST

Annexure-I

Directorate of Information Technology and Support Services (DIT & SS)

The initiative of establishing the Directorate of Information Technology and Support Services, **DIT & SS at IUST** is to facilitate widespread information support system, technology-driven institute governance system for achieving academic & administrative effectiveness to realise the strategic goals of the Islamic University of Science and Technology.

The key aim of the Directorate is to leverage ICT to provide various networking and support services through a state-of-the-art secure computing environment comprising of 1000+ nodes, high-end servers, firewalls, access control system, appropriate storage devices, and reliable internet bandwidth of over 1.5Gbps over OFC backed Wi-Fi and wired Network.

The enterprise is used by the University community to strengthen Teaching/learning processes and to administer transparent and efficient university governance through indigenously developed ERP; capable of meeting the challenges posed by the dynamic requirements of the University. That would explain the transformation of the erstwhile Advanced Center for information and Technology & e-Governance (ACIT & e-Gov.)to the establishment of new **DIT & SS in 2018.**

The administrative set-up of DIT&SS comprises of two main wings, namely:

- **Software and Support Services**
- **Network and Support Services**

Software and Support Services

Software and Support Services has been responsible for developing a comprehensive ERP built over web 2.0 technologies. The indigenously developed ERP that supports LMS (learning Management System) is managed by highly talented professionals who are IUST Pass-outs. The main features of the ERP developed by the **Software and Support Services** team include crucial academic & administrative activities of the University like:

- Admission Process Management,
- Course and Programme Management,
- Examination Automation,
- Fee Management, Exam Schedule and Examination Centre Management,
- Grade Management System,
- Transcript Printing,
- CBCS Implementation,
- Lecture Schedules,
- Online Student Attendance,
- Semester Registration,
- Human Resource Management,
- Transport & Hostel Management,
- Recruitment management,
- Online Student Feedback,
- Online Grievances,
- Online File Tracking System,
- Online Store Management,
- Identity Card Generation,
- Departmental Notice Boards,
- Expenditure Management,

- Budget Management
- Statistical Reporting and many more

NETWORK SUPPORT SERVICES:

The Network Support Services wing of DIT &SS is responsible for architecting, designing, engineering, configuring, managing, securing, supporting, maintaining, monitoring University wired, wireless network environments and server infrastructure spread over 1000+ nodes. The role of the network support services is to fulfil the University's mission by ensuring network services are operated securely and efficiently and that they are reliable, robust, and meeting the current and future needs of the University. DIT & SS provides customer support services through its help desk to resolve day-to-day issues related to troubleshooting networks and computers to university users.

KEY FEATURES:

- The Directorate of IT & SS provides reliable internet bandwidth of 1 Gbps under National Knowledge Network along with Internet bandwidth through OFC based STM-1 (155Mbps) network to the users of the University
- DIT & SS provides the university users an advanced unified threat management system (UTM), namely SOPHOS-XG650 which connects unlimited concurrent users and has firewall, Intrusion prevention system, and bandwidth management, antivirus and anti-spam, application , web filtering features.
- The Directorate of IT and SS uses Symantec Endpoint protection Antivirus server for all the users of the University to keep the university data secure and virus free.
- DIT&SS provides support to more than 1000 computers installed in different departments of the University.
- The Network comprises of more than 70 layer-2 manageable switches installed in every block/ building of the University. Every layer-2 switch is connected to the main layer-3 core switch installed in the IT Server room via optical fibre for fast and secure data transfer.
- The University has more than 1000 networking nodes installed in various labs , faculty rooms, browsing centres across the University Campus. In addition to the LAN connectivity, DIT & SS provided Wi-Fi facility to cover the entire Campus through 100+ Hotspots.