

(55)

59



LALIT NARAYAN MITHILA UNIVERSITY  
KAMESHWARANAGAR, DARBHANGA

Information Technology Policy

[Framed under Section 4(1)(22) of the Bihar State Universities Act, 1976.]

**1. Preamble**

Today, most of the information is used and shared in a digital format by students, faculty, and staff, both within and outside the University. It is, therefore, essential to protect the information and the technology resources of the University that support it. The primary purpose of this Policy is to ensure increased protection of our information and Information Technology Resources to assure the usability and availability of those resources. The Policy also addresses the privacy and usage of those who access University Information Technology Resources.

**2. General Principles**

**a. The balance between Academic Freedom and Accountability**

Academic freedom, the freedom of teachers and students to teach, study, and pursue knowledge and research without unreasonable interference or restriction, has been a fundamental value of L N Mithila University. This Policy will be administered in a manner that supports and promotes the principle of academic freedom. Members of the University community must be accountable for their access to and use of university resources. They have to be responsible to protect the University resources for which they have access or custodianship.

**b. Personal Use and Privacy**

The University will apply all legal and ethical restrictions to ensure the due privacy of its IT resource users. However, the University owns and supplies these Information Technology resources to its faculty, staff, and students fundamentally to accomplish its academic missions, hence these resources are primarily intended for use for the purpose of the University, not for personal or business communications.

**c. Departmental IT Policies**

Departments/Institutes within the University may adopt additional information technology policies that are specific to their operations, provided that such policies are

Handwritten signatures and dates: 24/3/22, 24.3.22, 24.3.22, 24.03.22, 24/3/22

consistent with this Policy and the Department/Institute provides a copy of its policies to the Public Information Officer of the university. In the event of inconsistency, the provisions of this Policy will prevail.

**3. Scope**

**a. Application**

This Policy applies to everyone who accesses IT resources of the University, whether related to or affiliated with the University or not, whether inside the campus or from remote locations, including but not limited to students, faculty, staff, and guests. By accessing Information Technology resources of the University, the user agrees to comply with this Policy.

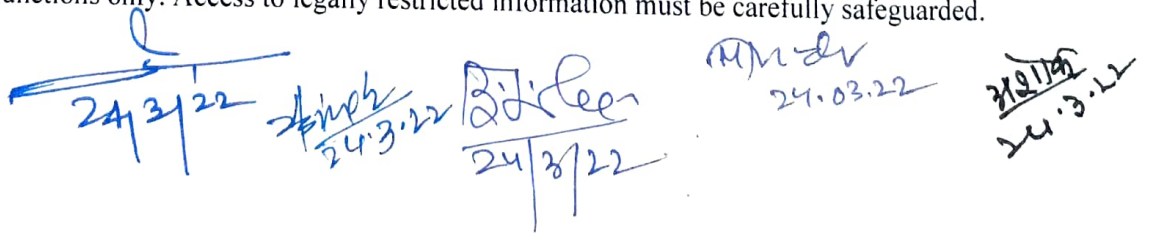
**b. Definition**

- i. Information Technology Resources for purposes of this Policy include but are not limited to, university-owned transmission lines, networks, wireless networks, servers, exchanges, internet connections, terminals, applications, and personal computers which are used by the University under license or contract. It will also include but not limited to information recorded on all types of electronic media, computer hardware and software, paper, computer networks, and telephone systems.
- ii. "Personal Communications" is limited to faculty and student research, teaching, learning, or personal (i.e., non-University related) emails, documents, and correspondence. All other emails, documents, and correspondence prepared by a faculty member, student, or employee in connection with his or her job responsibilities are defined as "University Communications".
- iii. "University Business" refers to the University's activities and functions, including, but not limited to, administrative and academic functions in the areas of teaching, student life, and research, as well as supporting administrative services.

**4. Data Classification and Access Restrictions**

**i. Legally Restricted Information**

The disclosure of some of the information is restricted by laws like the Official Secrets Act, 1923, and Section 8 in The Right to Information Act, 2005, and other laws. Legally Restricted Information must be stored, used, and disclosed to others only on a case-to-case basis to permit the individual faculty or staff member to perform their university functions only. Access to legally restricted information must be carefully safeguarded.


  
 24/3/22      24/3/22      24/3/22      24.03.22      24.3.22

**ii. Confidential Information**

The information which is of sensitive or proprietary nature, the University users shall treat it as confidential. It will include information that the University has agreed to hold confidential under a contract with another party. Confidential information in electronic form must be stored in secure designated data centers or, if authorized to be stored elsewhere, only in encrypted (or similarly protected) form. It must not be stored on a desktop, laptop, or other portable devices or media without encryption or similar protection. If any such data is transmitted by e-mail or another electronic transmission, it must be encrypted or otherwise adequately protected.

**iii. Information for Internal Use Only**

Much information necessary for people to perform their work at the University is properly available to others at the university but is not appropriate to be known to the general public. Information for Internal University Use Only shall be protected behind electronic firewalls in secured offices and shall not be accessible to the public at large or media persons.

**iv. Public information**

Public information is information that is available to all members of the University community and may be made available to the general public. The University reserves the right to control the content and format of public information.

**v. Accounts & Passwords:**

The User of a Net Access ID guarantees that the Net Access ID will not be shared with anyone else and it will only be used for educational/official purposes. The User guarantees that the Net Access ID will always have a password. Network IDs will only be established for Students, teachers, and staff who leave the University will have their Net Access ID and associated files deleted.

No User will be allowed more than one Net Access ID at a time and one login is permitted at a time, with the exception that faculty or officers, who hold more than one portfolio, are entitled to have a temporary Net Access ID related to the functions of that portfolio. For teachers and staff, the validity for Net Access ID will be for their tenure of service. For students, the validity for Net Access ID will be semester-wise and will be renewed on a semester basis after re-verification.

**vi. Computer Ethics & Etiquettes**

The User will not attempt to override or break the security of the University computers, networks, or machines/networks accessible therefrom. Services associated with the Net

*Handwritten signature and date: 24/3/22*

*Handwritten signature and date: 24/3/22*

*Handwritten signature and date: 24/3/22*

*Handwritten signature and date: 24.03.22*

*Handwritten signature and date: 24.3.22*

Access ID will not be used for illegal or improper purposes. This includes, but is not limited to, the unlicensed and illegal copying or distribution of software, and the generation of threatening, harassing, abusive, obscene, or fraudulent messages or violating University policy prohibiting sexual harassment. It shall not be used for commercial purposes, to access TORRENT sites, to represent other organizations or companies, to material that violates pornography laws, or algorithms or software which if transferred violate such laws. Even sending unsolicited bulk email messages comes under IT Policy violation.

**v. Social Networking**

All Social networking sites are barred on the campus. Accessing such a site through PROXY or by using special browsers will result in the deactivation of his/her NET Access ID. Also, legal and disciplinary action will be taken against the rule violator.

**5. Internet Connectivity to Hostels**

University shall provide Internet connectivity to hostels for use of students/scholars. They will have to abide by No extra Internet fee/charges shall be levied upon the hostel boarders for the same. However, any theft of IT equipment installed in the hostels shall be deducted from the hostel borders collectively.

**6. Account Termination & Appeal Process**

Accounts on LNMU network systems may be terminated or disabled with little or no notice. If the termination of the account is temporary, due to inadvertent reasons, and is on the grounds of virus infection, the account will be restored as soon as the user approaches and takes necessary steps to get the problem rectified and communicated to the PIO of the same. But, if the termination of account is on the grounds of wilful breach of IT policies of the University by the user, termination of account may be permanent. If the user feels such termination is unwarranted, or that there are mitigating reasons for the user's actions, he or she should approach the PIO, justifying why this action is not warranted. Users should note that the University's Network Security System maintains a history of infractions, if any, for each user account. In case of any termination of a User Account, this history of violations will be considered in determining what action to pursue. If warranted, serious violations of this policy will be brought before the appropriate University authorities.

**6. Enforcement**

There shall be an IT Cell of the University which shall function under the Public Information Officer of the University. The Cell will include, among others, persons

*Shinich*  
*24.3.22*

*24/3/22*

*B. J. Jolee*  
*24/3/22*

*PT Jolee*  
*24.03.22*

*24/3/22*  
*24.3.22*

having expertise in hardware and software. The Cell will routinely monitor the use of Information Technology Resources to assure the integrity and security of university resources. The PIO will refer suspected violations of applicable law to the appropriate university authority on time.

Violations of this Policy will be handled under normal disciplinary procedures as per the University Laws applicable to the relevant persons or departments. The University may suspend, block or restrict access to information and network resources when it reasonably appears necessary to do so to protect the integrity, security, or functionality of university resources or to protect the University from liability. Unauthorized access to the IT Resources by residents or employees residing nearby can lead to disciplinary action under rules against them and can lead to a fine of Rs. 50,000, and/or lodging an F.I.R.

**7. Review**

The university reserves the right to review the policy from time to time and to bring appropriate amendments as and when required.

*Amey*  
24.3.22

*[Signature]*  
24/3/22

*[Signature]*  
24/3/22

*[Signature]*  
24.03.22

*[Signature]*  
24.3.22