The LNM Institute of Information Technology, Jaipur

Rupa Ki Nangal, Post-Sumel, Via-Jamdoli, Jaipur, PIN 302031, Rajasthan

The LNMIIT e-Governance Policy

January 2022, Version 1.2

1. Preamble

The LNM Institute of Information Technology, Jaipur (LNMIIT) is an institution of higher learning that was jointly established under the public-private-partnership model, by the State Government of Rajasthan and the Lakshmi & Usha Mittal Foundation in 2002. It is deemed to be a university by the University Grants Commission since 2006. It is situated at the outskirts of Jaipur, in the state of Rajasthan in India.

The institute has had its deep connections derived from an apex institution in technology (IIT Kanpur), a major multinational company (ArcelorMittal Inc.) and a state government (Govt. of Rajasthan) from all of which it has derived its initial wisdom in its formative years. A vast majority of its initial structure and processes were inspired by those of the IIT-K whereas as it imbibed its agility, contemporariness, competitiveness, and industry-readiness from the AM-Inc. In those early days (2002-03) e-Governance concept was just beginning to evolve inn the country, particularly in the academic settings. Therefore, even though, right from the first year of its operation, it had used ICT for its range of purposes, it took some time before making its majority of the systems and functions involving majorly digital ways of data storage and use. Over the years, the Institute adapted itself to the best practices, often ahead of many institutions of its age and adopted several elements of computerized services which put together have enabled a major set of components of a full-fledged e-Governance System.

The LNMIIT aspires and attempts to provide its services to all the stakeholders through good and effective e-Governance. The 'Information Technology Act' mentions that public services should be delivered electronically wherever and to the extent possible. As part of its journey towards this primary objective, the institute has had for almost a decade its ERP system, that is now cloud-based has multiple modules including the student lifecycle (from admission to graduation: admissions, academics, examinations, finance, library management, learning management, complaint management, recruitments etc.) and beyond. It, in turn, connects to a set of external cloud based and local server-based software systems and thus enables a wide range of collective service enable ICT-driven governance of the Institute. As of this writing, efforts are on to upgrade the Governance of the Institute including aspects of financial and people management so that a fully unified, seamless and largely paperless system of decision support via e-Governance becomes possible without the risks of a few remaining island entities to explicitly exchange data.

It is envisioned that all the existing and forthcoming services of the Institute will be successfully implementing under e-Governance plan following National e-Governance Plan and Digital India flagship initiatives of Government of India.

The LNMIIT has also formulated its own IT policy more than half a decade ago and created a document called as "IT Policy & Guidelines". This document enables the implementation of this policy by providing the best practices related to implementation and use of e–Governance services. Through e-Governance, the Institute would ensure that all its services are delivered to and accessible by the teachers, students, staff and all other stakeholders (alumni, parents, collaborators, recruiters and select agencies) efficiently, transparently and conveniently in a reliable manner.

This policy is a step further towards the promotion and implementation of e-Governance in the sense that it would enable The LNMIIT to have a data-driven and transparent information, resource planning and decision support systems.

2. Vision and Objectives

The LNMIIT has a vision to provide its services to all the stakeholders through good and effective e-Governance.

Its consequent objectives are:

2.1. To provide all the best possible services of the Institute through e-Governance modules thus enabling the users to access these services through a range of computing and communication devices (ranging from Smartphones and Tablets to Notebooks, Laptops, Desktops as well as

any other contemporary devices over the intranet or the Internet, depending upon access rghts (authorization level), with required degree of security as per respective need and convenience.

2.2. To enable the Institute to function more efficiently and accomplish the visions of e-Governance.

2.3. To adopt and implement an appropriate form of e-Governance, so as to enable the Institute to promote transparency and accountability and eliminate avoidable function-specific / service-specific delays and undue loss of energy leading to increased productivity and a good level of trust.

2.4. To provide easy access and convenient access to information. The modules shall be strategically implemented by completely automating administrative work-flow processes. This shall enhance effective data storage and retrieval at all levels as per hierarchal permissions.

2.5. To further encourage and enhance a more comprehensive implementation of electronic mode of communication, over and above the prevailing system of emails, among all departments/centres / cells /sections or any other entity of the Institute and ultimately moving towards paperless office.

2.6. To put in place a framework for development and implementation of e-Governance systems and applications in the Institute.

2.7. To enable desired level of compliance as may be rerecommended by the national standards and policies established or prescribed by the applicable governmental bodies and statutory bodies, from time to time, in respect of e-Governance with necessary fine-tuning, amendments or enhancement as may be required.

3. Applicability

3.1. The policy shall be applicable to all the employees of the Institute including its faculty members, and staff, all its scholars (post-doctoral and doctoral / graduate), all students and any other stakeholders who may have to use the services provided by the Institute .

3.2. This policy is applicable to all divisions, departments, centres, cells, groups, sections or any other organizational unit of the Institute.

4. Infrastructure

For any e-Governance services to be implemented and delivered, the following key ICT infrastructure should be deployed.

4.1. LNMIIT Unified Computing Service (LUCS) Center

All the IT enabled services including the e-Governance modules shall be hosted and delivered from the Institute server. Adequate servers, network and security devices should be populated in the LUCS. The LUCS data center should be equipped with 24x7 uninterrupted power supply and air conditioning.

4.2. Campus wide Local Area Network (LAN) / Campus Intranet

a) The services shall be delivered to the users through a robust and efficient Campus wide Intranet. The network/internetwork architecture should be built based on the contemporary / emerging global standards. <Current Status: exists>

b) The Intranet / LAN / Wireless LAN should provide appropriate bandwidth inside the campus. Architecture should allow scalability. <Current Status: exists, being further upgraded>

c) High speed Internet connectivity of capacity at least 1 Gbps should be available inside the campus. <Current Status: exists>

d) To provide Redundant Internet connectivity, the Institute should take services from multiple Internet Service Providers (ISPs) <Current Status: exists>

4.3. Cloud Infrastructure

The Institute will use public, private or hybrid virtualization-enabled scalable infrastructure (like cluster / grid / container / cloud) and services including those featuring or supporting required forms of virtualization so as to enable reasonably fast, efficient, cost-effective deployment. These may include both local and remote resources of the authorized kinds,

including but not limited to IaaS, PaaS, SaaS, Storage (SAN/NAS/Cloud-based Storage) etc. <Current Status: exists>

4.4. National Knowledge Network (NKN)

The National Knowledge Network (NKN) is a state-of-the-art multi-gigabit network for providing a unified high speed network backbone for all knowledge related institutions in the country. The purpose of such a knowledge network goes to the very core of the country's quest for building quality institutions with requisite research facilities and creating a pool of highly trained professionals. Best use and advantage should be taken of NKN. <Current Status: exists>

4.5. Power Backup System

a) All the core IT and network access devices in the Institute campus should be provided with adequate power backup solution. <Current Status: exists>
b) The Institute's key Server Farms, HPC Clusters, Supercomputing unit(s) which form part of the current Server Room(s), Network Room(s) and the upcoming Data Centre as well as Disaster Recovery (DR) facility and essential equipment at the academic and research laboratories should be powered through stabilized and surge-protected uninterrupted power supply with required back-up capacity, except for certain emergency / disaster situations. <Current Status: exists, being further enhanced>

4.6. Email and messaging Services

a)- For seamless communication with the users, proper institute-owned or subscribed and controlled /administered / managed secure email and messaging services infrastructure should be deployed.
b)- These services, full or in part, may only be used for official communications to / from the Institute and its employees, current / registered students, alumni / institute-assigned-contractual entities, and authorized official groups.
c)- Any email/message sent by using the Institute Email services should NOT violate applicable code of ethics and use.

5. e-Services Delivery

All services that are feasible to be delivered electronically would be made available online through appropriate vehicle of delivery including but not limited to the Institute's official web-services and / or official desktop or mobile applications. The users, depending upon their authorization status and access rights, shall be able to use these vehicles (including any applicable official / authorized / permitted web-based applications etc.) to access the e-Governance services provided by the Institute.

5.1. Web Portals

a) As per the requirement of the application, service delivery should be done through web portals / services / other appropriate vehicles.
b) Valid types of digital certificates should be used, as per need, for certain class of services.
c) Separate web portals should be developed and deployed for different applications, as appropriate, subject to assed need / considered requirement, impact and security analysis.
d) Any service that involves confidential or privacy-sensitive exchanges must necessary use appropriately / reasonably / computationally secure communication channels.
e) It should be ensured that adequate design, thorough testing and pre-deployment pilot, as a case might deserve) and pre-deployment pilot run of the processes along with the frontend processes are done before making the portal live. This applies to backend as well as front-end elements.
f) Every care should be taken to make the applications secure, robust, error-free, capable of exception/error handling and their user interfaces user-friendly but client-side /user-agent accessible. It should, preferably have accessibility support as well.
g) As far as possible, platform independent services may be preferred over the platform-dependent services unless technically infeasible in view of any major constraint.
h) Multi-language support, where possible, would be a good consideration.

i) All the web portals should be accessible from mobile devices of various form factors and capabilities and should preferably also support adaptability (such as rich or bare minimum functionality-based user experience) in terms of bandwidth / data transfer rates data handling capability, unless security, technology or time-constraints prevent.

Based on the requirements of the e-Governance applications, they would have verifiable security provisions and secure interfaces with a well-known, highly trusted Payment Gateway to enable secure payments / transactions online. A secure Mobile Payment Gateway should also be considered, where feasible.

5.2. E-mail Gateway

All communications from the applications to the users should be communicated through emails. For this purpose, as per need, secure email gateways may need to be integrated with the application(s).

5.3. Messaging Gateway

Based on the requirements of the e-Governance applications, communications with the users may also be done through various messaging platforms wherever feasible. Corresponding secure messaging gateways should be integrated with every web application.

5.4. Payment Gateway

Based on the requirements of the e-Governance applications, they would have interfaces with one or more trusted secure Payment Gateways to enable payment transactions online. A secure Mobile Payment Gateway should also be considered, where feasible.

5.5. Open Source and Open Standards

a) It would be ensured that use of Open Source and Open Standard technologies for software development is used unless otherwise the use of proprietary technology is unavoidable. This would prevent vendor lock-in, unnecessary cost on user licenses and long-term cost liabilities.
b) Service-Oriented Architecture for software development would be followed to ensure interoperability.

6. Application Development

Irrespective of multiple choices / approaches and styles being in vogue or available, there is a definite need for an informed design and implementation methodology involving a consistent, efficient, effective and maintainable approach. A well-documented and systematic approach involving stages like the requirement capture in form of an SRS, post-capture analysis, design, design-verification and refinement as per need, implementation, version control, thorough testing, bug-reporting and correction/patching provision as well as limited-scope based pilot deployment prior to full-fledged production level rollout processes would be highly desirable. As majority of projects might involve a team, awareness and understanding of a team-based quality software design and development process may be considered. Choice of agile or any other paradigm, as appropriate may be chosen as the base strategy. Where necessary, any need for transition from paper based/manual process to online processes is made smooth and adequate safeguards are put in place to ensure implementation that is both incident free and within a secure environment. Institute would adhere to the Standards, Guidelines and Orders issued for software development by the Government of India from time to time.

6.1. Software Codebase

In general, the ownership of the source code of custom developed software for institute whether it be developed in-house or by any third party would rest with The LNMIIT, and the reuse of these software components in other projects of institute would be highly encouraged.

6.2. Upgradation to New Technologies

The Institute would support adoption and usage of emerging digital technologies in e-Governance like Social Media, Internet of Things, Digital Payments, Data Analytics, etc. which will play an active role in improving the delivery of e-Services to its users.

6.3. Security

The Institute shall have periodic cyber security audit of their websites, portals and applications as per GIGW and CERT-IN guidelines. All the applications developed for e-Governance shall be compliant to GoI policies that were in force during the time of development of the application. To protect the IT infrastructure, websites, applications and information of the Government Departments from external attacks, intrusion and hacking, an enhanced IT Security Policy should be drawn and updated from time to time.

7. Institutional Framework

For successful implementation of the e-Governance services in the institute the following institutional mechanism should be put in place.

7.1. The Institute through LUCS, as the Implementing Agency (IA) would be the overall facilitator for promoting Information Technology and e-Governance in The LNMIIT.

7.2. The LUCS shall provide hand holding support to various departments/ sectionsin the areas of infrastructure for e-Governance, capacity building, procurement of hardware, software, services etc.

7.3. The departments/ sections should ensure that the e-Governance services are being utilized by users within their respective departments/ sections and also should ensure that such services are being delivered to users efficiently on time.

8. Data Usage

This section relates to the databases maintained by the Institute administration under the Institute's e-Governance. Data is a vital and important Institute resource for providing useful information. Its use must be protected even if the data may not be confidential.

8.1. Database Ownership

The LNM Institute of Information Technology is the overall data owner of all the Institute's institutional data generated in the Institute. Apart from this, every set of data must have a Data Owner. The Data Owner has overall responsibility for the quality, integrity and security of the data.

8.2. Custodians of Data

The Registrar, LNMIIT is the overall custodian of data of the Institute. IDAAR cell is the owner of the institutional information required for various external agencies. Individual departments/ sections generate portions of data that constitute Institute's database. Individual department/section head have responsibilities for portions of that data.

In many cases data will be entrusted to an individual or a department/ section/administrative unit/ research unit for the purposes of storage and/or processing in which case they take on the responsibilities of the Data Custodian. The following are some of the responsibilities Data Custodian (but not limited to).

a) Maintaining the integrity and confidentiality of the data entrusted to them.
b) Ensuring that access to the data is restricted to those individuals authorized by the data owner.
c) Ensuring that processes undertaken on the data have been authorized by the data owner.
d) Having adequate backup and recovery procedures in place for the data, considering the sensitivity and criticality of the data as characterized by the Data Owner.
e) Providing any information necessary for the Data Owner to fulfill their responsibilities.

8.3. Data Administrators

Data administration activities outlined may be delegated to the nominated person by the data custodian. Presently, IDAAR Cell is working as data administrator of the institute. The data administrators have been assigned database access privileges as per their roles and responsibilities.

8.4. Data Users

Anyone using or processing Institute Data must ensure that they do so in a manner that safeguards and protects the integrity, confidentiality and availability of the data at all times. They must comply with the relevant policies of the Institute (as may be amended from time to time) and with all applicable legal requirements, particularly in relation to data protection and copyright. The data should only be used for the purposes approved by the data owner.

The following are some general policy guidelines and parameters for departments, sections and any other entity who are data users of the Institute:

8.4.1. The Institute's data policies do not allow the sharing of data that is identifiable to a person outside the Institute, except for any explicitly stated and agreed upon / consent-based lawful purposes.

8.4.2. Data from the Institute's Database including data collected by departments or individual faculty and staff, is for internal intuitional purposes only. Only the relevant data as may be required as per statutory/ regulatory provisions and select accreditation and ranking agencies with specific prior authorization alone may be shared, with due conditions as applicable.

8.4.3. One's role and function define the data resources that will be needed to carry out one's official responsibilities/ rights through its data access policies, the institute makes information and data available based on those responsibilities/ rights.

8.4.4. No data directly identifying a person and his/ her personal information, except for the explicitly stated purpose, without first following a well-defined consent-based or lawful process, may be used, shared, or distributed in any form to outside persons or agencies and surveys and other requests for data. All such requests are to be forwarded to the IDAAR Cell or Registrar office. If necessary, the Institute may take legal advice before taking any decision on any such data sought by any agency not directly related to the data sought.

8.4.5. Requests for information from any courts, attorneys, etc. are handled by the Registrar Office of the Institute and departments/sections should never respond to requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the Office of the Institute Registrar for response.

8.4.6. At no time may information, including that identified as 'Directory Information', be released to any outside entity for commercial, marketing, solicitation or other purposes. This includes organizations and companies which may be acting as agents for the university or its departments.

8.4.7. All reports for UGC, MoE and other government or private agencies will be prepared/ compiled and submitted by the IDAAR Cell, Registrar or any other officer delegated to do so by the competent authority of the Institute.

8.4.8. Tampering of the database by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to:

- Modifying/deleting the data items or software components by using illegal access methods.
- Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ departments.
- Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.
- Trying to break security of the Database servers.

Such data tampering actions by institute member or outside members will result in disciplinary action against the offender by the institute authorities. If the matter involves illegal action, law enforcement agencies may also be involved, after due legal consultation.

9. Capacity Building

9.1. The Institute shall formulate and provide appropriate capacity building training sessions for all the e-Governance modules and applications developed and implemented / deployed till then to all its users.

9.2. Timebound training programme in any required Information and Communication Technology (ICT) skill development and capacity building of the university employees would be conducted by the LUCS or any agency explicitly identified by appropriate division, centre, department, cell or section in consultation with the LUCS.

9.3. The LUCS would build capacities within the system for enabling e-Governance, program and change management by training the manpower and deploying appropriate infrastructure and machinery, in consultation with appropriate domain expert, as per need.

9.4. For the purpose of training, employees would be categorized based on their roles and responsibilities and they would be given suitable training as per a defined schedule and process.

9.5. Suitable machismos and processes may need to be created, as an when necessary, for dissemination of knowledge and information regarding the e-Governance services and processes.

10. Budgetary Allocation

The LNMIIT may earmark an appropriate part of the total budget for e-Governance annually, as per need.

11. Review and Audit

11.1. The LNMIIT shall constitute an internal committee for periodic review of the implementation of the policy and would provide necessary guidelines for its implementation from time to time.

11.2. The Institute shall conduct regular audits across all divisions / departments / sections / cells / centres to verify the compliance of the department/ section with respect to its e-Governance Policy, and to ensure that outcomes envisaged as per the plan are achieved.

11.3. All e-Governance projects implemented till ta given point in time shall be reviewed periodically to ensure that they meet the policy, standardization and any regulatory guidelines.

12. Implementation

The LUCS, LNMIIT shall act as a nodal and Implementing Agency for all e-Governance implementation in the institute. LUCS shall coordinate the overall implementation of the policy. In this aspect the LUCS shall be answerable to the Institute leadership and would submit period report to the Institute along with an executive summary of the progress made, any impediments identified and any solutions suggested alongside any identified resource requirement and timeline for required correction or progress.

13. Revisions

The Institute reserves the right to revise the terms of this Policy at any time. Any such revisions will be noted in the revision history of the policy. The most recent version of the approved policy shall be made available at the LNMIIT website and all employees and students of the Institute shall be bound by the provision of the most recent approved version of the policy with effect from its date of implementation as duly notified by the Institute from time to time.

14. Contact Us

If you have any queries in relation to this policy, please contact the Registrar of the Institute at the Email ID: registrar@lnmiit.ac.in with a copy marked to e.gov@lnmiit.ac.in.

Approved