NATIONAL LAW UNIVERSITY DELHI

Information Communication and Technology Policy

(ICT Policy)

2024

CONTENTS

ABBREVIATIONS

AMC – Annual Maintenance Contract

CCTV – Closed Circuit Television

Email – Electronic Mail

HDD – Hard Disk Drive

ICERT - Indian Computer Emergency Response Team

ICT – Information and Communication Technology

IP Address – Internet Protocol Address

IT – Information Technology

LAN – Local Area Network

NAS – Network Attached Storage

NLUD – National Law University Delhi

OTP – One time password

ROM – Read only memory

SMS – Short Message Service

UPS – Uninterruptible Power Supply

I

DEFINITIONS

1) A security incident is defined as any adverse event that impacts, or can impact the availability, integrity, confidentiality, and authenticity of university data, or data pertaining to an individual. Such incidents may include, but are not limited to virus, and other malware attacks, and physical loss of a device or component.

2) Competent Authority: The competent authority for the purpose of this policy is the Vice-chancellor, or in the absence, the Registrar of NLUD, or any other designated person duly authorized, in writing, by the Competent Authority.

3) Confidential information: information marked as such by the Competent Authority, or User.

4) Designated officer: An official designated as such by the competent authority.

5) Head of the centre: An official designated as such by the competent authority.

6) ICT: It refers to all Information Communication Technology facilities, equipment, systems, and services owned, provided, or used by the University.

7) IT department: the person(s), or department designated by the competent authority to deal with IT resources, and services.

8) Personal information: means any information about an individual who is identifiable by such information.

9) Purchase Committee: Means Committee constituted by the Competent Authority for the purpose of procurements.

10) Resources: It includes, but is not limited to computational resources, e.g., computers, networks (wired and wireless), servers, software systems, off-campus network access, the gateway used for world wide web, email, university portal, file tracking system, and others.

11) The University: The term 'University' for the purpose of this policy stands for National Law University Delhi (NLUD)

12) Third party contractor: Any person or entity engaged for procurements, or any goods or services related to the University.

13) User: includes all users of the ICT facilities who access the ICT resources of the university, irrespective of their status of employment, or association with the university, including third party users.

14) Unauthorized use: Unauthorized use may be considered to be any use of the ICT facilities, services, and infrastructure by the users without due authorization/permission of the competent authority.

II

OBJECTIVES OF THE POLICY

This policy aims at:

1) Providing guidelines and strategies for legitimate use, including collection, processing, storage, and disclosure of the information, while maintaining confidentiality and integrity of such information, in accordance with the applicable laws, existing regulations, University policies and principles.

2) Ensuring that the information be used for University's academic, research, or administrative functions, or other legally required purposes only.

3) Ensuring the safety of the users, and entities (sections, branches, departments, etc.) of the university, while keeping in mind the freedom, and dignity of the individuals, to reduce the threat of crime in general.

4) Ensuring the lawful, secure, and effective use of the ICT resources, infrastructure, and equipment in furtherance of the vision, and goals of the university.

5) Providing guidelines with respect to the accessibility and the use of the email services in an efficient, effective, lawful, and ethical manner.

6) Establishing security guidelines for formulating, modifying, storing, and using codes and passwords.

III

PRIVACY AND SECURITY

1) National Law University, Delhi is committed to protecting the privacy of Personal Information, in accordance with the applicable laws.

2) This policy applies to any information including that collected through visits to the University website (http://www.nludelhi.ac.in); information gathered through the University logins; CCTV feeds, and other information/communications that follows from these activities.

3) The University may authorize access to certain types of information including CCTV footage based only on a legal request made by an authority who has powers to make a legitimate demand, such as legal action (E.g. in response to court orders, or legal instruments that require/authorize disclosure), or in the interest of safety and security of individuals, or the community, or as required by law.

4) The University's website may provide links to other websites. In case the User leaves the NLUD website, (www.nludelhi.ac.in) they will be visiting sites that are beyond the control of NLUD. These other websites may send their own cookies to Users, collect data, or solicit Personal Information. This policy does not extend to any external links.

5) The information collected by the University will be within its control and in a manner consistent with applicable laws, existing regulations, University policies, and principles which guide such collection. The collection, use, disclosure, or storage of information will be restricted to that which reasonably serves the legitimate needs of University's academic, research, or administrative functions, or other legally required purposes.

6) The university shall only use Personal Information for the purpose(s) for which it was collected, and no longer than is required, for the purposes, for which the information was originally collected.

    a. The individual concerned has the right to review the information provided to the University, and to ask for inaccurate, or deficient information to be corrected.

    b. Personal Information of individuals shall not be disclosed by the University, except in accordance with the provisions of existing laws and/or University policies.

7) In the interest of student safety and security; crime prevention, and community policing initiatives; and the UGC norms, surveillance cameras may be installed in the University premises. Such technologies will be used to meet the objective of protecting persons and property, while avoiding unnecessary intrusions upon academic freedom, or individual civil liberties including privacy, freedom of expression, and freedom of assembly.

8) Any information collected through the use of surveillance equipment is considered the University's property and/or records. The Vice-Chancellor/Registrar or their designee is authorized to determine the specific personnel in the University who shall have access to the video surveillance equipment and recordings.

9) Disclosure of information obtained from video surveillance to law enforcement agencies or any designate of the Vice Chancellor/Registrar for resolving internal complaints, will be subject to the approval of the Vice Chancellor/Registrar.

10) Subject to technical feasibility, security camera recordings will be retained for a minimum period of 14 days. However, recordings from surveillance equipment may be retained longer under the circumstances listed below:

    a. Upon receiving authorization from the Competent Authority in writing where such a retention reasonably appears necessary to protect the interest of the stake holders,

    b. Upon receiving credible notification by law enforcement authorities for an alleged illegal activity that has occurred, is occurring, or is imminent.

III

INFORMATION AND COMMUNICATION TECHNOLOGY INFRASTRUCTURE AND RESOURCES

1) The ICT infrastructure and Resources should be used only for the legitimate purposes carried out by the Users.

2) The University Intranet, and Internet access should not be used for unauthorized commercial activities, personal advertisements, or promotions ("unauthorised use").

3) The downloading of text, audio, and video files using University infrastructure and services is to be done for academic purposes only.

4) It shall be the responsibility of the Users to maintain Confidential Information, including password used by them.

5) Only authorized Users, or devices can be connected to the University intranet/ internet.

6) Any device belonging to the University, such as network cables, network boxes, podiums, mikes, projectors, biometric systems, sound systems, CCTV Cameras, wireless etc. should not be used for unauthorized use.

7) In case an IT infrastructure equipment is damaged by a User, then an appropriate fine may be imposed upon the User (or an identical equipment of the same description, may be provided in replacement), and a warning may be issued.

8) The Users shall exercise due care and caution while accessing blocked websites. Only the IT Department will be authorized to change the access on a *suo moto* basis or upon receiving a request from the users.

9) Only the IT Department is authorized to issue, and provide a unique IP address to every computing device wherever required, and possible.

10) The assignment and allocation of unique IP addresses should be carried out, and if possible the identity of the unit/block/building should also be represented in these allocations.

11) The users should use only licenced, and authorized software for the university systems and ICT equipment, and it must be ensured that such software/hardware is compatible with the ICT infrastructure of the university.

12) The IT department shall be responsible for the compliance of the terms of software licenses, including allocation to the permissible number of devices.

13) Software installation shall be carried out by the IT Department where required.

14) Moving of computers, systems and components from one location to another must be done with due intimation, and approval of the IT Department, in order to allow the IT Department to maintain records.

15) The IT Department should investigate any hardware or software failure, as soon as it becomes aware of such a failure, and should take appropriate steps to rectify it at the earliest opportunity.

16) IT Department may backup the university data at regular intervals, using appropriate means, and in the process should keep the safety, privacy, dignity, and rights of the users in mind.

17) IT Department should facilitate the users, and ensure that the university data are protected by active, and effective antivirus software(s).

18) The users may contact the IT Department for assistance software and hardware updated.

19) Each user should be provided with usernames and passwords by the IT Department to access the ICT facilities in an individually identifiable manner.

20) The IT Department may be instructed by the competent authority to allow the simultaneous use of a specified number of devices by the individual users, university officials, centres, and departments.

21) IT Department should undertake efficient bandwidth distribution and management over different users of the university.

IV

EMAIL

1) Only the email services provided by the University shall be used for official communications by staff, employees, faculty member, and students including employees and staff of different centres of NLUD.

2) Use of the University email service amounts to the User's agreement to be governed by this policy.

3) It is recommended for Users working in areas dealing with sensitive and confidential data to use 2-Step Verification (also known as two-factor authentication)/ OTP for secure authentication.

4) It is recommended that University officials on long deputation/ stationed abroad and handling sensitive or confidential data should use 2-Step Verification (also known as two-factor authentication)/ OTP for accessing email services.

5) Users shall ensure that the latest operating system, anti-virus, and application patches are available on all the devices.

6) Based on the request of the respective centres, the IT Department will create two IDs, one based on the designation, and the other based on the name. Designation-based ID's are recommended for officers dealing with the public. Use of alphanumeric characters as part of the email id is recommended for Users.

7) By default, the address 'username@nludelhi.ac.in' will be assigned by the IT Department to the users. University officers who resign, or superannuate will be allowed to continue the use of the official email ID for 12 months after the end of their service.

8) Due care should be taken when typing email addresses to ensure that it reaches the intended recipient.

9) Bulk emails by students with multiple intended recipients (e.g., faculty/staff/students) shall be routed through the office of the Registrar.

10) Creation, and exchange of emails that could be categorized as offensive, harassing, or obscene must be avoided.

11) It is acknowledged that individuals, for the purpose of official work/legitimate research, may be required to receive/send content which may, in normal course, be considered as offensive, harassing, or obscene. Such transfer for official work or legitimate research will not amount to a breach of the policy.

12) Creation and exchange of advertisements, solicitations, and other unofficial, unsolicited email (such as spam messages, or campaign emails) should be avoided.

13) Transmission of emails involving language derogatory to religion, caste, ethnicity, gender, sexual orientation must be avoided.

14) Any case of inappropriate use of email accounts shall be considered a violation of the policy and may result in deactivation of the account after consultation with the Vice Chancellor/ Registrar.

15) The 'reply all' and the use of 'distribution lists' should be used with caution to reduce the risk of sending emails to the people who are unrelated to the subject of such emails.

16) Taking backups at regular intervals is the responsibility of the User.

17) Users must not open attachments, or click on links in emails received from unsolicited/untrusted sources.

18) NLUD may define and implement storage quotas for both employee, as well as, student email accounts. Users are responsible for regular deletion of email which is not of use to save storage space. Users will be notified via email when they are approaching the end of their storage limit. Once the storage limit is exhausted, one final email will be sent to the User, notifying them to reduce the storage below the sanctioned limit. After exhaustion of the storage limit, Users will not receive any further emails until the storage is reduced below the storage limit.

19) It shall be within the rights of the IT Department to deactivate or remove any feature of the email service if it is deemed a threat and can lead to a compromise of the service after approval of the Vice Chancellor/ Registrar. Any security incident noticed or identified by a User must immediately be brought to the notice of the IT Department.

20) In case of threat to the security of the service, the email id being used to impact the service may be suspended or deactivated immediately by the IT Department after approval of the Vice Chancellor/ Registrar. The concerned User and the Head of the Centre shall be informed of the security threat and the deactivation.

21) The email ID provided to students shall remain active until three months from the date of convocation of graduating students. On request, a distinct alumni ID may be created and provided to the alumni. All rules applicable under this policy to NLUD students shall apply to NLUD alumni.

V

GENERAL PASSWORD GUIDELINES

1) It is recommended that all passwords be changed every four months. However, the IT Department must change passwords under its direct control at least quarterly, and other users should change their passwords biannually.

2) Email, and other communication apps like WhatsApp should not be used for the transmission of any passwords. Further, it is recommended that the passwords should not be written down, or stored on the computer or a storage device.

3) Every User should be aware of how to select strong passwords.

4) Personal and university passwords should not be common, and the same password should not be used for different access needs.

5) In case of the breach of a password, the user should intimate the IT Department immediately, who in turn take immediate and appropriate action.

6) Following points should be kept in mind to create a strong password:

    a. Inclusion of both upper- and lower-case letters (e.g., a-A)

    b. Inclusion of a combination of letters, numbers, and special characters.

    c. There should be at least eight alphanumeric characters.

    d. It is recommended that personally identifiable information like names, and birthdays should be avoided.

VI

BREACH OF THE UNIVERSITY'S ICT POLICY

In case of a breach of this policy, the matter shall be referred to the Competent Authority for appropriate action within seven days. The competent authority may take steps to ensure the safety and security of ICT equipment, services, and facilities including appropriate action against the concerned user, including, but not limited to the confiscation and/or deletion of ICT resources.