NATIONAL LAW UNIVERSITY AND JUDICIAL ACADEMY, ASSAM

IT (Information Technology) REGULATIONS

May 2019

Table of Contents

CHAPTER – I

I.1. Name of the regulations

These regulations may be called the "National Law University and Judicial Academy, Assam IT Regulations"

I.2. Scope

- To enable all members of the University community to achieve their academic and/or administrative work objectives through use of a secure, efficient, and reliable technology environment.
- To protect academic, administrative, and personal information from current and future threats by safeguarding its confidentiality, integrity and availability.
- To encourage and support management, faculty, staff and students to maintain an appropriate level of awareness, knowledge and skill to enable them to minimize the occurrence and severity of information technology security incidents.
- To ensure that the University is able to effectively respond to, contain, and address significant security incidents, while being able to continue its instructional, research, and administrative activities.

I.3. Definitions

Computer System means

i. any computer system or mobile device and its peripherals owned or administered by the University, together with any associated electronic or optical data storage systems, and
ii. any network, including the internet, intended for the transfer of information in digital form, accessed on University property or through University facilities, and
iii. any machine connected by physical or wireless connection to a network administered by the University.

System Administrator in relation to a computer system means

i. Head of Division (or equivalent)
ii. Head of Information and Technology Services.

University means National Law University Assam and Judicial Academy, Assam.

User means person using a computer system who is

i. a staff member of the University, whether employed on a fixed-term, continuing, full-time, part-time or casual basis
ii. a student enrolled at the University
iii. a person authorised by the University Authority to use the computer system.

CHAPTER – II

Computer and Information Control Policy

All involved systems and information are assets of the University and are expected to be protected from misuse, unauthorised manipulation, and destruction. These protection measures may be physical and/or software based.

II.1. Requirements of users

1.1 Users must not use or attempt to use a computer system without the authorisation of System Administrator.

1.2. Users must take all reasonable precautions to maintain the integrity of passwords and any other security mechanisms.

1.3. Users must not cause costs to be incurred

i. by the University without the authority of System Administrator, or
ii. by any person or organisation without the consent of that person or organisation.

1.4. Unless they have the authorisation of System Administrator, users must not

i. do anything that damages, restricts, jeopardises, impairs or undermines the performance, usability, reliability, confidentiality or accessibility of any digital information system, program, or other stored information or data
ii. access, read, alter, delete or in any other way interfere with, any information, data or files (including electronic mail) held by another person, or attempt to do any of these things, regardless of whether the operating system of the computer permits these acts.

1.5. Users must

i. comply with any instruction by System Administrator about the use of the University's computer system
ii. respect the rights of other users with respect to access to computer systems and enjoyment of use
iii. comply with all applicable Indian law, including law on copyright, privacy, defamation, objectionable material, and human rights.

1.6. Users must not

i. ignore or breach any lawful and reasonable instruction by System Administrator
ii. use a computer system in any way that constitutes discrimination, harassment, or sexual harassment
iii. use a computer system in a manner, or for a purpose, which would bring the University into disrepute, or, if they are staff, which would otherwise breach the University's Staff Code of Conduct or Code of Ethics for Academic Staff
iv. assist, encourage or conceal any unauthorised use, or attempt at unauthorised use, of any computer system.

II.2. Use of IT Equipment

IT equipment includes desktop, laptop and server and associated infrastructures, monitors, printers, scanners, phones, mobile, smartphones, portable computing equipment, Lecture Theatre and General Teaching Space equipment (projectors, microphones, cameras, Video Conferencing Systems, Audio Systems etc.), routers, firewalls, switches, access points and other network infrastructure, Software licenses etc. User has a duty of care to protect IT assets at all-time whether they are in use, storage, movement.

i. Loss or theft of IT equipment must be reported immediately to the IT Section in writing or through email.
ii. All IT equipment must be returned to the IT section upon replacement, equipment redundancy (i.e. no longer required for University business) or when the holder severs affiliation. Equipment holders will be responsible for equipment issued to them until it has been returned to IT Section.
iii. Equipment holders are not permitted to transfer IT Equipment to another member of the University without the consent of the IT Section.
iv. Fixed IT equipment must not be moved without the consultation of IT Section.
v. Equipment holders must present mobile assets such as laptops and mobile phones to their support team for auditing within 2 weeks of request.
vi. IT equipment holders must make every effort to ensure that the equipment asset tag is not damaged or destroyed.

II.3. Use of licensed software

i. All computer software developed by the University employees or contract personnel on behalf of University or licensed for the University use is the property of the University.
ii. University owned licensed software are not allowed to install on a user's privately owned computer.
iii. The terms of any licence agreement between the University and any third party that governs the use of software must be complied by the user.
iv. Making copies of proprietary software unless explicit authority is granted by either the software provider is prohibited.
v. Users must not make proprietary software available for use by any other organisation or individual without the authority of the software provider or System Administrator.
vi. A user who intends to distribute outside the University, in whole or in part of an application program containing embedded proprietary software, must first obtain the written permission of the software provider for each instance of distribution.
vii. A user who publishes material identifying proprietary software must include in the publication explicit and accurate identification of the software provider.

II.4. Use of Internet or other online information repository

4.1. Users of the internet facility must conform to any requirements established and notified by the University for the use of a system or network accessed over the internet.

4.2. Any publication on the internet or other online information repository using University facilities must

i. not be designed to mislead or deceive
ii. not breach the Copyright Law
iii. not promote the personal commercial interests, or political, religious or other personal views of a user or a user's acquaintances, friends or family in such a manner that it appears to have the endorsement of the University
iv. conform to lawful and reasonable employer instructions and policies on online publication.

4.3. Unless authorised by a System Administrator, a user must not request or accept payment, in money, goods, services, favours or any other form of remuneration, either directly or indirectly, for any activity using a computer system.

4.4. The University is not responsible for the content of, or events arising from, communications or interactions between users and others on internet sites where access is not controlled by the University.

II.5. Use of Remote Access Service

Access into University network from outside will be granted using University approved devices, pathways and application software on an individual user and application basis. All other network access options are strictly prohibited.

II.6. Use of University Email Service

i. User shall be responsible for the content generated from his/her email account.
ii. All the official email accounts can be accessed by one assistant. The officer / In-charge will remain responsible for fair and legal usage of these accounts.
iii. Shared email accounts for any purpose whatsoever are not allowed. Any special accounts, if need for conferences, Committees and other valid reasons as determined by the University authorities and it must be applied in writing endorsed by the Registrar and the email account must have a single responsible user.

Email from University facilities should **not** be used for

iv. the creation, storage or transmission of any objectionable communications
v. the creation, storage or transmission of material of a threatening, discriminatory or harassing nature
vi. the creation, storage or transmission of illegal or defamatory material
vii. the creation, storage or transmission of material that brings the University into disrepute
viii. the use of impolite terms or language, including offensive or condescending terms
ix. The sharing or distribution of material in breach of copyright.

The University Management shall investigate all email complaints and will exercise its discretion in judging reasonable bounds within the above standards for acceptability of email communications.

II.7. Use of Computer / Digital Lab

i. No eating or drinking is allowed in the labs at any time.

ii. Making noise through either games / music or even talking and / or singing loudly is prohibited.
iii. No use of profanity, racial slurs, sexual innuendos or pornographic material will be allowed in the lab.
iv. Use of viruses, Trojans, worms or other malicious hacking/cracking software will not be tolerated in the lab.
v. Cell phone use is not permitted in the lab. User must turn cell phone off, or set the ringer to "vibrate," before entering the lab.
vi. Only students, faculty and staff are allowed in the lab unless prior authorization is obtained through University Authority.

II.8. Personal use

Users must not publish online information that is of a personal nature and unrelated to research or career as if it were part of any officially published information; personal information must include a disclaimer that makes clear its unofficial status.

II.9. User Access to University Records

The University provides limited access to academic and administrative data to those whose educational or administrative responsibilities require it to perform their job function. Multiple levels of access exist which are generally determined by the nature of the position held rather than by the individual. This practice helps to ensure that data access restrictions are consistent and based on legal, ethical, and practical considerations. The University expects all custodians of its academic and administrative records to access and utilize this information in a manner consistent with the University's need for security, integrity, and confidentiality. Each University functional unit must develop and maintain clear and consistent procedures for access to academic and administrative data within its area of responsibility, and review access levels and procedures regularly.

i. Access Rights and Responsibilities

Access rights for certain applications are automatically assigned based on role. Department/Section In-Charge must ensure that their representatives maintain only those access privileges required to perform their official job functions.
Users may only access, change, or delete data as required in fulfilment of assigned University duties. User is not allowed to

a. change data about himself/herself or others for reasons other than usual administrative purposes.
b. use information (even if authorized to access it) to support actions by which individuals might profit (e.g., a change in salary, title, or band level; a better grade in a course, financial aid, student account).
c. disclose information about individuals without prior supervisor authorization.
d. engage in any type of unauthorized data analyses (e.g., tracking a pattern of salary raises; determining the source and / or destination of telephone calls or Internet protocol addresses; exploring race and ethnicity indicators; looking up grades).
e. circumvent the nature or level of data access given to others by providing access or data sets that are broader than those available to them via their own approved levels of access
f. facilitate another's illegal access to University administrative systems or compromise the integrity of the systems or data by sharing your passwords or other information.

g. release institutional data to internal departments, external organizations or governmental agencies without prior approval from the authority.
h. retrieve, view, or examine any University document or file, except those to which you are given access or otherwise authorized to handle.

ii. Identification/Authentication

Unique user identification (user id) and authentication is required for all systems that maintain or access the University data. Users will be held accountable for all actions performed on the system with their user id. At least one of the following authentication methods must be implemented:

1. strictly controlled passwords or
2. biometric identification

The user must secure his/her authentication control and must log off or secure the system when leaving it.

II.10. Requirements and authority of System Administrator

i. System administrator is responsible for maintaining security of the systems for which they are responsible, sufficient for authorised users to make effective use of the facilities on those systems and to maintain the integrity of their passwords and any other security mechanisms.
ii. System administrator is authorised to monitor the activities of users and to inspect files and other information for the specific and sole purpose of ensuring that the provisions of these regulations are being met.
iii. System administrator must respect the rights of users to privacy and avoid any unnecessary disruption to the legitimate activities of users.

II.11. Authority to issue standards

i. System Administrator has authority to determine and issue standards to ensure appropriate levels of performance, security, compatibility and legal compliance of computer systems.
ii. Unless he or she judges it necessary to issue a particular standard urgently because of a serious and imminent threat to the operation or security of a computer system, the determination of a standard by the System Administrator is subject to consultation with the University's ICT Committee.
iii. Where the System Administrator believes on reasonable grounds that a standard issued under this section has been breached, he or she may take any immediate action that he or she thinks appropriate to ensure that system performance, security, compatibility and legal compliance are protected. If he or she considers that the breach is sufficiently serious, System Administrator may refer the matter to the Vice-Chancellor who may arrange for the matter to be dealt with in the terms provided under section II.14(3) of these regulations.

II.12. Disclosure of Information

i. In order to exercise the authority provided under section II.14 of these regulations, a system administrator is entitled to access personal information about a user and the user's activities on the computer system if there are reasonable grounds for suspecting that the user may have breached these regulations.

ii. A system administrator who accesses personal information about a user under these circumstances may provide the information to relevant authorities for cost centre management, student discipline and staff discipline.

II.13. Complaints

A dispute or complaint concerning any matter under these regulations may be referred to the system administrator who will determine, on the evidence provided by the complainant and any other evidence that the System Administrator may obtain at his or her discretion, whether there has been a breach of these regulations.

II.14. Breaches

14.1. Where the System Administrator believes on reasonable grounds that a user has breached these regulations, such that the activities or rights of other users of a computer system or of the University are impeded or prejudiced, the system administrator may

i. exclude the user from the system for a period not exceeding one week
ii. remove any relevant material
iii. take any other immediate action that he or she thinks appropriate to protect the integrity of the computer system or the rights of other users.

14.2. If a standard issued under section II.11 of these regulations has been breached, the matter must be handled by, or in consultation with, the System Administrator

14.3. A system administrator who has made a decision under this section may, if he or she considers that the breach is sufficiently serious, refer the matter to the Vice-Chancellor, who may arrange for the matter to be dealt with,

i. if the user is a student, under the provisions of the *Student Discipline Regulations*
ii. if the user is a staff member, under the provisions of the *Staff Code of Conduct*
iii. in cases other than (i) or (ii), as the Vice-Chancellor thinks fit.

II.15. Appeals against decisions by System Administrator

A user may appeal to the Vice-Chancellor against any action or decision under these regulations by the System Administrator.

CHAPTER-III

Responsibilities of IT Section

III.1 IT Asset Management

IT assets shall be protected against physical or financial loss whether by theft, mis-handling or accidental damage. All IT assets shall be traceable and auditable throughout the entire lifecycle. Information about all IT assets shall be held in a suitable electronic database that enables them to be tracked, managed and audited throughout the entire lifecycle. The IT section shall responsible for

i. Issuing of IT asset to the users
ii. Applying barcode asset tag before issue of IT equipment to the user.
iii. Care of IT equipment held in stock for issuing and awaiting transfer for disposal
iv. Ensuring that any IT asset that is retired is disposed of in the correct way
v. Ensure updating central asset registers correctly and as soon as a change is made
vi. Giving correct and appropriate advice to users on the correct handling of IT assets
vii. Creating management reports including the annual audit report

IT Section is responsible for the purchasing, renewal, and disposal of IT assets as per University regulations. Further, IT section will keep records and monitoring of licence quantities of the software purchased by the University.

III.2. University Website and Domain Maintenance and Upgradation

IT Section is responsible of managing the Domain Names of the University. IT Section shall administer the domain 'name space' in accordance with the following principles

1. To maintain and safeguard the image of the University by properly allocating and monitoring the uses of its domain names.
2. To maintain a consistent naming convention on domain names so that the public can easily identify the University with its domain names and related services.
3. To facilitate the use of domain name and to ensure a fair allocation of domain names with an aim to minimizing the disputes that may arise.

Any content that requires to be uploaded on the website much have the approval from the Vice-Chancellor or from the official authorised by the Vice-Chancellor. IT Section shall maintain the design, performance and security standards of the website so that the site functions properly and the university's data is protected, as well as the university's reputation and good name. Any content or data created by university faculty and staff published on the University Web site to represent the work of the university would be owned by the university. Web content shall be hosted by the university on the domain nluassam.ac.in.

III.3. Data Backup and Recovery Management

Production servers and computer systems offering shared network resources shall be backed up regularly by IT Section to provide protection against hardware failures and other disasters. Individual computers are not backed up by IT Section. It strongly recommends that users make individual backups of critical data.

III.4. Risk Management

All Information Systems must be assessed for risk that results from threats to the integrity, availability and confidentiality of University. Assessments must be completed prior to purchase of, or significant changes to an Information System. Risks identified by a risk assessment must be mitigated or accepted prior to the system being placed into operation. Residual risks may only be accepted on behalf of the university by a person with the appropriate level of authority as determined by the Registrar and System Administrator. System Administrator is responsible for ensuring that IT section conducts risk assessments on Information Systems, and uses the university approved process.

III.4. Third-Party Services

When a third party is used to provide services or to store data, security requirements should be considered and made part of any contractual agreements. Such vendor agreements must include appropriate safeguards for the security of the University's information and resources and audit rights. The third party may only have access to the minimum necessary information to perform the tasks for which they have been retained and their activities should be logged.

III.5. Audit Controls

Hardware, software, and/or procedural mechanisms that record and examine activity in computers systems must be implemented. Further, procedures must be implemented to regularly review records of Computer system activity, such as audit logs, access reports, and security incident tracking reports. These reviews must be documented and maintained for at least 1-year by the IT Section.

III.6 Training / Workshops for Users

It is essential that new ICT features and information technology security, including confidentiality, privacy and procedures relating to system access shall be incorporated into new student, staff and faculty orientation procedures and conveyed to existing University community members on a regular basis. Required training/workshops would be conducted for all students, staff and faculty in the University by the IT Section. Further, IT section shall arrange meetings with various sections/departments of the University so that current and pending security issues and new potential risks are discussed and mitigation strategies would be shared. IT section shall also hosts web pages containing resources on information and system security.

CHAPTER –IV

IT Guidelines

Guidelines for Green Computing

"Green computing" represents a responsible way of using Computer systems to reduce power and environmental waste. Green computing best practice and policy covers power usage, reduction of paper consumption, as well as recommendations for new equipment and recycling old machines. Users should adopt the following steps towards green computing strategy

i. Discard used or unwanted electronic equipment in a convenient and environmentally responsible manner.

ii. Reduce paper consumption by using e-mail, electronic archiving, use the "track changes" feature in electronic documents. Use both sides of the paper when printing documents.

iii. Turn off the computer when it is not in use for an extended period of time. Use power management that makes monitors and computers to enter low-power states when sitting idle. It will save energy and help protect the environment.

Guidelines for Open Source Software use

Open Source Software can be freely used, changed, and shared (in modified or unmodified form) by anyone" (http://opensource.org/) and is distributed under a license approved by the Open Source Initiative.

Guidelines for the Connection of Wireless Devices to the University Network

The aim is to prevent the potential security risks that accompany Wireless Devices and to promote the recognised standard practice for connecting such devices to the University network.

Preamble

A Wireless Access Point gives people with a wireless LAN card the ability to work in areas where traditional networks would be expensive or difficult to provide. It also allows the user to work at various places in a Campus without the overhead of finding, livening and connecting to a network port at each location.

Wireless networking presents some potential security problems that cannot be addressed in the same manner as traditional networking.

Wireless Security

The major security risks posed by wireless connectivity are the interception of data and/or the unauthorised gaining of access to University systems and networks.

Such breaches potentially compromise data and machines on the University network, allow the network to be used as a base of attack on others, and may also allow someone to run up large costs to the University for Internet usage.

Because of their insecure nature wireless networks should be treated with the same caution as the Internet is treated. To help prevent security breaches such as those outlined above, wireless devices will

- be firewalled from the rest of the network and from the Internet
- have layered levels of security on top of the base level of security that the equipment comes with.

Connection of Wireless Devices

NLUJAA charged with the provisioning and associated security of the internal and external network infrastructure for the University. The addition of wireless access to the network is no different to adding additional routing or switching gear to the network.

Any user of the University computer infrastructure, who wishes to connect or relocate any form of wireless host device to the network, **must** first seek permission from IT Section.

Permission will only be given for approved devices, and these devices will not necessarily enjoy the same privileges as those connected directly to the internal LAN. Because of the risk of compromise, such devices will, for security purposes, be treated as potentially hostile and will be partitioned from the rest of the network using such mechanisms as are deemed necessary.

Users are expected to connect only to the official NLUJAA network for wireless access. Setting up of unsecured Wi-Fi systems on the University network is strictly prohibited.

Guidelines for Email

This guideline provides a framework for "best practice" in the use of email within the University.

1. General Standards of Use

Email is a forum which could be compared to a conversation. Anything that would not be acceptable in a public arena is not acceptable in email. Similarly, with the ability of messages to be forwarded in whole or part, the sender should be aware that part or parts of a message or messages could be taken out of context and appear inflammatory.

2. Privacy

Users should be aware that email can be a less private form of communication than many people may think. The ease with which messages can be forwarded to other people both inside and outside of the University means that any email (no matter how confidential it was intended to be) has the potential of being read by any number of eyes.

3. Personal Use

It is accepted that University email services may be used for personal communications. Limited, occasional or incidental personal use is permitted when such use, in the judgement of the supervisor of the user, does not generate a significant cost to the University.

Personal use must not be of a commercial nature, or for any other form of personal financial gain.

4. Viruses / Attachments

Users must take all reasonable precautions to prevent the receipt and transmission by email of computer viruses. In particular, users must not transmit by email any file attachments which they know to be infected with a virus and must not open any suspicious file attachments from unsolicited or not to be trusted sources without prior consultation with the IT Section.

5. Records Retention

Emails relating to University business are often used in place of other written communication. As such, it is important for this information to be available to other University personnel if required. It is advisable to retain copies of important emails that have been either sent or received.

Commitments made by email do have some legal standing. There have been situations where people have entered into agreements by email, then left the University. Later, the contracting party has come back with a printed email (which could just as easily have been faked) which may or may not bind the University.

CHAPTER –V

Undertaking with respect to IT Usage

Shall be applicable to the users of National Law University and Judicial Academy, Assam (NLUJAA) who use the University Computer Systems

1. **[Content]** I shall be responsible for all use of this network. In case I own a computer and decide to connect it to NLUJAA network, I will be responsible for all the content on it, especially that which I make available to other users. (This provision will also apply to any computer or device for which I am responsible, and is included in the meaning of "my computer".) In case I do not own a computer but am provided some IT resources by NLUJA, I will be held responsible for the content stored in the designated workspace allotted to me (examples: file storage area, web pages, stored/archived emails, on Computer Lab or Department machines).

2. **[Network]** I will be held responsible for all the network traffic generated by "my computer". I understand that network capacity is a limited, shared resource. I agree that physically tampering with network connections/equipment, sending disruptive signals, or making EXCESSIVE USE of network resources is strictly prohibited. Repeated offenses of this type could result in permanent disconnection of network services. I shall not share the network connection beyond my own use and will not act as a forwarder/ masquerader for anyone else.

3. **[Academic Use]** I understand that the IT infrastructure at NLUJAA is for academic use and I shall not use it for any commercial purpose or to host data services for other people or groups. Also, I shall not host or broadcast information that might harm others or may be otherwise considered objectionable or illegal as per Indian law.

4. **[Identity]** I shall not attempt to deceive others about my identity in electronic communications or network traffic. I will also not use NLUJA IT resources to threaten, intimidate, or harass others.

5. **[Privacy]** I will not intrude on privacy of anyone. In particular I will not try to access computers (hacking), accounts, files, or information belonging to others without their knowledge and explicit consent.

6. **[Monitoring]** I understand that the IT resources provided to me are subject to monitoring, with cause, as determined through consultation with the NLUJAA administration, when applicable. The monitoring may include aggregate bandwidth usage to effectively manage limited IT resources as well as monitoring traffic content in response to a legal or law enforcement request to do so. I authorize NLUJAA administration to perform network vulnerability and port scans on my systems, as needed, for protecting the overall integrity and efficiency of NLUJAA network.

7. **[Viruses]** I shall maintain my computer on this network with current virus detection software and current updates of my operating system, and I shall attempt to keep my computer free from viruses, worms, trojans, and other similar programs.

8. **[File Sharing]** I shall not use the IT infrastructure to engage in any form of illegal file sharing (examples: copyrighted material, obscene material).

In particular, I have noted the following:

Electronic resources such as e-journals, e-books, databases, etc. made available by the Central Library, NLUJAA are for academic use. These resources can be searched, browsed, and material may be downloaded and printed as single copies of articles as is done in the case of printed library material. Downloading or printing of a complete book or an entire issue or a volume of one or more journals (called systematic downloading) is strictly prohibited. Use of robots, spiders or intelligent agents to access, search and/or systematically download from the e-resources is also prohibited. Any violation of this policy will result in penal action as per the rules and regulations of the Institute. I am aware that Systematic downloading will result in the publisher blocking the entire community of users at NLUJAA from accessing these resources.

9. **[Security]** I understand that I will not take any steps that endanger the security of the NLUJAA network. Specifically, I will not attempt to bypass firewalls and access rules in place. This includes not setting up servers of any kind (examples: web, mail, proxy) that are visible to the world outside the NLUJAA campus. In critical situations, NLUJAA authorities reserve the right to disconnect any device or disable any account if it believed that either is involved in compromising the information security of NLUJAA.

10. **[Penalties]** I understand that any use of IT infrastructure at NLUJAA that constitutes a violation of NLUJAA Regulations could result in administrative or disciplinary procedures.

-----000-----