Effective Date: 29th December, 2020
Version History: V.1.0
Version Date: 29.12.2020

NATIONAL LAW SCHOOL OF INDIA UNIVERSITY
INFORMATION TECHNOLOGY POLICIES, 2020

A. The National Law School of India Act, 1986 ("**the Act**") mandates the University to "*advance and disseminate learning and knowledge*" [§.4(1)]. Consequently, the University has progressively introduced various Information Technology ("**IT**") resources for use by its students, staff, visitors and other authorised persons to support the teaching, learning, clinical and research missions of the University and their supporting administrative functions. In doing so, the University also has a duty to create a safe and inclusive social environment, and accessible IT-environment, which is conducive to learning and sharing knowledge.

B. The Vice-Chancellor is the statutory authority responsible for the maintenance of discipline in the University [§.4(d), Schedule to the Act]. In order to carry out the Objectives set out above and in compliance with the responsibility to maintain discipline, the Vice-Chancellor directed the introduction and implementation of these Policies and accompanying procedures.

C. The following Information Technology Policies are thereby notified from the date specified above, with a view to give clarity to the purpose, and the acceptable usage of the Computing Resources, email and other facilities provided by NLSIU and covered by these IT Policies.

D. These Policies have been issued for the first time, and do not replace or repeal any pre-existing regulation, rule or policy. All Users are requested to take note of these IT Policies and ensure compliance with them.

1. Definitions and Interpretation

1.1 In these IT Policies, unless the context otherwise requires, the following capitalised terms have the meanings ascribed to them below.

"Broadcast Email"	means an email message that is sent by a User to other current or former Users and/or parents of current or former Users and is typically targeted at a population of more than fifty addressees, including email messages sent out in more than one batch (with each individual batch consisting of fewer than fifty addressees) which collectively are addressed to more than fifty addresses.
"Confidential Information of NLSIU"	covers sensitive information about individuals, sensitive information about NLSIU, and proprietary academic, scholarly and pedagogical material of NLSIU, provided that any information that is freely available or accessible in public domain, without a breach of confidentiality obligations of any party or furnished under the Right to Information Act, 2005 or any other law for the time being in force, shall not be regarded as Confidential Information of NLSIU for the purposes of the NLSIU Policies. Below is an indicative list of the types of information covered under this definition:

	• Academic, health, disciplinary, insurance, and financial information, records of the Users; • Academic and research study material, papers, and projects generated as part of the NLSIU curriculum or mission and objectives by the Users; • Employment and payment data of NLSIU staff and faculty members; • Information about NLSIU's administrative matters, information technology and security data, operations, finances, legal matters, or other matters of a sensitive nature.
"Computing Resources"	means (i) computing and communication devices, information resources, networks, computer system accounts, telephone and voice mail systems, digital assets and resources which access, store or transmit information related to the Users which are owned or managed by or licensed to NLSIU; (ii) technology administered in individual departments of NLSIU, the resources administered by central administrative departments and in various NLSIU Locations; (iii) technologies, services, and software-as-service owned, licensed, developed or managed by NLSIU including email service, learning management service, remote access software, enterprise resource planning software and (iv) personally owned computers and devices when connected by wire or wireless modes to NLSIU network, and off-campus computers and devices when connected remotely to NLSIU network services.
"Email Service"	means the email service provided by NLSIU.
"External Arrangements"	means contractual arrangements between NLSIU and any vendor or other third-party engaged by NLSIU from time to time, in relation to which, the Users have been notified of their obligations by NLSIU, the vendor or other third-party engaged by NLSIU as applicable.
"Group Email Supervisor"	means the student or faculty member of NLSIU responsible for ensuring the use of a group email address or email list for purposes consistent with the NLSIU Policies.
"IT"	means information technology.
"IT Incident"	means any incident that violates, potentially violates or threatens the confidentiality, integrity, or availability of NLSIU Data, the Computing Resources, Restricted Personal Information, Restricted Sensitive Personal Information, or is in the nature of hacking, cyberbullying, spam or online abuse or harassment involving a User (as a victim, abettor or perpetrator) or NLSIU Data, the Computing Resources, Restricted Personal Information or Restricted Sensitive Personal Information or an incident that results from a violation of any provision of these IT Policies.

"IT Officer"	means a member of the NLSIU faculty or staff who is appointed as the IT Officer by the Vice Chancellor and shall be responsible for the supervision, administration, implementation and response in relation to these IT Policies.
"IT Policies"	means the IT-related policies contained in this document/URL as amended and modified from time to time.
"NLSIU" or "University"	means the National Law School of India University, Bengaluru.
"NLSIU Data"	electronic data and communications collected, stored, transmitted or communicated using NLSIU's network or the Email Service.
"NLSIU Locations"	means all locations, structures, building owned, used or managed by NLSIU including the library, the student hostels, the faculty quarters, the academic block, offices, and other areas.
"NLSIU Policies"	means all policies, codes of conduct, rules and regulations of NLSIU, including these IT Policies.
"Restricted Personal Information"	means any information in electronic format that relates to a User which, either directly or indirectly, can be used to identify such User: provided that any information that is freely available or accessible in the public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as Restricted Personal Information for the purposes of the NLSIU Policies.
"Restricted Sensitive Personal Information"	means such personal information in electronic format that relates to a User and which consists of information relating to: (i) password; (ii) financial information such as bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sex life, sexual orientation, transgender status, intersex status; (v) medical records and history; (vi) biometric information; (vii) caste, tribe, religious or political belief or affiliation; (viii) any information covered under other categories of sensitive personal data as notified by the Indian Central Government from time to time; (ix) any of the information received under above clauses by NLSIU for processing, stored or processed under lawful contract or otherwise: provided that any information that is freely available or accessible in public domain, or furnished under the Right to Information Act, 2005 or any other law for the time being in force, shall not be regarded as Restricted Sensitive Personal Information for the purposes of the NLSIU Policies.
"Student Welfare Officer"	means a member of the NLSIU faculty or staff who is appointed as the Student Welfare Officer by the Vice Chancellor and who shall be responsible for the

	supervision, administration, implementation and response mechanism in relation to the Accessibility Policy contained in these IT Policies.
"Users"	means NLSIU faculty and visiting faculty, staff, students, alumni, guests or agents of the administration, external individuals and organisations accessing network services via NLSIU's computing facilities.
"Vice Chancellor"	means the Vice Chancellor of NLSIU.

1.2 In these IT Policies, unless the context otherwise requires:

a. words importing the singular include the plural and *vice versa*;
b. words importing a gender include every gender;
c. references to 'persons' and 'parties' include companies, bodies corporate, unincorporated associations, trusts and partnerships, in each case whether or not having a separate legal personality;
d. a reference to a law includes amendments, modifications, re-enactments, interpretations or reinterpretations thereof and rules made thereunder, in force from time to time;
e. headings are for convenience of reference only and do not affect interpretation;
f. the words 'includes', 'including' or other words of similar import shall be construed without limitation; references to a policy, section, paragraph, or Annexure are references to such policy, section, paragraph, or Annexure in these IT Policies;
g. the provisions of these IT Policies should be read in conjunction with other related provisions and not in isolation;
h. the word 'harm', in relation to an individual, includes the following:
   (i) bodily or mental injury;
   (ii) loss, distortion or theft of identity;
   (iii) financial loss or loss of property;
   (iv) loss of reputation, or humiliation;
   (v) loss of employment;
   (vi) any discriminatory treatment;
   (vii) any subjection to blackmail or extortion;
   (viii) any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about an individual;
   (ix) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear or being observed or surveilled; or
   (x) any observation or surveillance that is not reasonably expected by an individual.

2. Scope

2.1 The provisions of these IT Policies are subject to the requirements of applicable law. These IT Policies will be a part of the NLSIU Policies. In addition to complying with these IT Policies, Users are also required to ensure that they do not engage in any conduct that results in a violation of any External Arrangement. It is neither intended nor guaranteed that mere compliance with these IT Policies is enough to comply with the requirements of applicable law or the terms of External Arrangements. Users should independently ensure compliance with the provisions of applicable law and the terms of External Arrangements.

2.2 If any violation of these IT Policies constitutes or could potentially constitute, a criminal offence or present a serious risk to the safety of other people, NLSIU may, in consultation with the potential or actual victim thereof, if any, choose to report the same to the police or other government authorities.

2.3 NLSIU will follow the applicable legal principles, applicable principles of natural justice, and applicable substantive and procedural due process before taking punitive action against any individual.

2.4 Unless specified otherwise, these IT Policies will be generally applicable:

a. throughout the NLSIU Locations;
b. to all academic and other programmes of NLSIU; and
c. to all the Users.

3. Computing Resources Acceptable Use Policy

3.1 Purpose

3.1.1 The Computing Resources support the academic, research, and administrative activities of NLSIU and the permission to use the Computing Resources is a license that is extended to Users as members of the NLSIU community at the discretion of NLSIU. Users should consider the fact that the Computing Resources allow them access to valuable NLSIU resources, sensitive NLSIU Data and other data, and the infrastructure that supports the NLSIU networks. Any User who abuses, misuses or exploits the Computing Resources or uses them irresponsibly, unethically, or illegally can potentially cause a high degree of damage or injury to the Computing Resources, the Users and the objectives or reputation of NLSIU.

3.1.2 Each User is, therefore, urged to remember, at all times during their use of the Computing Resources, that the core underlying principle of 'acceptable use' is to respect the rights of other Users, the integrity of the infrastructure and networks of NLSIU, and the license and External Arrangements through which the Computing Resources are made available by NLSIU to the Users.

3.1.3 Due to the nature and severity of the damage that can be caused by an individual who chooses to violate these IT Policies, when a person is found doing so, NLSIU will be constrained to take disciplinary action, including suspension of the person's rights to use the Computing Resources, or imposition of restriction on use of network privileges. A serious violation could result in grave consequences, including suspension or termination from NLSIU and the involvement of law-enforcement authorities.

3.2 Users' Rights and Responsibilities

3.2.1 Each User has a reasonable expectation of unobstructed access to the Computing Resources, privacy, and of protection from abuse, spam and exploitation by others sharing the Computing Resources. Each User also has an expectation that the good name and the reputation of NLSIU will be respected and preserved.

3.2.2 To ensure that the above expectations are met, each User is expected to exercise good judgment in the use of the Computing Resources and remember that merely because an

action is technically possible (through circumvention or otherwise or is not explicitly prohibited by NLSIU) it may not be appropriate to perform that action. All Users are required to:

a. Ensure that his/her account or password is properly used and is not transferred to or used by another individual;
b. Log off from a computer/system after completing access at any location where such computer/system may potentially have multiple Users;
c. Report the loss or theft of any Computer or System containing confidential NLSIU Data or Restricted Sensitive Personal Information in compliance with Electronic Data and Privacy Policy;
d. Use University Email Service only in compliance with the Email Usage Policy; and
e. Take responsibility for any traffic that appears on the University Network that originates from a network jack assigned to such User or from his/her wireless device(s) and/or network(s).

3.2.3 Use of the Computing Resources in a manner that is harmful, detrimental, injurious or damaging to any User, or inconsistent with the purpose for which the privileges in relation to the Computing Resource have been allowed, are strictly prohibited. Prohibited uses of the Computing Resources include but are not limited to:

a. Use of the Computing Resources without authorisation;
b. Violating any institutional policies or procedures or use Computing Resources for unethical, illegal or criminal purposes;
c. Violating the privacy of faculty, staff, students, research subjects, alumni(ae) or members of Governing Body and Executive Council of NLSIU;
d. Using another individual's account or attempt to capture or guess other Users' passwords without authorisation;
e. Not exercising appropriate care in protecting the Computing Resources assigned to the User;
f. Using the Computing Resources in a manner that may violate any External Arrangement;
g. Violating the rights of any person protected by copyright, trade secret, patent or other intellectual property or similar laws and regulations (i.e., installing or distributing pirated or other inappropriately licensed software);
h. Copying, distributing or transmitting copyrighted materials unless authorised;
i. Obstructing University work by consuming excessive amounts of Network bandwidth and other System resources forming part of the Computing Resources, or by deliberately degrading the performance of a computer;
j. Intimidating, harassing, threatening or otherwise doing harm to other Users or damaging, degrading or attempting to damage or degrade Computing Resources;
k. Making offers of products, items or services that are fraudulent;
l. Intentionally causing an IT incident;
m. Not using appropriate password protection and appropriate security measures to protect Computing Resources allocated to the User and thereby making the same vulnerable to hacking, unauthorised use or access, or impersonation. (Users must configure hardware and software in a way that reasonably prevents unauthorized users from accessing NLSIU's network and Computing Resources.);
n. Attempting to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorisation by the system owner or administrator;

o. Attempting to bypass or overcome any restrictions imposed by NLSIU, its vendors or its network the Computing Resources in conjunction with the execution of programs, software, processes, or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users, or damage or degrade performance, software or hardware components of a system;

p. Using tools that are normally used to assess security, or to attack computer systems or networks (e.g., password 'crackers,' vulnerability scanners, network sniffers, etc.) unless specifically authorised to do so by NLSIU;

q. Creating or intentionally releasing computer viruses or worms or otherwise compromising a computer.

3.3 Fair Share of Resources

3.3.1 The Computing Resources are expected to maintain an acceptable level of performance and any frivolous, excessive, or inappropriate use of Computing Resources by one person or a few people should not diminish or degrade the performance of the Computing Resources for others. The campus network, computer clusters, mail servers and other central Computing Resources are shared widely and are limited, and it is essential that these resources be utilised with consideration for others who also use them. Therefore, the use of any automated processes to gain technical advantage over others in the NLSIU community is explicitly prohibited.

3.3.2 NLSIU may choose to set limits on a User's use of a Computing Resource through quotas, time limits, and other mechanisms to ensure that these Computing Resources can be used by anyone who needs them.

3.4 Applicable Laws including Copyright Law

3.4.1 As a member of a premier institution of legal scholarship, each User is expected to uphold applicable laws in their use of the Computing Resources and including the laws regarding licence and copyright, and the protection of intellectual property.

3.4.2 Users must exercise care in ensuring that they abide by all applicable copyright laws and licences. NLSIU has entered into legal agreements or contracts for software and network resources which require each individual using them to comply with those agreements. It is also critical that Users study and understand copyright law as it applies to downloading, uploading or using music, videos, games, images, texts and other content and media over the Internet. The Computing Resources should not be used for unauthorised access, invasion of privacy or copyright infringement in relation to such electronic content or media. Engaging in such activities may attract disciplinary action and prosecution.

4. Email Usage Policy

4.1 Purpose

4.1.1 NLSIU provides the Email Service to certain classes of Users to support academic, administrative and extra-curricular activities of NLSIU and Users should ensure that they use NLSIU's Email Service in a manner that is consistent with this purpose. The Email Service serves as a means of official communication by and between Users and between Users and

NLSIU. Users are responsible for ensuring that they comply with the NLSIU Policies as well as applicable laws when using the Email Service.

4.2 Use of the Email Service by Faculty and Staff

4.2.1 The Email Service has been provided by NLSIU to the faculty and staff at NLSIU to conduct and communicate NLSIU's mission and objectives in relation to their employment or retainership with NLSIU. Use of the Email Service for incidental personal use is allowed provided that such use does not adversely impact NLSIU's mission or objectives, work responsibilities of the faculty or staff member, or the performance of the network.

4.2.2 The Email Service has been provided to faculty and staff members of NLSIU only while they are employed or retained by NLSIU. Once terminated, they shall not use the Email Service through any means or access the contents of their mailboxes that are a part of the Email Service. They shall not bulk-export their Email Service mailbox or export any emails containing Confidential Information of NLSIU or Restricted Sensitive Personal Information of the Users from the mailbox of the Email Service provided to them, or the contents of such emails to any personal or other email account or word processing files.

4.2.3 Faculty and staff email users are advised that electronic data (and communications using the NLSIU network for transmission or storage) may be reviewed and/or accessed by authorized NLSIU officials for purposes related to NLSIU's mission or objectives. NLSIU has the authority to access and inspect the contents of any equipment, files or email on its electronic systems and the faculty and staff members are advised not to use the Email Service for sharing Restricted Sensitive Personal Information.

4.2.4 Prior to termination of employment or retainership of any faculty or staff member, NLSIU may direct such person to handover the access to their mailbox to another person in the interest of smooth and seamless transition of their work-related responsibilities. Every faculty and staff member shall comply with such directions and shall not modify their mailbox in any manner that may make such transition unsuccessful or partly successful.

4.3 Use of the Email Service by Students

4.3.1 The Email Service has been provided by NLSIU to its students to support their educational objectives and for communication by and between the students and between NLSIU and the students. Use of the Email Service for incidental personal use is allowed provided that such use does not adversely impact the purpose for which the Email Service has been provided.

4.3.2 The Email Service is intended to be provided to a student of NLSIU only while a student is enrolled in NLSIU and once a student's Email Service is terminated, such person may no longer access the contents of the mailbox that is part of the Email Service.

4.3.3 Student users of the Email Service are advised that NLSIU may review or access the mailboxes of their official NLSIU email addresses on the occurrence of any of the events specified in *Annexure B* in accordance with NLSIU Policies. NLSIU generally has the authority to access and inspect the contents of any equipment, files or email on its electronic systems.

4.4 Acceptable Use

4.4.1 Users of the Email Service have a responsibility to learn about and comply with the NLSIU Policies and violation may result in disciplinary action dependent upon the nature of the violation.

4.4.2 Use of the Email Service in a manner that is harmful, detrimental, injurious, or damaging to any User and which is not consistent with the primary purpose for which the Email Service has been provided shall be strictly prohibited. Prohibited uses of the Email Service include but are not limited to:

a. Sharing one's email login credentials or gaining unauthorised access to other persons' email accounts;
b. Sending spam, chain mail, anonymous mail, abuse or any type of unauthorised or unsolicited email;
c. Use of the Email Service for commercial activities, personal monetary gain unrelated to NLSIU's activities or for political activities, except as specifically authorised by the NLSIU Policies or in writing by an authorised official of NLSIU;
d. Sending messages or material that constitute a violation of NLSIU Policies;
e. Creation or use of a false or alias email address to impersonate another or send fraudulent or anonymous communications;
f. Use of the Email Service to transmit materials in a manner that violates copyright law or any other applicable law;
g. Falsely representing oneself as a representative of NLSIU or any body or association of persons of NLSIU without due authorisation; and
h. Making statements that defame NLSIU as an institution.

4.5 Broadcast Emails

4.5.1 NLSIU recognises that most email users receive unwanted and unsolicited Broadcast Emails. If spam emails increase in numbers it invariably leads to legitimate emails being ignored, regardless of its origin. At present, faculty Users, staff Users as well as student Users are being permitted to send and receive Broadcast Emails on the condition that it will not be abused, misused or used for purposes other than for those that the Email Service is being provided by NLSIU. In addition to the other provisions of the NLSIU Policies in relation to the acceptable uses of the Email Service, all senders of Broadcast Emails should adhere to these guidelines on Broadcast Emails.

4.5.2 A group email address or an email list consisting of email addresses of Users should be created only after intimating the IT Officer in writing of: (i) the purpose for which it is being created and (ii) details of the Group Email Supervisor. The above details should be intimated to the IT Officer within 15 days of this IT Policy coming into force in relation to group email address and email lists created prior to this date. Where no such Group Email Supervisor is notified in respect of a group email address or an email list in relation to an organisation unit, the head representative of such organisational unit shall be considered the Group Email Supervisor by default.

4.5.3 Before a User sends any Broadcast Email they should obtain prior approval of the Group Email Supervisor. In the ordinary course, prior approval should be provided by the Group Email Supervisor on a per-message basis, although blanket authorisation may be provided for purposes in relation to time-bound academic, administrative and extra-curricular activities permitted by NLSIU. No blanket authorisation shall be given by any Group Email Supervisor

for activities that are not consistent with time-bound academic, administrative and extra-curricular activities permitted by NLSIU. Whenever there is a violation of the above requirement for prior approval or any other violation of the NLSIU Policies through the use of a Broadcast Email, through the use of a group email address or an email list, the Group Email Supervisor shall, in the first instance of violation, issue a warning and take actions to mitigate the consequences of the same and in the second instance of violation, report the violator to the IT Officer.

4.5.4 Before approving the transmission of any Broadcast Email that contains material that is controversial or otherwise likely to attract media attention, whether such material is related to academic, administrative or extra-curricular activities permitted by NLSIU, the Group Email Supervisor shall coordinate with the IT Officer and obtain their written approval.

4.5.5 Broadcast Emails should typically not contain attachments as they place a significant strain on resources that enable the Email Service and thereby adversely affect its performance. However, broadcast emails may contain attachments with the following file extensions so long as they relate to strictly to the academic, administrative and extra-curricular activities of NLSIU: .txt, .pdf, .doc, .docx, .ppt, .xls, .xlsx. xml, .json, .csv, and .log. Prior written approval of the Group Email Supervisor should be obtained prior to circulating any files as attachments to a Broadcast Email other than those with the above extensions.

4.5.6 Broadcast Emails must not display the names and addresses to which the message is sent and should always use approved group email addresses only.

4.5.7 The sender and the relevant Group Email Supervisor are severally responsible for the appropriateness of a Broadcast Email.

4.6 Security and Privacy

4.6.1 NLSIU attempts to ensure that the Email Service is secure, private and reliable. However, NLSIU cannot guarantee the security, privacy or reliability of its Email Service. All users of the Email Service, therefore, should exercise caution in using it and always follow security and privacy best practices. Set out below is an indicative list of best practices that are strongly recommended:

a. Users should avoid transmitting sensitive and confidential NLSIU Data over email including via the Email Service since email is not generally considered to be a secure mode of transmission of sensitive or confidential information. However, where there is no other convenient alternative and such information must be transmitted through email, Users should use the Email Service only for such transmission and also encrypt the contents of the email where possible.
b. Users of the Email Service should exercise caution when opening unexpected attachments, especially from unknown senders.
c. Users should not open hyperlinks to external URLs within an email message unless they are certain that they are legitimate.
d. Users of the Email Service are required to use strong and unique passwords that contain digits, punctuation characters, and letters in lowercase and uppercase. In addition, your email password should be different from your NLSIU network password.
e. Users of the Email Service should use all the security features made available to them as part of the Email Service such as two-factor authentication.

4.6.2 Immediately after a User discovers that an email account that has been created as part of the Email Service has been compromised, the same must be remedied by using means such as resetting the password, reviewing account settings, running computer scans, and malware removal to prevent possible leakage sensitive personal information or NLSIU Data, spamming, potentially infecting others and causing any degradation of NLSIU's network. If the account is being used to harm others at NLSIU and the owner cannot be reached in a reasonable period based on the nature of the harm, NLSIU reserves the right to take actions necessary to stop such harm and prevent future harm including by taking measures such as resetting the password, suspending the account, etc.

4.6.3 Student email users are advised that electronic data (and communications using the NLSIU network for transmission or storage) may be reviewed and/or accessed in cases of emergency or cases that may potentially involve offences of criminal nature. NLSIU has the authority to access and inspect the contents of any equipment, files or email on its electronic systems.

4.6.4 The IT Officer will be the final authority in relation to all violations or abuses of this email policy and the reporting authority for the same.

5. Accessibility Policy

5.1 Purpose

5.1.1 NLSIU is committed to providing equal access to its educational services, programs and activities in accordance with applicable laws and, as part of that commitment, to creating an information and communication technology environment that is accessible to all, including individuals with disabilities and will take all reasonable measures to ensure the same from time to time. Creating an accessible information and communication technology environment is the responsibility of all Users.

5.1.2 This policy applies to NLSIU's Computing Resources and includes their procurement, development, implementation, and ongoing maintenance. It is hoped and expected of the Users that each of them will take positive and proactive measures to ensure that every User has equal access to the educational services, programs and activities through the Computing Resources.

5.2 Reporting and Corrective Measures

5.2.1 The Student Welfare Officer is responsible for notifying responsible parties, including the heads of departments, of issues with the accessibility of their Computing Resources and overseeing the resolution of these issues. Any person experiencing accessibility issues with a Computing Resource should notify the Student Welfare Officer. Such notification to the Student Welfare Officer can be anonymous and also made by a User on behalf of another User.

5.2.2 As the Student Welfare Officer becomes aware of accessibility issues relating to a Computing Resource, they will notify the relevant NLSIU staff member, employee or service provider, who must then:

a. correct the identified accessibility issues;
b. if applicable, justify why modifying the relevant Computing Resource would create an undue hardship or result in a fundamental alteration of the service, program, or activity; and

c. work with the Student Welfare Officer and the affected persons to identify a reasonable accommodation that provides equal access.

5.2.3 If the relevant NLSIU staff member, employee or service provider fails to provide a satisfactory response to the Student Welfare Officer's inquiry or do not address accessibility issues within 2 weeks of being notified of the accessibility issue, the Vice Chancellor will be contacted by the Student Welfare Officer and required to address the issue, in consultation with an accessibility compliance team if necessary. The accessibility team will consist of one technical member and one faculty member appointed by the Vice Chancellor and will be responsible for resolving the issue within 2 weeks of being constituted.

6. Electronic Data and Privacy Policy

6.1 Purpose

6.1.1 NLSIU is committed to ensuring the privacy of the Restricted Personal Information and Restricted Sensitive Personal Information collected by NLSIU from the Users and will take all reasonable measures to ensure the privacy of Users. Likewise, it is expected that the Users become aware of this policy and the NLSIU Policies and comply with all applicable laws and regulations on privacy and data protection. This policy is only intended to specify the minimum levels of protection of Restricted Personal Information and Restricted Sensitive Personal Information. All Users shall limit access to Restricted Personal Information and Restricted Sensitive Personal Information to those individuals who meet the following criteria:

a. have a need for such information for carrying out the objectives and the mission of NLSIU;
b. can show institutional need for accessing such information;
c. have received approval from the IT Officer; and
d. if not a User, can provide annual audit trail to NLSIU for the usage of such information.

6.2 Access, Disclosure, Storage, Transmission, Back-up, Disposal

6.2.1 The concerned Departments of NLSIU that manage Computing Resource which contain Restricted Personal Information and Restricted Sensitive Personal Information shall maintain strict control over access to the same. Users who are assigned keys, given special access or assigned job responsibilities in connection with the safety, security or confidentiality of Restricted Personal Information and Restricted Sensitive Personal Information should use sound judgment and discretion in carrying out their duties and will be held accountable for any wrongdoing or acts of indiscretion. Furthermore, information shall not be divulged, copied, released, sold, loaned, reviewed, altered or destroyed except as properly authorised by the IT Officer.

6.2.2 At the end of their employment or affiliation or other association with NLSIU, Users shall relinquish ownership and possession of Restricted Personal Information, Restricted Sensitive Personal Information, NLSIU documents and records and after creating clear documentation on the manner of such relinquishment and how the same can be accessed by those authorised to handle the same following such relinquishment. They shall maintain the confidentiality of Restricted Personal Information and Restricted Sensitive Personal Information after they leave NLSIU. Questions regarding Restricted Personal Information, Restricted Sensitive Personal Information, NLSIU documents and records should be directed to the IT Officer.

6.2.3 While efforts are made to ensure reasonable expectations of privacy for the Users, legitimate reasons will arise that will require that access to Restricted Personal Information and Restricted Sensitive Personal Information be maintained on NLSIU workstations, servers or peripherals, provided to Users and also to third-parties. These exceptions may be required based on legal action (such as a court order), reasons of health or safety of an individual or group, NLSIU's academic, research or technological initiatives.

6.2.4 Access provided to all Restricted Sensitive Personal Information must be documented and the persons providing such access shall ensure that the same is documented. Persons giving such access should be authorised by the IT Officer to give such access. As far as possible, Users should be informed of the purpose for which any Restricted Sensitive Personal Information is being collected. Upon collection, the Restricted Sensitive Personal Information should be used only for the purpose for which it has been collected and the same should be removed in accordance with this policy when that purpose has been met, fulfilled or is no longer relevant.

6.2.5 Individuals shall not disclose any Restricted Personal Information and Restricted Sensitive Personal Information that they obtain as a result of their employment at NLSIU to unauthorised persons.

6.2.6 Restricted Personal Information and Restricted Sensitive Personal Information must be stored on a server centrally managed by under the supervision of the IT Officer or in an environment that is under strict supervision of officials and staff members of NLSIU and such officials and staff shall maintain the privacy of the Restricted Sensitive Personal Information. Restricted Sensitive Personal Information shall not be stored or handled on any personal workstation, laptop, portable storage device, or locally managed server. Exceptions must be reviewed and approved in writing by the IT Officer.

6.2.7 Restricted Sensitive Personal Information must be housed on a server or a local machine that is secured with a strong password and meets current operating system, hardware, and software support levels.

6.2.8 Wherever possible, Restricted Sensitive Personal Information on a bulk-basis should be transmitted by using encryption or password-lock mechanisms.

6.2.9 Restricted Sensitive Personal Information concerning Users may be released to third-parties (other than when called for under applicable law) only if the Users have been informed of the possibility and purpose of such release at the time of collecting the Restricted Sensitive Personal Information and the Users have consented to such release. All such release shall be also be authorised by the IT Officer and shall be released only after the third-parties enter into standard-form confidentiality agreements which also contain adequate privacy-protection provisions. All authorised Users who access Restricted Sensitive Personal Information in relation to other Users are also required to enter into a standard-form confidentiality agreement with NLSIU before accessing the Restricted Sensitive Personal Information.

6.2.10 It is the responsibility of each User entrusted with Restricted Personal Information and Restricted Sensitive Personal Information to back it up and store it in a secure and controlled location. Such backup should be encrypted if technically feasible.

6.2.11 Restricted Personal Information and Restricted Sensitive Personal Information shall be disposed of in a confidential manner. To dispose of Restricted Personal Information and Restricted Sensitive Personal Information departments and offices must:

a. take extra measures to wipe clean the hard drive of any machine or device that may contain such information before discarding, sending to backup, or transferring it to another individual or department or a third-party;
b. use a hard drive crusher for crushing no-longer needed drives containing such information.

6.2.12 Violation of this policy by a User will be cause for disciplinary and possible legal action. Unauthorised access indicating that privacy, copyright, or other laws may have been broken by an individual may be referred to legal authorities, at NLSIU's discretion.

7. IT Incident Response Procedure

7.1 Purpose

7.1.1 This is the procedure for actions that must be taken in response to an IT incident.

7.2 Reporting

7.2.1 NLSIU takes a complaint about an IT Incident very seriously, especially where any individual is victimised by such IT Incident. NLSIU strongly encourages Users to report IT Incidents regardless of whether they are victims of the IT Incidents themselves. Depending on the nature of the IT Incident, a User may choose to report an IT Incident by identifying themselves or anonymously, in each case by filing the 'IT Incident Reporting Form' provided as the *Annexure A* and emailing the same to the following email address: [itresponse@nls.ac.in].

7.2.2 NLSIU is committed to extending protection to the victim of an IT Incident as well as a person who reports an IT Incident. Any form of bullying, abusing, harassing, threatening, or otherwise targeting a victim of an IT Incident or a person who has reported an IT Incident will be dealt with very seriously. The University may initiate inquiry proceedings against persons accused of bullying, abusing, harassing, threatening, or otherwise targeting a victim or a User who reports an IT Incident, in accordance with the NLSIU Principles of Conduct, 2002, the Code to Combat Sexual Harassment, 2019 or the UGC Anti-Ragging Regulations, 2019, as applicable.

7.3 Authority

7.3.1 The IT Officer is tasked with executing this procedure whenever there's an IT Incident or a violation of the IT Policies that no other NLSIU office, department or authority is specifically authorised to respond to. The IT Officer may initiate a response under these Policies either acting on an IT Incident Report received in the form provided as the *Annexure A* or otherwise.

7.4 Methodology

7.4.1 The IT Officer's response to an IT Incident shall have the following phases:

a. Preparation
b. Identification and Containment
c. Investigation
d. Repair
e. Debriefing

f. Reporting (if necessary)

7.4.2 Preparation: Preparation includes activities that enable and empower the IT Officer to respond to an IT Incident and may include reviewing policies, enlisting the help of other Users or external consultants (after they execute legal contracts for confidentiality), and purchasing services or tools for investigation, repair or recovery. Any expenditure to be incurred for this phase shall be incurred after obtaining the approval of the Finance Committee of NLSIU.

7.4.3 Identification and Containment: Identification is the process of discovering and detecting the IT Incident by the IT Officer with or without the help of third-parties or external consultants with the goal of estimating and limiting the extent and scope of the consequences of the IT Incident, repercussions to any victim thereof and the initial classification of the IT Incident.

7.4.4 Investigation: Investigation is the phase where the IT Officer conducts a 'root-cause analysis' of the IT Incident, rechecks the initial classification of the IT Incident and if necessary reclassifies the same.

7.4.5 Repair: Repair is the rectification of Computing Resources, NLSIU Data, Restricted Personal Information, Restricted Sensitive Personal Information, facilitating protection and providing assistance to any victim or affected User or other person, and taking all measures to ensure that the IT Incident is contained.

7.4.6 Debriefing: Debriefing is the analysis of the IT Incident by the IT Officer for its procedural and policy implications, the gathering of metrics, and the incorporation of "lessons learned" for future reference and training in consultation with the victims, affected Users or persons, the relevant NLSIU authorities, and any external consultants qualified to advise on the same.

7.4.7 Reporting: The determination by the IT Officer in consultation with the victims, affected Users or persons, and the relevant NLSIU authorities of whether there are regulatory requirements for reporting the IT Incident to outside parties, including the police or other government authorities and completion of any such reporting requirement.

7.4.8 At any point during the response to an IT Incident, the Vice Chancellor may call upon the IT Officer to escalate any issue regarding the response or the IT Incident and separately, devise appropriate mechanisms to resolve the IT Incident.

8. Review

8.1 NLSIU will review and update these IT Policies from time to time and oversee the implementation, modification, amendment and revision of these IT Policies. Suggestions for modifications or amendments to these IT Policies may be initiated at any time by a User by submitting a detailed proposal for the same to the IT Officer after considering any inconvenience or prejudice that may be caused to NLSIU or any User if such modification or amendment were to be implemented. A suggestion or proposal may not receive a response from NLSIU. All proposals for modifications or amendments are subject to discussion, revision, and recommendation by the IT Officer. All modifications, amendments and revisions of these IT Policies require the approval of the Vice Chancellor.

Annexure A

IT Incident Reporting Form

** indicates that a field is required*

You are reporting this on behalf of: *	• Yourself • Someone else who is a student of NLSIU • Someone else who is a staff member of NLSIU • Someone else who is a visitor to NLSIU • Other person (and their relationship to NLSIU): _____
Choose one option from the list You are:	• A student of NLSIU • A staff member of NLSIU • A visitor to NLSIU • Other person (and relationship to NLSIU): _____
The perpetrators is/was:	• NLSIU student(s) • NLSIU staff member(s) • Someone known to me/the victim • A stranger to me/the victim • I am not sure Other person (and relationship to NLSIU, if any): _____
Choose the most appropriate category You identify your gender as: *	• Woman • Man • Other • Prefer not to say
If reporting anonymously, why are you reporting anonymously? *	• I'm concerned that the perpetrator might retaliate • I feel partly guilty for what happened • Making a complaint would have a negative impact on my health or well-being • I have concerns that it might affect my career • I cannot prove the behaviour that took place • I am worried about being victimised further • I don't want anyone other than the IT Officer and the persons responsible for responding to this IT Incident to know that it took place • I feel embarrassed or ashamed • It's not serious enough to warrant a complaint • I'm worried that there would be repercussions in my social circle • I don't want to get another person/other people into trouble • I'm worried that I won't be believed • The victim did not want to report it themselves • Other reasons: _____

When did the IT Incident take place? *	• In the last week • In the last month • In the last year • Over a year ago
Choose the most accurate description of where the incident took place	• In NLSIU academic block • In NLSIU library • On NLSIU hostel premises • On other NLSIU property • I choose not to say because: _____
Choose all the relevant real or perceived personal traits to which the IT Incident may have been linked?	• Age • Disability • Gender • Sexual orientation • Ethnicity • Religion or belief • Transgender status • Caring responsibilities • Nationality • I don't know
Explain the type of IT Incident that took place: * (you may attach a detailed description to this form)	_____
What, in your opinion, would immediately offer relief or protection to the victim of the IT Incident?	_____
How you may be contacted by NLSIU through its authorised persons in response to this Report: *	• By email: _____ • By phone: _____ • In-person (preferred date, time and venue): _____ • Other means: _____ • I choose not to be contacted further in relation to the IT Incident for the following reasons: _____

Annexure B

Emergency Access to Accounts and Information

If NLSIU or its IT Officer receives a complaint or any evidence about or have a reasonable basis to believe that any of the following may have occurred:

- *Use of the Computing Resources or Email Service for illegal or criminal purposes;*
- *Use of the Computing Resources or Email Service in a manner that violates the privacy of faculty, staff, students, research subjects, alumni(ae) or members of Governing Body or Executive Council of NLSIU;*
- *Unauthorised use of another User's email or other accounts without authorisation;*
- *Using the Computing Resources in a manner that may violate any External Arrangement;*
- *Use of Computing Resources to in a manner that violates the intellectual property rights of any person;*
- *Obstructing University work by consuming excessive amounts of Network bandwidth and other Computing Resources or otherwise deliberately degrading performance of a computer;*
- ***Intimidating, harassing, threatening or otherwise doing harm to other Users, or damaging, degrading or attempting to damage or degrade internal or external Computing Resources;***
- *Intentionally causing an IT incident;*
- *Not using appropriate password protection and appropriate security measures to protect resources allocated to the User and thereby making the same vulnerable to hacking, unauthorised use or access, or impersonation;*
- *Attempting to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorisation by the system owner or administrator;*
- *Attempting to bypass or overcome any restrictions imposed by NLSIU, its vendors or its network the Computing Resources in conjunction with the execution of programs, software, processes, or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users, or damage or degrade performance, software or hardware components of a system;*
- *Using tools that are normally used to assess security, or to attack computer systems or networks (e.g., password 'crackers,' vulnerability scanners, network sniffers, etc.) unless specifically authorised to do so by NLSIU;*
- *Creating or intentionally releasing computer viruses or worms or otherwise compromising a computer.*