CONFIDENTIALITY POLICY OF DAMODARAM SANJIVAYYA NAITONAL LAW UNIVERSITY (DSNLU)

Policy Statement

Information collected and stored by Damodaram Sanjivayya National Law University (DSNLU) remains the property of DSNLU, and may be considered confidential. The release of confidential information by any University representative puts the University at substantial risk of both legal and financial repercussions. To that end, this Policy is intended to describe several categories of Confidential Information and to establish the consequences for the distribution or other improper use of Confidential Information. The University reserves the right to modify or amend this Policy at any time, at its sole discretion. Any change to this Policy will become effective at the time designated above, and the changes will apply to both current and future students and employees. This Policy does not constitute an express or implied contract between DSNLU and any past, present, or prospective student, employee (including administrator, faculty, or staff), contractor, or volunteer. This Policy governs conduct on all of the University's properties. Unless otherwise stated, the term "Employee" as used in this Policy shall refer to all employees (including administrators, faculty, and staff), contractors, and volunteers.

Purpose

This policy is intended to provide Damodaram Sanjivayya National Law University (DSNLU) employees with a basic understanding of their responsibilities to protect and safeguard the Confidential Information to which they have access as a result of their employment.

Scope

This policy applies to all faculty, staff, and students as well as any other individuals or entities who use data and business systems at the University. This policy applies to all university data, even if stored without the use of an IT resource. Further, this policy applies to all IT resources owned or leased by DSNLU; to any privately-owned equipment connected to the campus network and includes, but is not limited to, computer equipment, software, operating systems, tablets, phones, multimedia devices, storage media; and the campus network itself.

Securing and protecting data and business systems from misuse or malicious activity is the responsibility of those who manage systems as well as those who use them. Effective security is a team effort involving the participation and support of every member of the University community who accesses and uses data and business systems.

Policy

Security and confidentiality of Confidential Information is of the utmost importance at DSNLU. It is the responsibility of every employee to respect and maintain the security and confidentiality of Confidential Information. A violation of this policy may result in disciplinary action.

For purposes of this policy, "Confidential Information" is defined as information disclosed to an individual employee or known to that employee as a consequence of the employee's employment at DSNLU, and not generally known outside DSNLU, or is protected by law. Examples of "Confidential Information" include but are not limited to – student grades; financial aid information; social security numbers; (Aaadhar Card, PAN etc) payroll and personnel records; health information; self-restricted personal data; credit card information; information relating to intellectual property such as an invention or patent; research data; passwords and other IT-related information; and DSNLU financial and account information. Individual offices, departments, or programs may have additional types or kinds of information that are considered "Confidential Information" and are covered by this policy. "Confidential Information" includes information in any form, such as written documents or records, or electronic data.

Each employee shall have the following responsibilities under this policy:

1. During employment and after the termination of employment, an employee will hold all Confidential Information in trust and confidence, and will only use, access, store, or disclose Confidential Information, directly or indirectly, as appropriate in the performance of the employee's duties for DSNLU. An employee must comply with all applicable to Central, State laws and DSNLU policies relating to access, use, and disclosure of Confidential Information.
2. An employee will not remove materials or property containing Confidential Information from the employee's department or program area unless it is necessary in the performance of the person's job duties. Any and all such materials, property, and Confidential Information are the property of DSNLU. If materials or property containing Confidential Information are removed from DSNLU, the employee must safeguard the materials/property and control access as necessary. This responsibility to safeguard and control access to materials and property similarly applies to any telework/remote access situation as provided in DSNLU policy

3. Upon termination of any assignment or as requested by an employee's supervisor, the employee will secure all such materials/property and copies thereof or return all such materials/property and copies to the employee's supervisor.
4. An employee will not seek to obtain any Confidential Information involving any matter which does not involve or relate to the person's job duties. Confidential Information or DSNLU records, documents, or other information may not be maliciously tampered with, altered, or destroyed.
5. In the case of a health or safety emergency, relevant Confidential Information may be disclosed as necessary to appropriate individuals, e.g., a counsellor, a supervisor.
6. If an employee has any question relating to appropriate use or disclosure of Confidential Information, the employee shall consult with the employee's supervisor or other appropriate University personnel.
7. Each employee must promptly report to the employee's supervisor any known violation of this policy, other DSNLU confidentiality or privacy policies, or Central State confidentiality or privacy laws, by the employee or a DSNLU student, faculty member or staff member.

Misuse of Electronic Communications

Electronic communications are essential in carrying out the activities of the university and to individual communication among faculty, staff, students, and their correspondents. However, electronic communication must follow all university policies and should be in support of the university's mission.

Key prohibitions include:

- Sending unsolicited messages, including unsolicited commercial email ("junk mail") or other advertising material, to individuals who did not specifically request such material, except as approved by the University.
- Engaging in harassment whether through language, imagery, frequency, or size of messages.
- Masquerading as someone else by using their email address, internet address, and/or electronic signature.
- Creating or forwarding anonymous, deceptive, fraudulent, or unwelcome electronic communications, such as chain letters or solicitations for business schemes.
- Using email originating from university-provided accounts for commercial or personal gain not related to University business.

- Sending or broadcasting email or other electronic communications from a university account for lobbying of public officials, or to solicit support for a candidate or ballot measure, or using emails in a concerted effort to support a candidate or ballot measure.

Enforcement

The Acceptable Use of Information Technology Resources policy is enforced through the following mechanisms. The Registrar may grant permission to conduct certain activities otherwise prohibited by this policy, such as for purposes related to the university's mission or to validate the confidentiality, integrity, or availability of university data.

Interim Measures

The university may temporarily disable service to an individual or a computing device, when an apparent misuse of university computing facilities or networks has occurred, and the misuse:

- Is a claim under the Information Technology Act 2000 (amended in 2008),
- Is a violation of criminal law, license agreement, or intellectual property rights,
- Has the potential to cause a loss of confidentiality, integrity, or availability of university IT resources,
- May cause significant harm to another person and/or,
- May result in liability to the university.

The person responsible for any account or equipment to be disabled as an interim measure will be informed as soon as possible so that they may present reasons why their use is not a violation or that they have authorization for the use. However, some actions may be sealed for law enforcement or court orders.

Disciplinary Action

Violations of this policy may be referred for disciplinary action as outlined in the below and applicable staff and faculty employment policies. The university may assess a charge to offset the cost of the incident. In extreme cases, legal action may be prudent and necessary.

Suspension of Services and Other Action

Users may be issued warnings, may be required to agree to conditions of continued service, or may have their privileges suspended or denied if:

- After hearing the user's explanation of the alleged violation, an IT Committee has made a determination that the user has engaged in a violation of this policy, or
- A student or employee disciplinary body has determined that the user has engaged in a violation of the policy.

Usage of Terms

AVAILABILITY – Availability is the ability to assure that systems work promptly and service is not denied to authorized users. A loss of availability is the disruption of access to or use of information or an information system.

CONFIDENTIALITY – Confidentiality ensures that confidential information is only disclosed to authorized individuals. A loss of confidentiality, for the purposes of this policy, is the unauthorized disclosure of information.

INTEGRITY – Integrity is the appropriate maintenance of information and systems. A loss of integrity is the unauthorized modification or destruction of information.

IT RESOURCE—IT resource may include computers, software, servers, network utilization, storage utilization, virtual machine capacity, tablets, phones, multimedia devices, storage devices, wireless spectrum, and any other in-demand resource managed by IT staff.

POTENTIAL IMPACT - Potential impact is the level of adverse effect a loss of confidentiality, integrity, or availability could be expected to have on university operations, university assets, or individuals.

UNIVERSITY— University is the Damodaram Sanjivayya National Law University.

UNIVERSITY DATA – University data are information that supports the mission and operation of the university. It is a vital asset and is owned by the university.

USER—User includes any faculty, staff, student, developer, contractor, vendor, or visitor as well as any other individual or entity using information and IT resources at DSNLU.

Email Account Use Policy of Damodaram Sanjivayya National Law University (DSNLU)

In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the University's administrators, it is recommended to utilize the university's e-mail services, for formal University communication and for academic & other official purposes. E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal University communications are official notices from the University to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general University

messages, official announcements, etc. To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging on with their User ID and password. For obtaining the university's email account, user may contact IT Department for email account and default password by submitting an application in a prescribed proforma.

Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

1. The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.

2. Using the facility for illegal/commercial purposes is a direct violation of the university's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.

3. While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.

4. User should keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox all most full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.

5. User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer; as such messages may contain viruses that have potential to damage the valuable information on your computer.

6. Users should configure messaging software (Outlook Express/Netscape messaging client etc.,) on the computer that they use on permanent basis, so that periodically they can download the mails in the mailbox on to their computer thereby releasing the disk space on the server. It is user's responsibility to keep a backup of the incoming and outgoing mails of their account. 7. User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.

8. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.

9. While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.

10. Impersonating email account of others will be taken as a serious offence under the university IT security policy.

11. It is ultimately each individual's responsibility to keep their e-mail account free from violations of university's email usage policy.

University Database (of e-Governance) Use Policy

This Policy relates to the databases maintained by the university administration under the university's e-Governance. Data is a vital and important University resource for providing useful information. Its use must be protected even when the data may not be confidential. DSNLU has its own policies regarding the creation of database and access to information and a more generic policy on data access. Combined, these policies outline the university's approach to both the access and use of this university resource.

A. **Database Ownership:** DSNLU is the data owner of all the University's institutional data generated in the university.

B. **Custodians of Data:** Individual Sections or departments generate portions of data that constitute University's database. They may have custodianship responsibilities for portions of that data.

C. Data Administrators: Data administration activities outlined may be delegated to some of the officers in that department by the data Custodian.

Here are some general policy guidelines and parameters for Sections, departments and administrative unit data users:

1. The university's data policies do not allow the distribution of data that is identifiable to a person outside the university.

2. Data from the University's Database including data collected by departments or individual faculty and staff, is for internal university purposes only.

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

4. Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the Office of the University Registrar.

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

6. At no time may information, including that identified as ‘Directory Information’, be released to any outside entity for commercial, marketing, solicitation or other purposes.

This includes organizations and companies which may be acting as agents for the university or its departments.

7. All reports for UGC, MHRD and other government agencies will be prepared/compiled and submitted by the Registrar, Director Academic Affairs, Controller of Examinations and Finance officer of the University.

8. Database users who repackage data for others in their unit must inform the recipients of the above data access issues.

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

- Modifying/deleting the data items or software components by using illegal access methods.
- Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ departments.

- Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.

- Trying to break security of the Database servers. Such data tampering actions by university member or outside members will result in disciplinary action against the offender by the university authorities. If the matter involves illegal action, law enforcement agencies may become involved.