

**National-Louis University Policy on Acceptable Use of NLU Information Systems
AP: 305 (030100)**

Approved: Senate Academic Technology Committee

Date: May 11, 1999

Approved: Faculty Senate

Date: May 19, 1999

Approved: Senior Cabinet and President

Date: March 1, 2000

EFFECTIVE DATE: March 1, 2000

National-Louis University provides resources to the University community (which includes all NLU students, staff, faculty, board members, alumni, and administrators) through its Information Systems and services (as defined in Guidelines for Users of Information Systems in the National-Louis University Community). NLU is responsible for providing University community members with Information Systems and services adequate to support the mission of the University. NLU is accountable to University community members for providing Information Systems and services adequate to support the goals and objectives of the University.

Use of Information Systems and services must be consonant with the mission, goals, and objectives of the University. Therefore, NLU community members are responsible for their activities and accountable for their individual conduct while using NLU Information Systems and services.

The NLU Community Acceptable Use Policy outlines those responsibilities and provides a framework for accountability for appropriate use of the University Information Systems and services.

NLU Community Members

1. Are responsible for abiding by United States copyright and intellectual property laws applicable to computer-accessible materials.
2. Are responsible for using information resources for educational, instructional, service, research, administrative, and other purposes consistent with their roles in the University community.
3. Are responsible for respecting the integrity of NLU. Information Systems and services, including refraining from activities to gain unauthorized access to or use of University Information Systems and services or software, which are intended to circumvent security measures.
4. Are responsible for conducting themselves in a professional and ethical manner in all communications conducted via the University Information Systems.

The above policy will be implemented according to the “Guidelines for Implementation of National-Louis University Community Policy on Acceptable Use of NLU Information Systems.”

Guidelines for Implementation of National-Louis University Community

Policy on Acceptable Use of NLU Information Systems

Definitions

National-Louis University Information Systems refers to all computers and Information Systems owned or operated by NLU and include: hardware, software, data, communication networks associated with these systems and services. These systems range from multi-user systems to single-user terminals and personal computers, whether freestanding or connected to networks.

System users are all those individuals with privileges to use NLU computing systems and services; including but not limited to students, faculty, University staff and administrative officers.

Deans and Vice Presidents with the assistance of System Administrators will determine who is permitted access to a particular system. System Administrators and other designated system users hold responsibility for the maintenance and security of NLU Information Systems as a part of their stated responsibilities as academic or non-academic employees. System Administrators report directly to the Collegis/NLU Technical Director. The Collegis/NLU Technical Director directly reports to the Collegis/NLU Executive Director who reports directly to the University President’s designee. The Collegis/NLU Executive Director holds ultimate responsibility for the maintenance and security of NLU Information Systems.

1. Adherence to Laws Governing Ownership and Copyright Law

Users must observe intellectual property rights including, in particular, copyright laws as they apply to software and electronic forms of information.

Users may use only legally obtained, licensed data, or software in compliance with license or other agreements and federal copyright and intellectual property laws.

Users shall not place copyrighted material (software, images, music, movies, etc.) on any NLU computer without prior permission from the copyright holder or as granted in a license agreement or other contract defining use.

2. Authorized Use

Individuals using NLU Information Systems and services must be identified either through the physical location of an office or instructional computer or through an authorized NLU computer account, as with multiple user systems. System users may not access or use another user’s computer account or allow another person to use his or her account.

System Administrators create accounts and regulate access to NLU Information Systems by authorized system users.

System Administrators privileges are granted only for official purposes and under the authority of designated academic and administrative officers. Unauthorized usage or assignment of administrative privileges is expressly prohibited.

Users must not conceal their identity when using NLU systems, except when anonymous access is explicitly provided (as with anonymous ftp).

NLU computing systems and services may not be used as a means of unauthorized access to computing accounts or systems inside of or outside of NLU's Information Systems.

Other users of NLU Information Systems may be permissible including revenue generating activities subject to policies and procedures governing contractual agreements.

3. Privacy

All access to protected information stores in NLU records systems will be in strict compliance with the provisions of Federal and State laws. The Family Educational Rights and Privacy Act (FERPA) or "Buckley Amendment" (34 C.F.R. Part 99, as amended by 61 Fed. Reg. 59291 Nov. 21, 1996) provides for protection against unwarranted disclosure of private information contained in "official" University records. FERPA guarantees all postsecondary students the right to consent to disclosures of personally identifiable information contained in student education records, except to the extent that FERPA authorizes disclosure without consent see <http://www.edlaw.net>.

Computer users must respect the privacy of others by refraining from inspecting, broadcasting, or modifying data files without the consent of the individual or individuals involved. Administrative users may inspect or repair data files (including e-mail stores on NLU mail systems) as required as part of their employment, and then only to the extent necessary to maintain the integrity and operations of NLU systems.

University employees and others may not seek out, examine, use, modify, or disclose, without authorization, personal or confidential information contained in a computer, which they access as part of their job function.

Employees must take necessary precautions to protect the confidentiality of personal or confidential information encountered in the performance of their duties.

Use of Internet Systems (IP) to transmit information does not guarantee privacy and confidentiality. Sensitive material transferred over Information Systems (including e-mail and World Wide Web) may be at risk of detection by a third party. Users should exercise caution and care when transferring such material in any form.

4. Malicious and Destructive Uses of NLU Information Systems

The following uses of NLU computers and Information Systems are specifically prohibited:

- a. Use of computer programs to decode passwords or access control information.
- b. Attempts to circumvent or subvert system or network security measures.
- c. Engaging in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files or making unauthorized modifications to University data.
- d. Wasting computing resources or network resources; for example, by intentionally placing a program in an endless loop, printing excessive amounts of paper, or by sending chain-letters or unsolicited mass mailings.
- e. Using mail or messaging services to harass, libel, intimidate, or distribute misinformation, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted mail, or by using someone else's name or user ID.
- f. Users must not access or attempt to access data on any system they are not authorized to use. Users must not intercept or attempt to intercept data communications not intended for that user's access, for example, by "promiscuous" bus monitoring or wiretapping.

5. Enforcement

Authorized System Administrators may monitor computer activity for the sole purpose of maintaining system performance, security, and integrity. In instances when individuals are suspected of violating policies, the contents of user files may be inspected only upon the approval of the University officer having clear responsibility for the activity of the user.

At the discretion of the System Administrator(s) responsible for the resource or service in question, in collaboration with the appropriate administrative authority, information system computer use privileges may be temporarily or permanently revoked, following due process appropriate for the parties involved, pending the outcome of an investigation of misuse, or finding substantiating violations of these guidelines.

6. Due Process

NLU Information System users have the right to due process (consistent with respective policies governing the categories of users) in cases of discipline resulting from violations of the guidelines outlined in this document.

When a System Administrator believes it necessary to preserve the integrity of facilities, user services, or data, he or she may suspend any account, whether or not the account owner (the user) is suspected of any violation. Where practical, 24-hour notice will be given in advance of revocation.

If, in the judgment of the Systems Administrator, the violation warrants action beyond a System Administrator's authority, he or she will refer the case first to the University administrator or disciplinary body appropriate to the violator's status (e.g., in the case of a faculty member, his/her dean), and, as deemed appropriate, to a law enforcement authority.

An NLU Information System user accused of a violation will be notified of the charge and have an opportunity to respond (consistent with respective policies governing the categories of users) before a final determination of a penalty. If a penalty is imposed, the accused violator may request a review by the designated administrator or body empowered to assure due process and an impartial and timely review of the charges.

Bibliography

Software Publishers Association. 1998. SPA's Recommended University Internet Usage Policy. <http://www.spa.org/piracy/highered/univguide.html>.

The George Washington University. 1999. Code of Conduct for Users of Computer Systems at The George Washington University. <http://www.gwu.edu/~circ/docs/cofc.html>.

Virginia Tech. 1998. Acceptable Use of Information Systems at Virginia Tech. <http://www.vt.edu/vt97/misc/policies/acceptuseguide.html>.

Yale University. 1998. Information Technology Services: Appropriate Use Policy. http://www.yale.edu/policy/policy_doc.html.

Note: National-Louis University supports the EDUCAUSE Code of Software and Intellectual Rights. Users should consider the EDUCAUSE Code as a standard to guide their ethical use of electronic resources and information: respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applied to works of all authors and publishers in all media. It encompasses respect for the right acknowledgement, right to privacy, and right to determine the form, manner, and terms of publication and distribution.

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community. (See "Using Software: A Guide to the Legal and Ethical Use of Software for Members of the Academic Community," Educom/ITAA, 1992. www.educom.edu/web/pubs/usingsoftware.html.)