

# National-Louis University Community Acceptable Use of NLU Information Technology

*Approved by Senate Academic Technology Committee - May 11, 1999  
Amended & Approved by Faculty Senate - May 19, 1999  
Approved for Implementation by Senior Cabinet and President-March 1, 2000  
Revisions approved by the University Technology Council December 2003  
Revisions approved by University Counsel, January 2003  
Approved for Implementation by President, January 23, 2004*

**Purpose:** The NLU Acceptable Use Policy outlines user responsibilities and provides a framework for accountability for appropriate use of the University information technology and services.

**Policy:** National-Louis University provides resources to the university community (which includes all NLU prospective students, students, staff, faculty, board members, alumni, and administrators) through its information technology and services (defined as “NLU IT systems”, which include all hardware, software, networks, communications systems, data and other related technologies owned, leased, or licensed by National-Louis University, its partners and affiliates, that are available for use by the NLU community).

The use of NLU IT systems is a privilege and not a right. Inappropriate use may result in the cancellation of that privilege.

Use of NLU IT systems must be consonant with the mission, goals, and objectives of the university. NLU community members are responsible for their activities and accountable for their individual conduct while using NLU IT systems or engaging in NLU-related activities.

## NLU Community Members:

1. Are responsible for abiding by all laws applicable to their use of NLU IT systems. This includes but is not limited to those dealing with copyright, trademark, patent, privacy, and intellectual property. [Only licensed software allowed. Fair Use policy must be adhered to.]
2. May use NLU IT systems for educational, instructional, service, research, administrative, and other purposes consistent with their roles in the university community. Incidental personal use of NLU IT systems is allowed if (a) it does not interfere with the operations of any NLU IT system, as determined by any IT professional staff member, and (b) it does not interfere with the job performance of staff or faculty, as determined by the individual’s supervisor. [May not overload the system or detract from time spent “on the job”]
3. May not use NLU IT systems for commercial activity (other than NLU sponsored and authorized activities). May not use NLU IT systems for political, religious or other advocacy purposes unless related to the academic expertise and responsibilities of a faculty member.
4. Must refrain from activities to gain unauthorized access to or use of NLU IT systems, and any activities which would interfere with the normal operations of NLU IT systems. [No “hacking” allowed.]
5. Are responsible for observing secure computing practices and protecting the integrity of data and systems. [Maintain password security; log off systems when appropriate.]
6. Are responsible for conducting themselves in a professional and ethical manner in all communications conducted via NLU IT systems.

7. May not use NLU I.T. systems to transmit

- a. threatening, or harassing material;
- b. obscene or pornographic material (Faculty involved in research or teaching that requires reference to such material are advised to inform their Dean in advance that such material will be utilized. Faculty are also advised to prepare their students to handle such material.) or;
- c. any NLU proprietary or confidential information to any individual or group not authorized to view such information. [See Banner Confidentiality Agreement for details. The document is at <http://oit.nl.edu/documents/NLUBannerAccess092002.pdf>.]

NLU IT 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 this policy.

The contents of NLU IT systems are owned by National-Louis University, with the exceptions of any content specifically covered by NLU intellectual property agreements or contractual obligations.

Refer to the “Procedures for Implementation of National-Louis University Policy on Acceptable Use of NLU Information Systems” for procedures related to this policy.

# **Procedures for Implementation of National-Louis University Policy on Acceptable Use of NLU Information Systems**

## **Definitions:**

“Users” are all those individuals with privileges to use NLU IT systems. This includes faculty, students, staff, alumni, trustees, visitors and the general public.

## **1. Adherence to Laws Governing Ownership and Copyright Law**

Users must observe intellectual property rights including, in particular, copyright, trademark and property laws as they apply to software and electronic forms of information. Example: users may not copy entire works or significant portions of a work from an NLU IT system unless they have written permission of the owner (copyright holder).

Users may use only legally obtained, licensed data or software in compliance with license or other agreements and federal copyright and intellectual property laws and the NLU copyright policy. Example: every copy of software installed on every NLU IT system must be licensed. It is the Information Technology Department’s responsibility to assure that all software they install is licensed. It is the individual user’s responsibility to determine that all copies of software s/he installs are properly licensed. Assume that software is licensed for use on a single machine unless otherwise specifically noted in the purchase/license agreement.

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. Example: users may not place entire works or significant portions of a work onto an NLU IT system unless they have written permission of the owner (copyright holder) or have a license allowing them to use that software or material.

Failure to abide by these laws exposes the individual user to sanctions by both NLU and the respective federal enforcement agency. Example: violations of copyright law by copying software may result in discipline by NLU and personal civil liability for each count of purposive, willful or wanton disregard for the federal copyright laws. The violator may face fines and may be responsible for the payment of mandatory statutory attorney’s fees of the plaintiff.

## **2. Authorized Use**

- a) Use of NLU IT systems is based on the individual’s role and responsibilities within the NLU community. The individual’s supervisor and Vice President or Provost authorize the establishment of the appropriate accounts and access privileges for each user or class of users. Example: what information you have access to depends on the needs of your job at NLU and not on your personal curiosity.
- b) Unauthorized usage or assignment of account privileges is expressly prohibited. Example: you may not use an account that has access privileges to information not needed in your job. A Systems Administrator may not assign to you access rights not required for your job.
- c) System users may not access or use another user’s computer account or allow another person to use his or her account. Example: do not utilize any other person’s account.

- d) Users must not conceal their identity when using NLU systems, except when anonymous access is explicitly provided (as with anonymous ftp). Example: some software allows users to send anonymous emails, survey responses or votes.
- e) NLU IT systems may not be used as a means of unauthorized access to computing accounts or systems. Example: Using your NLU account to hack (break into) an account on another university's system.

### 3. Privacy

All access to protected information stored in NLU records systems will comply with the provisions of Federal and State laws. The Family Educational Rights and Privacy Act (FERPA, also known as the "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 student education records. See Banner Confidentiality Agreement for details. The document is posted at <http://oit.nl.edu/documents/NLUBannerAccess092002.pdf>.

Users may not inspect, broadcast, or modify data files without the consent of the individual or individuals specifically charged with creating and maintaining those data, unless such activities are part of the user's job duties.

Users must exercise reasonable judgment when forwarding email or files that may be confidential or contain sensitive information. Such information may not be forwarded or otherwise distributed to individuals or groups unless the user knows the recipients are authorized to access such information.

Administrative users (Information Technology staff or other staff members responsible for maintaining data quality) may inspect or repair data files (including e-mail stored 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.

Users may not seek out, examine, use, modify, or disclose, without authorization personal or confidential information contained in any NLU I.T. system. Employees must take necessary precautions to protect the confidentiality of personal or confidential information encountered in the performance of their duties.

NLU retains the unfettered right to view any information in any NLU I.T. System.

### 4. Malicious and Destructive Uses of NLU information systems.

Users may not vandalize or physically abuse any NLU IT system.

Uses of NLU IT systems specifically prohibited include but are not limited to:

- a) Using or attempting to use computer programs to decode passwords or other access control information.
- b) Circumventing or attempting 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 email or messaging services (such as AOL Instant Messenger) to harass, libel, intimidate, or distribute misinformation, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted email or instant messages, or by using someone else's name or user ID.
- f) Accessing or attempting to access data on any system they are not authorized to use. [If a user receives a message that s/he is not authorized to access an account or specific data, s/he should immediately cease trying to gain access. If s/he believes they need that access to fulfill his/her job responsibilities s/he should contact his/her supervisor to gain access rights.]
- g) Making or attempting to make any deliberate, unauthorized changes to data on an NLU system. [Example: Banner Student System users may not change personal data such as address or date of birth of any NLU employee's record.]
- h) Intercepting or attempting to intercept data communications not intended for that user's access, for example, by "promiscuous" bus monitoring, wiretapping, keystroke monitoring or other methods. [There are dozens of software and hardware techniques for spying on computer users. None of these may be used on NLU IT systems with the exception of use by NLU Information Technology administrators investigating violations of the NLU Acceptable Use Policy.] Additionally, such activity is a violation of federal law and violators are subject to prosecution.

## 5. Security and Data Integrity – User Responsibilities

Users must observe secure computing practices. Practices vary by user category or machine type.

- a) All Users, all NLU IT Systems:
  - i) Maintain password security according to current NLU password protocol for each user group or system. [Use a non-obvious password; do not leave a written copy of your password in plain view; do not share your password with other users.]
  - ii) Implement standard anti-virus practices ("virus" refers to the entire group of destructive software including but not limited to viruses, worms and Trojans), which include but are not limited to exercising reasonable judgment about handling email and other files that are likely virus carriers. [Do not open email or email attachments that come from unknown sources or that have unexpected subject headings or that show evidence of multiple forwardings.]
  - iii) May not install "Spy-ware", unlicensed software, password cracking software, hacking tools on NLU owned equipment or utilize any such software while using any NLU information system (this includes but is not limited to use of internet access provided by NLU from a user's personal or other non-NLU equipment).
  - iv) May not install any unauthorized or "rogue" networking components. (i.e. hubs, switches, servers, or wireless access points or other devices). Any unauthorized networking components identified by the Office of Information Technology will be removed immediately and reported to the CIO and corresponding Vice President or Dean of the person who installed it.

- b) Individually assigned and individually managed workstations (PC, MAC or other similar systems typically used by the same staff, faculty or student on a regular basis):
  - i) The same requirements stated in paragraph “5 a)” plus:
  - ii) Frequently (recommendation is weekly) update anti-virus software files (anti-virus software is installed on all NLU IT systems issued to end users; updates are available from the manufacturer’s web site). [Be certain that NLU’s current anti-virus software is installed on your PC/Mac. Be certain that it is operational (ask for assistance in the case that you are uncertain).]
  - iii) Backing up all NLU data files on a regular and frequent basis. “Backing up” means that files are saved to at least two separate physical locations and media. Examples would include (preferred) saving files to a network drive (known as H: or I: drives for non-MAC systems) which in turn are saved to a tape drive on a regular basis by an IT staff member, or saving files to the individual machine’s hard drive and making a copy of the files onto a floppy disk, zip disk, or CD.
- c) Public and centrally managed systems: these include end user workstations that are open to use by any NLU user (computing labs, library, Win Terminals, etc.)
  - i) The same requirements stated in paragraph “5 a)” plus:
  - ii) Anti-virus file updates: are handled by the Information Technology or other technology specialist staff assigned to manage these machines. Users of these public or centrally managed machines are specifically not allowed to install any software, including anti virus files.
  - iii) Backups: data files are not to be stored on public machines. Users will need to store data files on either network drives or removable media (floppy or zip disks). Users relying on removable media are expected to make copies of the removable media as their backup mechanism.

## 6. Security and Data Integrity – Information Technology Responsibilities

To support the academic, research and business operations of NLU, the Information technology staff:

- a) Will operate an industry standard backup process for all Information Technology-maintained servers and network drives.
- b) Will implement strong password security on all systems owned or maintained by the University.
- c) Will allow all data traffic destined for sources outside the University’s network so long as it is in support of the University’s processes and functions.
- d) Will provide access to the services required by NLU community members to complete their job function.
- e) Will actively maintain the highest level of data protection methods allowable with the provided resources. (i.e. Anti-virus software, firewalls, and physical security)
- f) Will deny any traffic identified as malicious, dangerous or otherwise harmful to the University’s data infrastructure, whether its source is inside or outside the University’s network.
- g) Will remove any networking hardware or software not installed and supported by or with the permission of the Office of Information Technology

## 6. Enforcement

While NLU retains the right to access all data on any NLU system, it imposes protocols on such access during normal operations.

Information Technology staff members who have responsibility for network security may utilize various software and/or hardware tools designed to locate and identify software, hardware, and user actions that pose threats to NLU Technology Resources and/or NLU Information. Information Technology staff may not utilize such tools for any other purpose. Any user information derived from security investigations is confidential and is shared only with individuals directly involved in the investigation of any alleged security violation.

In instances when individuals are suspected of violating policies, the contents of user files may be inspected only:

- a) At the request of the user's supervisor and the concurrence of the Vice President of H.R. (staff) or Provost (faculty) or VP of Enrollment Management (students).
- b) When a Systems Administrator has reasonable cause to believe that a user's activities pose a significant operational or security problem and has the concurrence of the CIO.
- c) When requested by NLU legal counsel or the NLU President
- d) In accordance with a subpoena.

At the discretion of the System Administrator or the appropriate Vice President or the Provost, NLU IT system use privileges may be temporarily suspended, pending the outcome of an investigation of misuse.

The determination that a user has violated the NLU Acceptable Use Policy may result in disciplinary action up to and including termination of employment or dismissal from the university.

## **7. Due Process**

### **a. General Public**

Users who are members of the general public (are not employees or students of NLU) who violate the NLU Acceptable Use Policy may be reported to the appropriate law enforcement authorities.

### **b. NLU Employees and Students**

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 NLU Acceptable Use Policy.

When a Systems Administrator reasonably believes it necessary to preserve the integrity of NLU IT systems, 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 suspension.

Violations of the Acceptable Use Policy identified by any member of the Information Technology staff will be reported to the user's supervisor and to the CIO. If appropriate, violations may also be reported to NLU counsel and/or law enforcement authorities.

A 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.



Curtis L. McCray  
President

1/28/04  
Date