



# **Policy for Responsible Use of University Computers and Information Systems**

## **Authority**

This Policy is pending review by legal counsel and the approval of the President of Alliant International University.

## **Policy Statement**

Users of Alliant International University network and computer resources have a responsibility not to abuse the network and resources and to respect the rights of others. This policy provides guidelines for the appropriate and inappropriate use of information technologies.

## **1. Policy Purpose**

The purpose of the Policy for Responsible Use of University Computers and Information Systems is to ensure an information infrastructure that promotes the basic missions of Alliant International University in teaching, learning, and research. Computers and networks are powerful enabling technologies for accessing and distributing the information and knowledge developed at the University and elsewhere. As such, they are strategic technologies for the current and future needs of the University. Because these technologies give individuals the ability to access and copy information from remote sources, users must be mindful of the rights of others to their privacy, intellectual property, and other rights. This Responsible Use Policy details what is considered appropriate usage of computers and networks with respect to the rights of others.

Access to the information systems at Alliant International University is a privilege, not a right, and with this privilege come specific responsibilities outlined in this Policy. Accepting any account and/or using Alliant International University information systems shall constitute an agreement on behalf of the user or other individual accessing such information systems to abide and be bound by the provisions of this Policy.

The University may restrict or prohibit the use of its information systems in response to complaints presenting evidence of violations of University policies or state or federal laws. When it has been determined that there

has been a violation, the University may restrict or prohibit access by an offending party to its information systems through University-owned or other computers, remove or limit access to material posted on University-owned computers or networks, and, if warranted, institute other disciplinary action.

## 2. Policy Summary

Users of Alliant International University information systems must respect software licenses, adhere to copyright laws of all electronic files and media, respect the integrity of computer-based information resources, refrain from seeking to gain unauthorized access, and respect the rights of other computer users. This Policy covers appropriate and inappropriate use of computers, networks, and information contained therein.

## 3. Definitions

For purposes of this policy the following definitions shall apply:

- a. **Electronic Communications** -- Shall mean and include the use of information systems in the communicating or posting of information or material by way of electronic mail, bulletin boards, World Wide Web (Internet), or other such electronic tools.
- b. **Information Systems** -- Shall mean and include computers, networks, servers and other similar devices that are administered by the University and for which the University is responsible. "Networks" shall mean and include data, voice and video networks, routers, switches, and storage devices.
- c. **Obscene** -- With respect to obscene material shall mean (1) that an average person applying contemporary community standards would find the material taken as a whole predominantly appeals to the prurient interest or a shameful or morbid interest in nudity, sex, or excretion, (2) the material depicts or describes in a patently offensive way sexual conduct, and (3) the material taken as a whole lacks serious literary, artistic, political, or scientific value.
- d. **Senior Management** -- This group is comprised of the President, Vice President, Provost and Deans. Supervisors and Program Directors shall report any violations to this policy to Senior Management.

## 4. Permitted Use

- a. University Business Use and Limited Personal Use.** University information systems are to be used predominately for University-related business. However, personal use is permitted so long as it conforms to this Policy and does not interfere with University operations or a user's performance of duties as a University employee. Personal use of any University information system to access, download, print, store, forward, transmit or distribute obscene material is prohibited. Under all circumstances, personal use of information systems must comply with **subsection b.** of this section and shall not conflict with any performance of duties and responsibilities for the University. Personal use may be denied when such use requires an inordinate amount of information systems resources.
- b. Prior Approval Required for Personal Use for Outside Consulting, Business or Employment.** Personal use of University information systems by any user for personal financial gain in connection with outside (non-University) consulting, business or employment is prohibited, except as authorized by the Senior Management. Employee personal use in conjunction with outside professional consulting, business or employment activities is permitted only when such use has been expressly authorized and approved by Senior Management.

## **5. Access**

Unauthorized access to information systems is prohibited. No one should use the ID or password of another; nor should anyone provide his or her ID or password to another, except in the cases necessary to facilitate computer maintenance and repairs. When any user terminates his or her relation with Alliant International University, his or her ID and password shall be denied further access to University computing resources.

## **6. Misuse of Computers and Network Systems**

Misuse of University information systems is prohibited. Misuse includes the following:

- a.** Attempting to modify or remove computer equipment, software, or peripherals without proper authorization.
- b.** Accessing without proper authorization computers, software, information or networks to which the University belongs, regardless of whether the resource accessed is owned by the University or the abuse takes place from a non-University site.

- c.** Taking actions without authorization, which interfere with the access of others to information systems.
- d.** Circumventing logon or other security measures.
- e.** Using information systems for any illegal or unauthorized purpose.
- f.** Personal use of information systems or electronic communications for non-University consulting, business or employment, except as expressly authorized by Senior Management.
- g.** Sending any fraudulent electronic communication.
- h.** Violating any software license or copyright, including downloading, copying or redistributing copyrighted software, without the written authorization of the software owner.
- i.** Using electronic communications to violate the property rights of authors and copyright owners. (Be especially aware of potential copyright infringement through transmission or downloading of copy written materials such as audio and music (mp3 etc), videos and movies (avi etc)).
- j.** Using electronic communications to harass or threaten users in such a way as to create an atmosphere that unreasonably interferes with the education or the employment experience. Similarly, electronic communications shall not be used to harass or threaten other information recipients, in addition to University users.
- k.** Using electronic communications to disclose proprietary information without the explicit permission of the owner.
- l.** Reading other users' information or files without permission.
- m.** Academic dishonesty.
- n.** Forging, fraudulently altering or falsifying, or otherwise misusing University or non-University records (including computerized records, permits, identification cards, or other documents or property).
- o.** Using electronic communications to hoard, damage, or otherwise interfere with academic resources available electronically.
- p.** Using electronic communications to steal another individual's works, or otherwise misrepresent one's own work.

- q. Using electronic communications to fabricate research data.
- r. Launching a computer worm, computer virus or other rogue program.
- s. Downloading or posting illegal, proprietary or damaging material to a University computer.
- t. Transporting illegal, proprietary or damaging material across a University network.
- u. Personal use of any University information system to access, download, print, store, forward, transmit or distribute obscene material.
- v. Violating any state or federal law or regulation in connection with use of any information system.

## 7. Privacy

- a. **User Data and Email Privacy Not Guaranteed.** When University information systems are functioning properly, a user can expect the files and data he or she generates to be secure information, unless the creator of the file or data takes action to reveal it to others. Users should be aware, however, that no information system is completely secure. Persons both within and outside of the University may find ways to access files. Accordingly, Alliant International University cannot and does not guarantee user privacy and users should be continuously aware of this fact.
- b. **Repair and Maintenance of Equipment.** Users should be aware that on occasion duly authorized University information systems technological personnel have authority to access individual user files or data in the process of performing repair or maintenance of computing equipment the University deems is reasonably necessary, including the testing of systems in order to ensure adequate storage capacity and performance for University needs. Information systems technological personnel performing repair or maintenance of computing equipment are prohibited by law from exceeding their authority of access for repair and maintenance purposes or from making any use of individual user files or data for any purpose other than repair or maintenance services performed by them.

- c. **Response to a Public Records Request, Administrative or Judicial Order or Request for Discovery in the Course of Litigation.** Users should be aware that the California public records statutes are very broad in their application. Certain records, such as unpublished research in progress, proprietary information, personal information in personnel and student records are protected from disclosure. However, most other University records contained in electronic form require disclosure if a public record request is made. Users should remember this when creating any electronic information, especially e-mail. Also, users should be aware that the University will comply with any lawful administrative or judicial order requiring the production of electronic files or data stored in the University's information systems, and will provide information in electronic files or data stored in the University's information systems in response to legitimate requests for discovery of evidence in litigation in which the University is involved. The Information Technology department will not release any electronic information unless it is formally requested by the University, Human Resources or Legal Department.
- d. **Response to Misuse of Computers and Network Systems.** When for reasonable cause, as such cause may be determined by the Office of the President and General Counsel, it is believed that an act of misuse as defined in **section 6** above has occurred, then the Chief Information Officer or a designated information system administrator serving the relevant campus may access any account, file or other data controlled by the alleged violator and share such account information, file or other data with those persons authorized to investigate and implement sanctions in association with the misuse of the University's computer and information systems. Should The Chief Information Officer or the designated information system administrator reasonably believe that a misuse is present or imminent such that the potential for damage to the system or the information stored within it, is genuine and serious (e.g. hacking, spamming or theft), then the Chief Information Officer may take such action as is necessary to protect the information system and the information stored in it, including the denial of access to any University or non-University user, without a determination from the Office of the President and General Counsel regarding reasonable cause; provided however, that the Chief Information Officer shall contact the Office of the President and General Counsel as soon as possible to confirm that any protective actions taken were appropriate and within the parameters of this executive memorandum.

**e. Access to Information Concerning Business Operations.**

Employees regularly carry out the business functions of the University using the University's information systems. Business records, inquiries and correspondence are often stored such that individuals may control the access to particular information stored within the University's information system. Should any employee become unavailable, be incapacitated due to illness or other reasons, or refuse to provide the information necessary to carry out the employee's job responsibilities in a reasonably timely manner, then following consultation with the Department head, a formal request will be sent to the Information Technology department to carry out University business operations on behalf of the unavailable or uncooperative employee.

## **8. E-Mail**

- a.** The purpose of this policy is to ensure the proper use of Alliant International University's e-mail system by its students, faculty, and staff. Electronic Mail is a tool provided by the University to complement traditional methods of communications and to improve education and administrative efficiency. Users have the responsibility to use this resource in an efficient, effective, ethical and lawful manner. Use of the University's e-mail system evidences the user's agreement to be bound by this policy. Violations of the policy may result in restriction of access to the University e-mail system and/or other appropriate disciplinary action.
- b.** The University owns all e-mail accounts and all data transmitted or stored using Alliant e-mail capabilities.
- c.** While incidental personal use of e-mail is acceptable, conducting business for profit using University resources is forbidden.
- d.** While the University will make every attempt to keep e-mail messages secure, privacy is not guaranteed and users should have no general expectation of privacy in e-mail messages sent through the University System. Under certain circumstances, it may be necessary for the Information Technology staff or other appropriate University officials to access e-mail files to maintain the system, to investigate security or abuse incidents or violations of this or other University policies. Such access will be on an as needed basis and any e-mail accessed will only be disclosed to those individuals with a need to know or as required by law.
- e.** Individuals are responsible for saving e-mail messages, as they deem appropriate. Due to limited resources, the University IT department has the right to restrict the amount of user space on the e-mail server as necessary and to purge and remove e-mail accounts of students who have

not registered for the current or following Fall or Spring semester, or faculty and staff no longer employed by the University.

- f.** When using e-mail as an official means of communication, students, faculty and staff should apply the same professionalism, discretion, and standards that they would use in written business communication. Furthermore, students, faculty and staff should not communicate anything via e-mail that they would not be prepared to say publicly.
- g.** Students, faculty and staff may not disclose University information in e-mail that they are privileged to access because of their position at the University.
- h.** Approval and transmission of e-mail containing essential University announcements to students, faculty, and /or staff must be obtained from the appropriate authority. Only the Offices of Director, Dean, Executive Director, Vice President, or President may authorize the sending of broadcast messages to system group e-mail accounts of students, faculty, and staff within the scope of their authority.
- i.** The Department of Information Technology maintains the University's official e-mail system; faculty, staff and students are expected to read e-mail on a regular basis. Faculty, staff, or students who choose to use another e-mail system are responsible for receiving University-wide broadcast messages and personal mail by checking the University's official e-mail system, newsgroups, and the University's World Wide Web Homepage. An e-mail message regarding University matters sent from an administrative office, faculty, or staff member is considered to be an official notice.
- j.** Any inappropriate e-mail, examples of which are described below and elsewhere in this policy, is prohibited. Users receiving such e-mail should immediately contact the Dean of Students, Program Director, Faculty Advisor or Supervisor as appropriate. They will then contact the appropriate university official in the Human Resources or Legal department.

  - The creation and exchange of any message that is harassing, obscene or threatening.
  - The unauthorized exchange of proprietary information or any other privileged, confidential sensitive information.
  - The creation and exchange of advertisements, solicitations, chain letters and other unofficial, unsolicited e-mail.
  - The creation and exchange of information in violation of any laws, including copyright laws, or University policies.

- The knowing transmission of a message containing a computer virus.
  - The misrepresentation of the identity of the sender of e-mail.
  - The use or attempt to use the accounts of others without their permission.
- k. E-mail Retention.** E-mail messages should be deleted once the information contained in them is no longer useful. When e-mail communications are sent, the e-mail information is stored in one or more backup files for the purposes of "disaster recovery", i.e. inadvertent or mistaken deletions, system failures. In order to provide for the recovery of deleted e-mail, while maintaining efficient use of storage capabilities, e-mail information on backup files shall be retained for a period of time not to exceed seven days.

## 9. Web Pages

The Creative Services Department may establish standards for those Web Pages considered as being "official" pages of the University. All official Web Pages shall contain the administrative unit's logo in the header and footer in order to identify it as an official Alliant International University Web Page. No other Web Pages shall be allowed to use Alliant International University logos without the express permission of the University.

Originators of all Web Pages using information systems associated with the University shall comply with University policies and are responsible for complying with all federal, state and local laws and regulations, including copyright laws, obscenity laws, laws relating to libel, slander and defamation, and laws relating to piracy of software.

Maintenance of all pages is the responsibility of their owners and the Creative Services Department has responsibility for overall navigation, branding and content approval. Program offices, departments, and student groups creating official pages are responsible for the timely updating of the text and images contained on those pages. An internal review should be done by each department on an annual basis (from August to September), as well as by the Creative Services Department, to ensure their content is up-to-date on the website.

Web Pages should include a phone number or e-mail address of the person to whom questions/comments may be addressed, as well as the most recent revision date.

## 10. Applications and Enforcement

This Policy applies to all academic and administrative units of Alliant International University. The Senior Management and each University campus is encouraged to provide supplemental policy guidance, consistent with this Policy, designed to implement the provisions herein.

Each University campus shall be responsible for enforcing this Policy in a manner best suited to its own organization. It is expected that enforcement will require cooperation between such departments as computer systems administration, human resources, legal, academic affairs and student affairs. Prior to any denial of access or other disciplinary action, a user shall be provided with such due process as may be recommended by the President's Office of the General Counsel.

## **11. Cognizant Office** – Department of Information Technology

Questions, concerns or additional information about this and any Department of Information Technology policy should be directed to the Information Technology Helpdesk at [helpdesk@alliant.edu](mailto:helpdesk@alliant.edu).

## **12. Related Policies**

- a. Web Policy**
- b. Anti-Spam, Anti-Virus Policy – add link**
- c. Computer Theft and Loss Policy – add link**
- d. Cellular Telephone Policy – add link**
- e. Policy Violation Procedure – add link**

Created and dated November 15, 2001

Revised and dated February 12, 2004

Revised and dated August 9, 2006

Revised and dated April 30, 2006