



## Albany State University Acceptable Use Policy

### Purpose

To provide the Albany State University community with a set of guidelines and standards governing the use of technology at Albany State.

### Policy

The University or University System owns all University information resources; use of such resources constitutes consent for Albany State University to monitor, inspect, audit, collect, and remove any information without permission or further notice. Students and personnel shall be trained in what use is acceptable and what is prohibited. Violators of this policy are subject to University disciplinary action as described in the university catalog and the student and employee handbooks. Offenders may also face state and federal sanctions stemming from non-compliance with this policy.

### Scope

This policy applies to all individuals associated with Albany State University (hereinafter referred to "ASU"), including, but not limited to

- faculty
- staff
- students
- alumni
- student assistants
- contractors
- temporary staff

### Terms

**Appropriate use** is defined as usage performed for furthering the mission of Albany State University.

### I. Introduction

The appropriate use and protection of all information systems and associated resources is expected from all users including faculty, students, employees, and visitors throughout the institution. All users of information systems resources are expected to comply with existing ASU policies and procedures and those of the University system. In addition, users are expected to honor copyrights and software licenses and comply with all federal and state laws including those prohibiting slander, libel, harassment and obscenity. Users must obey laws prohibiting the private use of state property. Information that is confidential by law, including educational, financial and medical records as well as Social Security numbers, must be protected.

Users must be aware that information stored or transmitted electronically (or via computer), including e-mail and facsimile, may be subject to disclosure under open records laws. Users should have no expectation of privacy for information stored or transmitted using ASU information resources except for records or other information that is confidential by law (i.e., educational records).



## II. **Designation and Responsibility of Representatives**

### **A. *The President shall be responsible for the following:***

- Ensuring appropriate and auditable security controls are in place.

### **B. *The President's Cabinet shall be responsible for the following:***

- Informing personnel of university policies on acceptable use of information resources.
- Ensuring that personnel under their supervision comply with these policies and procedures.
- Ensuring that persons conducting business with the university comply with these policies and procedures.

### **C. *The Chief Information Officer (CIO) or one of his/her designees shall be responsible for the following:***

- Ensuring the availability, integrity, and confidentiality of the university's information technology resources.
- Addressing violations of university policies on information technology resources.
- Interpreting university policies on information technology resources.
- Developing and maintaining the university's information resource security policies.
- Developing and disseminating awareness and training materials.
- Assuring compliance through compliance auditing.
- Reporting compliance findings.

### **D. *Vice President for Student Affairs shall be responsible for the following:***

- Informing current and new students of university policies on acceptable use of information resources.
- Ensuring that students comply with university policies and procedures.

### **E. *System Administrators and Data Custodians shall be responsible for the following:***

- Monitoring systems for accuracy, integrity, confidentiality, and availability.
- Maintaining and ensuring data backups of critical electronic information.
- Promptly reporting suspicion or occurrence of any unauthorized activity to the Chief Information Officer or his/her designees.

### **F. *All students and personnel shall be responsible for the following:***

- Abiding by official university policies on acceptable use of information resources.
- Promptly reporting suspicion or occurrence of any unauthorized activities to the Chief Information Officer or one of his/her designees.
- Reporting any unacceptable use of their user accounts, passwords, personal identification numbers, and tokens to the Chief Information Officer or one of his/her designees.



## II. **User Accountability**

- A. **General:** Use of university computer and communication resources is a privilege which is provided to support the University's scholarly, educational, and administrative activities. Information technology resources are limited, and should be used wisely and with consideration for the rights and needs of others. As an authorized user, you are responsible for the security and use of your computer and/or system accounts. You accept full responsibility for your accounts, your data, and all activity performed on university computing resources by you or through your accounts. You agree to follow all Albany State University policies. The security of the ASU network is the responsibility of the ASU campus community, including administrators, faculty, staff, students, and other persons conducting business with the university that interacts with the ASU network.
- B. **Review:** For security and network maintenance purposes, authorized individuals within Information Technology (IT) may monitor equipment, systems and network traffic at any time. IT reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
- C. **Change in Status:** When Authorized Users change status, e.g., upon resignation, termination, graduation, retirement, imposition of a disciplinary sanction, or a change in position, role or responsibilities within ASU, the school or unit responsible for initiating a change in status must coordinate with central support units (e.g., Office of Information Technology, Human Resource Services, etc.) to discontinue or change access and authorization to ASU IT Resources accessible to the Authorized User before the change of status.
- D. **Right to Privacy**
- i **General:** While Information Technology (IT) desires to provide a reasonable level of privacy, users should be aware that the data they create using the institution's information systems remains the property of Albany State University.
  - ii **FERPA:** Pursuant to the Family Educational Rights and Privacy Act, schools must have written permission from a parent or eligible student in order to release any information from a student's education record. Faculty or staff cannot require students to utilize third-party software that solicits information from the student's education record, confidential information, or other personal student information unless that third-party vendor has a signed confidentiality agreement with the University.
  - iii **Gramm Leach Bliley Act (GLBA)** The Gramm-Leach-Bliley Act (GLBA) requires "financial institutions" as defined by the Federal Trade Commission (FTC), to protect and secure customer information such as names, social security numbers, addresses, account and credit card information. The GLBA sets forth extensive privacy rules which the University is deemed to be in compliance with because of its adherence to the provisions of the Family Education Rights and



Privacy Act (FERPA). The GLBA also establishes a Safeguards Rule, from which the University is not exempt, that requires the University to protect and safeguard customer information.

### III. **General Standards**

A. **Internet and Network:** Access to the Internet and ASU network is available to students, faculty, staff, and approved guests whose duties require it for the conduct of University Business. Since all internet and network activities can (and will) be monitored, all students and personnel accessing the Internet and network shall not have an expectation of privacy.

i **Acceptable Use:** The University provides Internet and network access to facilitate the conduct of University business. Use of the Internet and ASU network shall not be done in a manner that interferes with the work or students, personnel, or the University's ability to perform its mission, and shall meet the conditions outlined in official University directives or goals.

ii **Prohibited Use:** Prohibited activities when using the Internet and ASU network are included in Appendix A of this document.

B. **Email:** Access to the University electronic mail (email) system is provided to all students and personnel for dissemination of information and conducting University business. Since email may be monitored, all student and personnel using University resources for the transmission or receipt of email shall not have an expectation of privacy.

i **Acceptable Use:** The University provides email to facilitate the conduct of university business. Use of email and/or electronic messaging resources shall not be done in a manner that interferes with the University's ability to perform its mission and shall meet the conditions outline in official University Directives, missions, and/or goals. However, while messages remain in the system, they shall be considered to be in the possession and control of the University.

ii **Prohibited Uses** of the University email system are enumerated in Appendix B of this document.

### C. **Hardware and Software**

i **Acquisition of Hardware and Software:** To prevent the introduction of malicious code, protect the integrity of the University information resources, and provide for a consistent standard in technology resources, all hardware and software shall be obtained from the Office of Information Technology. Users shall not be permitted to install and/or modify information resources in a manner that diminishes security standards set forth by the institution.

ii **Complying with Copyright and Licensing:** All software used on University information resources shall be procured in accordance with the **Information Technology Asset Management** policy and the **EDP Approval Review**. All students and personnel shall abide by software copyright laws and shall not obtain, install, replicate, or use software except as permitted by the software licensing agreements.



**iii Using Personally-Owned Software:** To protect the integrity of the University information resources, students and personnel shall not use personally owned software on University owned computers. This includes purchased and licensed applications; shareware; freeware; downloads from bulletin boards, Internet, Intranet, FTP site, local area networks (LANs), wide area networks (WANs) or “warez” sites; and other personally-owned or controlled software unless otherwise authorized by the Director of Information Technology or his/her designee. Documented approval shall be secured prior to use and/or installation or personally owned software on University-owned equipment.

**IV. COPYRIGHT AND INTELLECTUAL PROPERTY:**

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 violation using University Computer and Network Resources are prohibited. Computer software protected by copyright is not to be copied from, into, or by using University Computer and Network Resources, except as permitted by law or by the license or contract with the owner of the copyright.

Computer networks and computer programs that facilitate and enable locating and downloading digitized works have made possession of copyrighted material such as music files, videos and software easier than ever before. In many cases, however, possession and/or distribution of such files is in direct violation of state and federal laws, and University policy. The University regards such copyright offenses very seriously. System users must remove any copyrighted materials that they do not have the copyright holder's specific permission to possess. As noted above, they must not place such material on University systems or to personally-owned systems attached to the University network at any time and must not engage in unauthorized copying, transmission, distribution and/or downloading of such works. System users are ultimately responsible for ensuring that the copyright holder has granted permission to make or distribute the copy in question. Suspected misuse of copyrighted materials by system users may result in exercise of the University's investigatory rights with or without notice to the user, suspension of network or other account access and disciplinary sanctions as defined in this policy. Additionally, the system user may face civil or criminal action that could result in fines, imprisonment or both upon conviction.

The TEACH Act (2002) modifies and clarifies the ways in which copyrighted material may be used without permission of the copyright owner. Faculty are protected under the TEACH Act only if they are in compliance with the new requirements. Such requirements include:

- a) Faculty will not interfere with technological controls within the materials they want to use
- b) The materials are specifically for students enrolled in a class, and only those students will have access to the materials. The class is part of the regular offerings of Albany State University



- c) The materials are directly related and of material assistance to the course
- d) Faculty will include a notice that the materials are protected by copyright
- e) Faculty will use technology that reasonably limits the students' ability to retain or further distribute the materials
- f) Faculty will make the materials available to the students only for a period of time that is relevant to the context of a class session
- g) Faculty will store the materials on a secure server and transmit them only as permitted by this law
- h) Faculty will not make any copies other than the one needed to make the transmission
- i) The materials are of the proper type and amount the law authorizes:
  - a. Entire performances of non-dramatic literary and musical works
  - b. Reasonable and limited parts of a dramatic literary, musical, or audiovisual works
  - c. Displays of other works, such as images, in amounts similar to typical displays in face-to-face teaching
- j) The materials are not among those the law specifically excludes from its coverage:
  - a. Materials specifically marketed for classroom use for digital distance education.
  - b. Copies that are known to be illegal or should be known are illegal

#### **IV. Penalties for Non-Compliance**

Use of the Albany State University's information technology resources is subject to all federal, state, and local laws. Penalties for violation of these information technology policies vary but may include:

- **Loss of computer resource privileges**
- **Confiscation of equipment**
- **Removal of material violating this policy**
- **Discipline of an individual in accordance with applicable university policies or state or federal law, including criminal prosecution.**

The Chief Information Officer (CIO) or one of his/her designees may temporarily suspend, block, or restrict access to Information Systems when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of Information Systems or to protect the university from liability.

##### **A. Responsibilities of Authorized Users**

Suspected violations of this policy shall be reported to the CIO, the IT Administrator of any school or unit involved, and the IT Administrator of any Affiliate involved. Within a school or unit, the IT Administrator will report the suspected violation to those responsible for supervision of the Authorized Users involved, unless complete confidentiality is required during an investigation of the violation, and to those responsible for administration of disciplinary policies applicable to the Authorized Users involved. Authorized Users who are accused of violating this policy and who have a student or employment relationship, or an



academic appointment with UMB, will be subject to disciplinary actions or other proceedings consistent with an accusation of misconduct.

The CIO and/or IT Administrator shall investigate thoroughly the issues concerning use of ASU IT Resources, provide a complete report to the School or employing unit, and cooperate in disciplinary proceedings.

Allegations of violations by Authorized Users other than students, employees or appointees will be resolved by the CIO in consultation with the applicable school, unit or Affiliate. The CIO may suspend an accused user's access to some or all ASU IT Resources until an investigation is completed and, if required, a hearing has been held to determine the validity of the allegations involved.

Authorized Users who commit serious or repeated violations of this policy are subject to additional sanctions. Such additional sanctions may include permanent termination of access to ASU IT Resources, use restrictions, or special monitoring of activities involving ASU IT Resources.

The CIO or any IT Administrator shall refer suspected criminal violations of law to the University Police and concurrently advise University Counsel of the matter.

Immediate action may be taken by the CIO or an IT Administrator in response to potential or ongoing threats to ASU IT Resource security, the health or safety of persons, the privacy rights of students, employees, patients, clients, research subjects or others, compliance with the law, or the security of confidential or proprietary information.

Violations of this policy may result in actions under Human Resource policies, faculty policies, or student policies, in addition to actions under this policy.

Termination of enrollment, employment or appointment may follow from violations of this policy.



## Appendix A

### Prohibited Uses of the Albany State University Network and Internet Connections

Prohibited activities when using the Internet and ASU network include, but are not limited to, the following:

- a) Use of any ASU-owned computer or network for private, commercial, non-ASU business purposes without explicit authorization is a violation of these terms and conditions of use and will result in the termination of computer privileges.
- b) The introduction of data or programs which in some way endangers computing resources or the information of other users (e.g., a computer worm, virus, or other destructive program), or which infringes upon the rights of other Albany State University users (e.g., inappropriate, obscene, pornographic, bigoted, or abusive materials) is prohibited.
- c) Users may not copy, publish, store or transmit data when doing so would constitute a violation of copyright. Users who are in any doubt as to the copyright status of data they wish to store or send should contact the ASU Office of Information Technology for help in determining the legality of their planned use of the data.
- d) Users are prohibited from installing, storing or using unlicensed software on ASU computers. Transmission of such software over either the ASU or University network is prohibited.
- e) Individuals may not attempt to circumvent security systems or to exploit or probe for security holes in any ASU network or system, nor may individuals attempt any such activity against other systems accessed through ASU's facilities. Execution or compilation of programs designed to breach system security is prohibited unless authorized in advance.
- f) The compilation or redistribution of information from University and/or ASU directories (printed or electronic) to third parties is forbidden.
- g) Physically damaging information technology resources;
- h) Using, or encouraging others to use, information technology resources in any manner that would violate this or other University policies or any applicable state or federal law; and
- i) Falsely reporting or accusing another of conduct that violates this policy, without a good faith basis for such an accusation.
- j) Sending messages that are malicious or that a reasonable person would find to be harassing;
- k) Accessing another person's computer account without permission. Users may not supply false or misleading data, or improperly obtain another's password to gain access to computers or network systems, data or information. Obtaining access to an account name or password through the negligence or naiveté of another is considered to be a specifically prohibited use;
- l) Modifying system or network facilities, or attempting to crash systems or networks.



## Appendix B

### Prohibited Uses of the Albany State University Email System

Prohibited activities when using the Albany State University email system include, but are not limited to, the following:

- a) Personal use that creates a direct cost for the University
- b) Use for personal monetary gain or for commercial purposes that are not directly related to University business.
- c) Sending copies of documents in violation of copyright laws
- d) Inclusion of the work of others into electronic mail communications in violation of copyright laws.
- e) Capture and "opening" of electronic mail except as required in order for authorized employees to diagnose and correct delivery problems.
- f) Use of electronic mail to harass or intimidate others or to interfere with the ability of others to conduct University business.
- g) Use of electronic mail systems for any purpose restricted or prohibited by laws or regulations.
- h) "Spoofing," i.e., constructing an electronic mail communication so it appears to be from someone else.
- i) "Snooping," i.e., obtaining access to the files or electronic mail of others for the purpose of satisfying idle curiosity, with no substantial University business purpose.
- j) Attempting unauthorized access to electronic mail or attempting to breach any security measures on any electronic mail system, or attempting to intercept any electronic mail transmissions without proper authorization.