The decision of the Criminal History Admissions Committee is final. Applicants and appropriate departments will be notified in writing of the decision.

Applicants may not reapply for admission in the same academic year that they were denied by the Criminal History Admissions Committee unless there has been a change in their information.

APPROPRIATE USE OF INFORMATION & TECHNOLOGY RESOURCES

http://www.astate.edu/dotAsset/42c06ed4-f1aa-43f2-88f3-b84cc32cb4b6.pdf

Information Technology resources are provided to support the academic, research, service, and campus life components of A-State. These resources are for the sole use of A-State students, faculty and staff and other authorized users to accomplish the mission of the university.

Rights and Responsibilities

Arkansas State University expects that users of campus computing and network facilities will respect the rights of other users as well as the integrity of the systems and related physical resources. Since electronic information is volatile and easily reproduced, users must exercise care in acknowledging and respecting the work of others through strict adherence to software licensing agreements and copyright laws. Because Arkansas State University is a state agency, all information stored within, or transmitted through systems and/or networks is considered public record and subject to disclosure under the Arkansas Freedom of Information Act unless exempt under the law.

Users do not own accounts on university computers, but are granted the privilege of exclusive use. The Electronic Communications Privacy Act authorizes system administrators and other university employees to access user data, activity, and information. By utilizing A-State computing and network resources, you give consent to accessing and monitoring by system administrators of any electronic communications, including stored and transmitted information, in order to enforce this policy or to protect the integrity of computer systems or the rights or property of the university. System administrators may examine or make copies of information and activities that are suspected of misuse or that have been corrupted or damaged.

User files may be subject to search by law enforcement agencies under court order if such files contain information that may be used as evidence in a court of law.

Computer and network usage and this policy is subject to the Arkansas State University Appropriate Use of Technology Resources Policy, as approved by the Board of Trustees. This policy can be found at the following link: http://www.astate.edu/dotAsset/42c06ed4-f1aa-43f2-88f3-b84cc32cb4b6.pdf.

Enforcement

Minor infractions of this policy, when accidental, such as consuming excessive resources or overloading computer systems, are generally resolved informally by the person administering the accounts or network. This may be done through electronic mail or in-person discussion and education. Repeated minor infractions or misconduct that are more serious may result in the temporary or permanent loss of computer access privileges or the modification of those privileges. More serious violations include, but are not limited to unauthorized use of computer resources, attempts to steal passwords or data, unauthorized use or copying of licensed software, and repeated harassment or threatening behavior. In addition, offenders may be referred to their sponsoring advisor, department, employer or other appropriate university office for further action. If the individual is a student, the matter may be referred to the Office of Student Conduct for disciplinary action. Any offense that violates local, state or federal laws may result in the immediate loss of all university computing privileges and will be referred to appropriate university offices and/or other law enforcement authorities.

Standards

Conduct that violates this policy includes, but is not limited to, the activities in the following list:

- Unauthorized use of a computer account.
- Using the campus network to gain unauthorized access to any computer systems.
- Connecting unauthorized equipment to the campus network.
- Physically tampering with university owned networking equipment. This includes, but is not limited to, switches, wireless access points and data ports.
- Unauthorized attempts to circumvent data protection schemes or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data.
- Knowingly or carelessly performing an act that will interfere with the normal operation of computers, terminals, peripherals or networks.
- Knowingly or carelessly running or installing on any computer system or network, or giving to another user a program intended to damage or to place excessive load on a computer system or network. This includes, but is not limited to, programs known as computer viruses, Trojan Horses and worms.
- Deliberately wasting/overloading computer resources, such as printing too many copies of a document.
- Violating terms of applicable software licensing agreements or copyright laws.
- Violating copyright laws and their fair use provisions through inappropriate downloading, reproduction, or dissemination of copyrighted text, images, multimedia, etc.
- Forging the identity of a user or machine in an electronic communication.
- Transmitting or reproducing materials that are slanderous or defamatory in nature or that otherwise violate existing laws or university regulations. Initiating or propagating electronic chain letters. Inappropriate mass mailing. This includes multiple mailings to newsgroups, mailing lists or individuals, e.g. "spamming," "flooding," or "bombing."
- Displaying obscene, lewd or sexually harassing images or text in a public computer facility or location that can be in view of others.
- Using university resources for commercial activity such as creating products or services for sale.