



PUDCJBR supports the teaching-learning process and research by providing the needed technological infrastructure to the academic community. This policy provides a guide on how the technology should be use.

### **Rights and Responsibilities**

Computers and networks can provide access to different remote resources, as well as the ability to communicate with other users worldwide. Such open access is a privilege, and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations.

Students and employees may have rights of access to information about themselves contained in computer files, as specified in federal and state laws. Files may be subject to search under court order. In addition, system administrators may access user files as required to protect the integrity of computer systems.

### **Existing Legal Context**

All existing laws (federal and state) and PUDCJBR regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct.

Misuse of computing, networking, or information resources may result in the restriction of computing privileges. Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable PUDCJBR policies, procedures, or collective bargaining agreements. Complaints alleging misuse of campus computing and network resources will be directed to those responsible for taking appropriate disciplinary action.

Reproduction or distribution of copyrighted works, including, but not limited to, images, text, or software, without permission of the owner is an infringement of U.S. Copyright Law and is subject to civil damages and criminal penalties including fines and imprisonment.

### **Examples of Misuse**

Examples of misuse include, but are not limited to, the activities in the following list.

- Using a computer account that you are not authorized to use.
- Obtaining a password for a computer account without the consent of the account owner.
- Using the Campus Network to gain unauthorized access to any computer systems.
- Knowingly performing an act which will interfere with the normal operation of computers, terminals, peripherals, or networks.
- Knowingly 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.
- Attempting to circumvent data protection schemes or uncover security loopholes.
- Violating terms of applicable software licensing agreements or copyright laws.
- Deliberately wasting computing resources.
- Using electronic mail to harass others.
- Masking the identity of an account or machine.

- Posting materials on electronic bulletin boards that violate existing laws or the University's codes of conduct.
- Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.
- Activities will not be considered misuse when authorized by appropriate PUDCJBR officials for security or performance testing.

### **Additional Use Policies**

The Computer Use Policy applies to the use of all PUDCJBR computing resources. Additional computer and network use policies and terms and conditions may be in place for specific electronic services offered by the institution.

In particular, POPULI, have an additional policy that govern use of this service. You must familiarize yourself with this policy when you agree to use this service.

### **Appropriate Use**

PUDCJBR extends to students, faculty, and staff the privilege to use its computers and network. When you are provided access to our campus network, you are enabled to send and receive electronic mail messages around the world, share in the exchange of ideas through electronic news groups, and use Web browsers and other Internet tools to search and find needed information.

In addition to formal policies, regulations, and laws which govern your use of computers and networks, the Internet user community observes informal standards of conduct. These standards are based on common understandings of appropriate, considerate behavior which evolved in the early days of the Internet, when it was used mainly by an academic and highly technical community. The Internet now has a much wider variety of users, but the early codes of conduct persist, crossing boundaries of geography and government, in order to make

using the Internet a positive, productive, experience. You are expected to comply with these informal standards and be a "good citizen" of the Internet.

### **Enforcement**

Penalties may be imposed under one or more of the following: PUDCJBR regulations, the laws of Puerto Rico and/or the United States.

Minor infractions of this policy or those that appear accidental in nature are typically handled informally by electronic mail or in-person discussions. More serious infractions are handled via formal procedures. In some situations, it may be necessary to suspend account privileges to prevent ongoing misuse while the situation is under investigation.

Infractions by students may result in the temporary or permanent restriction of access privileges, and/or referral of the situation to the Counselor. Those by a faculty or staff member may result in referral to the Chief Executive Officer.

Offenses which are in violation of local, state, or federal laws may result in the restriction of computing privileges, and will be reported to the appropriate University and law enforcement authorities.

### **Reporting Misuse**

Report misuse of campus electronic communication resources to the Chief Executive Officer through [ndominguez@eeapr.org](mailto:ndominguez@eeapr.org).