THE UNIVERSITY OF PUERTO RICO'S INSTITUTIONAL POLICY AND PROCEDURE FOR THE LEGAL ETHICAL USE OF INFORMATION TECHNOLOGY

Approved by the Board of Trustees,
Certification No. 72 (1999-2000)

I. INTRODUCTION

Institutions of higher learning are striving to integrate electronic environments into the value structures and ethics of their communities. Institutions of higher learning place a high value on creativity and on intellectual products. Their desire is to be able to do creative work of intellectual value, free of the fear that said work may suffer alterations or destruction. They also value the ease with which information resources may be used, and the availability of access to growing volumes of data. It is imperative that we protect ourselves in such a way that information technology may stimulate, rather than interfere with, access to such resources. Institutions of higher learning place a high value on individual experimentation and on different ways of learning. They also value the integrity of information resources and expect social responsibility. Therefore, we must stimulate individual experimentation and creativity while we promote the conscientious, ethical, and responsible use of information resources.

II. LEGAL BASIS

This statement of institutional policy and procedure has been formulated in accordance with the applicable provisions of the Law of the University of Puerto Rico, Law 1 of January 20, 1966, as amended, the General Regulations of the University of Puerto Rico, Law 16 of June 16, 1993, the Penal Code of Puerto Rico, and other applicable state and federal legislation.

III. APPLICABILITY

The provisions of this Institutional Policy and Procedure for the Legal Ethical Use of Information Technology applies to the entire University community, to external clients, and to service providers, as well as to all users of information technology resources and telecommunications services.

IV. PURPOSE

The purpose is to establish an institutional policy in order to safeguard the information technology resources and telecommunications services that are offered to the University community and to those who provide services to the University of Puerto Rico, as well as to external clients and to users of the information and telecommunication system of the University of Puerto Rico. This policy applies to the use of all institutional and university information and to the formats (paper, tape, electronic communication, and other analogous formats) in which it may be used.

V. INSTITUTIONAL POLICY

Access to networks and to the University of Puerto Rico's information technology environment is an institutional privilege granted by the University of Puerto Rico.

It is the University's policy to furnish its community with access to local, national, and international sources of information, and to provide an atmosphere that stimulates receptivity to knowledge and the sharing of information, as well as the utilization of information resources by the University community, by clients and users, always respecting public trust and ethics, and in accordance with the policies and regulations established by the University and its operational units.

The University of Puerto Rico strives to guarantee privacy and confidentiality in the use of information technology. It is the responsibility of all users to utilize the University of Puerto Rico's information technology efficiently, effectively, ethically, and legally, in conformance with the Law and with University regulations. The legal ethical standards that all users must observe are based on ethical and legal norms applying to the use of any public resource within or outside the University, as found in state and federal statutes, as well as in the regulations, policies, and procedures of the University.

It is the intention of the University of Puerto Rico to protect the information in its systems, which is acknowledged as a primary asset to the administration and to education and research, from modifications (both accidental, and intentional but unauthorized), misuse, destruction, or disclosure. In order to carry out its efforts to protect the integrity of its information systems, workstations, networks, laboratory facilities, and other analogous University properties or facilities, the University has the right to supervise its information systems and telecommunications resources and to take the corresponding corrective action. Access to the infrastructure of the information resources (both within and outside the University), the exchange of information, and the security of the intellectual products of the community entail the requirement that each user accept the responsibility of protecting the rights of the community. Any member of the University community, service provider, client, or user who, without authorization, accesses, utilizes, destroys, alters, dismantles, or changes the configurations of the University's information technology, its properties or facilities, including those held by third parties, is a threat to the atmosphere of maximum access to and exchange of information, violates the security of the environment in which members of the community may create intellectual products, and causes a breakdown in institutional order. Such person will be subject to disciplinary action in accordance with University regulations, as well as other actions to the full extent of the law.

Members of the University community, service providers, external clients, and users place themselves under the obligation of collaborating and cooperating with state and federal agencies and with other interested parties to see that the University of Puerto Rico's information technology and its internal and external networks are protected against any type of interference. It is an obligation of the University of Puerto Rico to respect the privacy and confidentiality of all files, e-mails, and printed user lists as efficiently as possible. For security reasons and to protect the University's interests, the

University of Puerto Rico may intervene in any and all aspects of a system, including individual online sessions, in order to determine whether anyone is violating the policies set out in this document, whenever a user files a complaint against the person who has sent an objectionable message or when University officials accidentally discover an improper use that is in plain sight. The granting of an access code or any other form of access is for the purpose of ensuring the confidentiality and privacy that are appropriate for University data files; it is not a guarantee of privacy or confidentiality for the personal or inappropriate use of University equipment and facilities.

The University classifies as unethical and unacceptable, and as sufficient cause for taking disciplinary action, which may include non-reassignment, expulsion, dismissal, or any other legal action, any activity by means of which an individual:

a) violates reserved rights or license protections and authorizations, registered agreements, or other contracts with the University or third parties;

b) interferes with the intended usage of information resources;[1]

c) obtains or attempts to obtain unauthorized access to information resources;[2]

d) without authorization attempts to destroy, alter, dismantle, disfigure, impede the right of access, or in any other way interfere with the integrity of computerized information or information resources.[3]

VI. GENERAL PROVISIONS

The following provisions guarantee ethical and acceptable behavior in accordance with established policy.

1. Users are subject to the stipulations of all software licenses, copyrights, and University policies regarding intellectual property, and to federal and state laws.

2. Users are responsible for safeguarding their usernames and access codes. Users must not print out, save on-line, or give out their access codes to other persons. The user is responsible for the authorized use of his or her identification, for that purpose only. Each user is responsible for all transactions carried out under the authorization of his or her identification.

3. Information system users must not intentionally seek, provide, or modify data or obtain copies of files, programs, or access codes belonging to other users. This includes the entire system files and accounts system.

[1]Information resources, as used in this document, refer to any information in electronic or audiovisual format, or any equipment or program for storing or using said information. For example, this definition includes e-mail, local databases, databases accessed externally, CD-ROMs, videotaped films, magnetic recording media, photographs, and digitalized data.

[2]Same as Note 1.

[3]Same as Note 1.

4. Files (data or programs) controlled by individual users are considered private, whether accessible or not by other users. A user must obtain written permission from the owner of a file before altering or copying a file that does not belong to him or her. The ability to read, alter, or copy a file does not imply permission to read, alter, or copy that file.

5. Each account holder or workstation user is solely responsible for the use that is made of his or her account or station. Individuals, who intentionally abuse their accounts and privileges, downgrade the performance of the system, make improper use of information system resources, or interfere with the functioning of the information or telecommunications systems are subject to disciplinary action. Removing, modifying, or reconfiguring files or equipment pertaining to information systems or software belonging to the University is prohibited.

6. E-mail facilities are not to be used for the transmission of commercial or political advertisements, personal messages, applications, promotions, destructive programs (viruses), or any other personal or unauthorized use.

7. Users of information systems may use network links for permissible purposes as outlined in network guides (for example, BITNET or INTERNET). Users are responsible for obtaining and complying with all policies for acceptable use of the network.

8. The existence of connections to other systems by means of the network does not imply the right to connect to or to make use of said systems, unless duly authorized by the owners.

9. Users share such resources as disk space, Central Processing Unit (CPU) cycles, printer queues, batch queues, online sessions, software licenses, etc. No user may monopolize these resources, and may use them only insofar as may be necessary for purposes related to authorized use.

10. Users must not intentionally develop or utilize programs that infiltrate the system or damage software or system equipment. Users have the right not to be subjected to physical, verbal, electronic, or any other form of abuse, and may file a formal complaint through proper University channels.

11. Although each user has a right to freedom of expression, this right does not include obscene or defamatory material, which may not be sent by e-mail or posted on electronic bulletin boards or to news groups, etc.

12. The use of communications facilities (such as e-mail, voice mail, or systems with similar functions) to send messages that, in violation of the penal or civil laws of Puerto Rico, propose a fraudulent business transaction or a violation of the law, or are obscene, defamatory, or threatening to specific persons, is prohibited.

13. Users must not cooperate, stimulate or participate with others for incite others to violate any part of these policies, rules, and conditions.

14. The occasional personal use of computing equipment and software is permitted when said personal use does not interfere with expected job performance and does not violate any applicable policy, rule, or law. Evaluation of an employee's performance may take into consideration the employee's personal use, and a supervisor may require, if he or she deems necessary, that a change be made in the employee's personal use, as a condition of employment.

15. No newly-created account will be authorized without the Application for Account Renewal, Creation, or Change, ("Formulario de Solicitud de Renovación, Creación o Cambio de Cuenta"), as revised in October, 1996. This must be filled out in full, with the required signatures in the spaces provided. This form is part of this Institutional Policy and Procedure for the Legal Ethical Use of Information Technology.

16. Institutional units within the University may define "conditions" for the use of those facilities under their control. These must be consistent with this general policy, but may include additional details, guidelines, or restrictions. If such "conditions" are defined, applicable mechanisms must also be defined for enforcing the conditions.

VII. ADMINISTRATION

The task of enforcing this policy is the responsibility of each institutional unit in coordination with the Office of Information Systems of the Central Administration. Each campus or college is responsible for developing the necessary specific procedures and for applying disciplinary measures.

VIII. EFFECTIVENESS

This policy, The University of Puerto Rico's Institutional Policy and Procedure for the Legal Ethical Use of Information Technology, will become effective thirty (30) days after it is filed at the Department of State in accordance with Law 170 of August 12, 1988, known as the Uniform Administrative Procedures Act, as amended.

A copy of the same must be given to each student, university employee, or any user of the information system at the time of granting access to the system; a receipt must be retained as proof. This policy must also be placed on bulletin boards or in other prominent places in all offices and agencies of our institution.

[Filed in the Department of State on 25 April, 2000, File No. 6136.]