Information Technology Acceptable Use Policy

1.0 Overview

The Information Technology (IT) department intentions for publishing an Acceptable Use Policy follows Polytechnic University of Puerto Rico (PUPR) established culture of openness, trust and integrity. The IT department is committed to protecting PUPR's Institutional members and the Institution from illegal or damaging actions by individuals, either knowingly or unknowingly.
Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of PUPR. These systems are to be used for business or educational purposes in serving the interests of the University in the course of normal operations.
Effective security is a team effort involving the participation and support of every PUPR Institutional member and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer and telecommunication equipment at PUPR. These rules are in place to protect the PUPR Institution. Inappropriate use exposes PUPR to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to all Institutional members, which includes employees, students, contractors, consultants, temporary employees, and other workers at PUPR, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by PUPR, either directly or indirectly (grants) and any other equipment connected to our data communication network.

4.0 Policy

4.1 General Use and Ownership

1. While PUPR's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the Institution systems remains the property of PUPR. Because of the need to protect PUPR's network, management cannot guarantee the

confidentiality of information stored on any network device belonging to PUPR or connected to our network.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, Institutional members should be guided by departmental policies on personal use, and if there is any uncertainty, Institutional members should consult their dean, supervisor or manager.
3. IT recommends that any information that users consider sensitive or vulnerable be encrypted.
4. For security and network maintenance purposes, authorized individuals within PUPR may monitor equipment, systems and network traffic at any time.
5. PUPR reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by PUPR confidentiality guidelines, see attached email confidentiality disclaimer. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Institutional members should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly; user level passwords should be changed every six months.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Window's users) when the host will be unattended.
4. Because information contained on portable computers is especially vulnerable, special care should be exercised.
5. Postings by Institutional members from a PUPR email address to newsgroups should contain the attached official disclaimer which states that the opinions expressed are strictly their own and not necessarily those of PUPR, unless posting is in the course of business duties.
6. Unless overridden by departmental or group policy, all hosts used by the institutional members that are connected to the PUPR Internet/Intranet/Extranet, whether owned by the Institutional members or PUPR, shall be continually executing approved virus-scanning software with a current virus database.

7. Institutional members must exercise extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Institutional members may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
Under no circumstances is an employee of PUPR authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing PUPR-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by PUPR.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which PUPR or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The IT department should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a PUPR computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction. Refer to the Title VII of the Civil Rights Act 1964 as amended, Age Discrimination in Employment Act of 1967 and the American with Disabilities Act of 1999.
7. Making fraudulent offers of products, items, or services originating from any PUPR account.

8. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
9. Port scanning or security scanning is expressly prohibited proper arrangement and previous notification and approval is obtained from the IT office.
10. Executing any form of network monitoring which will intercept data not intended for the Institutional member's host, unless this activity is part of the Institutional member's normal job/duty.
11. Circumventing user authentication or security of any host, network or account.
12. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
13. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

Email and Communications Activities

The following activities are strictly prohibited:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment or violation of federal and State laws via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within PUPR's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by PUPR or connected via PUPR's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Harassment (Cyber Bullying)

No member of the community may use Institutional resources to libel, slander, or harass any other person. Harassment includes, without limitation, the following:

1. Intentionally using Institutional resources to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or others;
2. Intentionally using Institutional resources to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease;
3. Intentionally using Institutional resources to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease;
4. Intentionally using Institutional resources to disrupt or damage the academic, research, administrative, or related pursuits of another;
5. Intentionally using Institutional resources to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

5.0 Enforcement

Any Institutional member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or dismissal from the Institution.

Email Confidentiality Disclaimer (For Employees)

Aviso de Confidencialidad:
Esta es una comunicación privilegiada y confidencial de la Universidad Politécnica de Puerto Rico (el remitente y la persona a quien va dirigida la misma). Cualquier uso del contenido del mensaje por una persona a quien no se dirige el mismo es ilegal y está estrictamente prohibido. Ninguna persona podrá divulgar, copiar o alterar el contenido de este mensaje. Si usted recibió esta comunicación por error, favor de destruirla junto con los anejos que haya podido tener la misma.

Notice of Confidentiality:
This is a confidential and privileged communication between the Polytechnic University of Puerto Rico (sender and the addressee). Any use of the contents of this message by someone not intended to receive it is illegal and prohibited. No person is authorized to disclose, copy or modify the contents of this message. If you received this message by mistake, please delete it along with any attachments it may have.

Revised by: Information Technology Office
November 2018