Blackboard™ System Policy and Procedures

I. Introduction

This document is designed to set policy and detail the procedures for using (PUPR) Learning Management System; Blackboard™. Given the frequently changing nature of the online learning environment, Blackboard Policy and Procedures may change often; therefore, it is important that the revision date on the current online policy matches the revision date of any printed documents.

II. Purpose

The Blackboard Learn™ System is a web-based learning platform and should be used for the purpose of enhancing the student learning experience. The System is integrated with the (PUPR) student information system, currently known as *Jenzabar.* Blackboard users and courses are populated through the Blackboard snapshot tool. As users and courses are entered into *Jenzabar*, the snapshot tool transfers this information to the appropriate course or organization within the Blackboard System.

III. Student Users

1. Only (PUPR) students who are enrolled in the current term / trimester in courses using Blackboard will have access to the Blackboard System. Students who have taken courses using Blackboard in previous terms / trimesters will not have access if not currently enrolled in a course using Blackboard.
2. Once a student enrolls in at least one course marked for Blackboard the student will have access again, using the same username and password as before.
3. In most cases, usernames for (PUPR) Blackboard System will be the same as the Institutional Email Account username. The institutional account is provided by the Educational Technology Center (ETC or CTE, its acronym in Spanish) and validated by the student. Once the student is admitted to the institution, ETC sends a message to the student's personal email with the information to activate the account and change the generic password.

4. If the student did not provide a personal email account, then the student must visit the ETC office or go online to request an institutional account.
5. Student enrollment is automated between the *Jenzabar* System and the Blackboard System. Once a student's registration is processed in *Jenzabar* for courses using Blackboard, the snapshot tool will automatically populate the course shell with that student's enrollment. The automated enrollment may take 24 hours to complete.
6. Students will not have access to their upcoming term / trimester courses until the Blackboard System Administrator has made the course available.
7. Students enrolled in Blackboard courses will only have access to those courses for three days following the last day of the term. Any information the student may need to retrieve from the course must be retrieved prior to the end of the third day after the term.
8. Students who receive an incomplete grade in a Blackboard course must wait until the instructor requests a course extension in which the reason and the dates the course will remain open for one or more students will be specified.
9. There may be exceptional circumstances where external users may request access to the Blackboard System. These requests should be submitted to the Director of Distance Education, and if approved these users will be granted Guest access.
10. All (PUPR) Blackboard System users must comply with the rules and regulations established
11. Instructors may choose to post student work on the Blackboard course site. Students must be informed if their work will be retained in the course site beyond the duration of the term / trimester if others will have access to it. No evaluative commentary or grade information from the instructor may be included with student work left on the Blackboard site, if the work includes information identifying its creator. Students retain rights to their work, including posted messages within the Communication area of the Blackboard System, but this work must be retrieved by the student from the Blackboard course before the end of the third day following the previous term.
12. Student access and movements within Blackboard can be tracked by the Blackboard System Administrator and the instructor of the course. Through statistical reports, information can be obtained upon request of the instructor, Academic Director or Dean.

IV. Instructors / Staff Users

1. Student enrollment is automated between *Jenzabar* Student Information System and Blackboard. Once a student's registration is processed in Jenzabar, the snapshot will automatically populate the course shell with that student's enrollment.
2. All Blackboard instructors must have their course content available to students two weeks prior to the beginning of the term.
3. Student information within a course will disappear when a student drops the course or is removed from Blackboard for any other reason during a term.
4. Instructors requesting that other instructors have access to their course for mentoring purposes may contact the Distance Education Director to have these instructors added to their course.
5. Instructors requesting that students have access to their course as guests for purposes such as auditing the class must contact the Distance Education Director to have these students enrolled.
6. Instructors are solely responsible for retaining copies of the Blackboard course Grade Center, and all student related data prior to the course archive schedule in the event of future grade disputes.
7. Every instructor should keep a separate Grade Center outside of Blackboard during the duration of each course in case the Blackboard System experiences technical difficulties and Grade Center information becomes unavailable for an extended period of time.
8. It is important that instructors do not rely on the Blackboard System as a record keeping source for important student records and Grade Center information.
9. Instructor access and movements within Blackboard can be tracked by the Blackboard System Administrator. Through statistical reports, information can be obtained upon request of the Academic Director or Dean.
10. Faculty and staff, who are not currently teaching a course through Blackboard, can still request an account by contacting the Distance Education director.

V. Faculty Development; Blackboard Learning Modules to enhance Teaching and Learning

1. Every instructor teaching online / hybrid or web-enhanced courses is required to participate in the Institutional Blackboard Certification Program. The Faculty Certification Program focuses on the mastery of Learning Modules used to package and present content that allows instructors to organize related course materials. The program is offered face to face and consists of four workshops, 12 contact hours (3.0 hours for each of the four workshops) structured around themes and exercises that foster interaction and facilitate the transition from a face to face course to an online/hybrid course. Instructors are responsible for the design and course content using learning modules.

VI. Blackboard Course Copy

1. Course copy is a tool used for the process of transferring course material from one course shell to another. This is done when the new course shell for the next term / trimester is available. It is the responsibility of the Blackboard System Administrator to copy over course material from one term / trimester to the next.

VII. Blackboard Administrator & Blackboard Support Staff

The Blackboard System Administrator shall publish information regarding:

1. Blackboard System scheduled outages.
2. Announce plans for Blackboard System Upgrades.
3. Create and modify Blackboard training material.
4. Plan and schedule Blackboard training courses.
5. Create and update Blackboard Policy and Procedures.
6. Assist Blackboard users with technical problems and issues.

CEDUP will answer all Technical Support requests only through email.

1. Technical Support: bbsupport@pupr.edu
2. Tools/Features Support: bbcourses@pupr.edu

All technical support requests will be answered in a period of time of no more than 24 hours including weekends and holidays. The Blackboard Platform users should include the following information at the moment of requesting technical support.

1. Name and Last name
2. Student ID number
3. Course name and Section
4. Professor's name
5. Detailed explanation of the problem
6. Print Screen - (In case a message appears or an error screen)

VIII. The Blackboard System Information

1. The Blackboard System might require periodic downtime in order to apply security updates, patches, system reconfigurations, system upgrades and other scheduled maintenance to the Blackboard System. Notice will be given in advance of any scheduled downtime. All Blackboard System routine maintenance is scheduled during the early morning hours. It is the instructor's responsibility to maintain an archived file of all course material in the event of system failure.

IX. Copyright Regulations

Copyright law and Fair Use Guidelines allow faculty to provide access to copyrighted materials using the Blackboard System. Persons using PUPR's Blackboard System are strongly encouraged to respect the property of others by obeying copyright law and requesting permission, when appropriate, before using the work of others.

X. Harassment Prevention

Blackboard allows access to a number of tools, such as discussion boards, which enable text-based communication.

1. Postings should not be offensive, inflammatory, racist / sexist or abusive in any other way.
2. Remember that textual interaction takes place without normal visual / verbal clues, which help to interpret meaning.
3. Your posts will be visible to all students registered within the course, as well as instructors and system administrators and will be eventually archived for future reference.
4. Your posts should be related to the topic of the discussion and the tone of the posts should be in accordance with the discussion. Excessive use of obscenities could be considered offensive and are strongly discouraged.
5. The laws of copyright apply so users should not copy other user's posts / information without permission.
6. If Blackboard discussion board postings count towards a grade, precautions against plagiarism should be taken, the same as with written material.

If you are offended by a posting, please consider the following before replying:

1. Will your post contribute positively to an academic discussion?
2. How would you respond if you were in a face-to-face situation?
3. Would this issue be best dealt with by contacting your instructor rather than the individual concerned?
4. In the case of an offensive post, you may wish to contact your instructor privately rather than escalate the situation in an online and public environment.

XI. Family Educational Rights & Privacy Act (FERPA)

Polytechnic University of Puerto Rico compiles and maintains student information which facilitates the educational development of students and effective administration of the university, in order to guarantee the rights of privacy and access as provided by the Family Educational Rights and Privacy Act of 1974 (Buckley Amendment, 20 U.S.C. 1230, 1232). More information on the FERPA Guidelines:
http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Academic Integrity

Students must comply with the following notifications displayed in the Blackboard course announcements:

Academic Honor Pledge

I affirm I am the student registered for and taking this course. Misrepresentation is considered academic misconduct and may result in failure of the course and/or further disciplinary action, including dismissal from the University.

Conditions of Use

For purposes of these Conditions of Use, the term "Content" means any material, information, communication, text, graphic, link, electronic art, animation, audio, video, photo, or other data used in connection with a Polytechnic University of Puerto Rico's ("PUPR") online course (a " Course"). With respect to any Content posted by you in connection with a Course, you represent and warrant to PUPR that you either (a) own the copyright to the Content, (b) obtained appropriate consent for the use of the Content, or (c) are otherwise lawfully using and/or posting the Content. With respect to any Content that you (a) do not own the copyright to, (b) have not obtained appropriate consent for the use of, or (c) are otherwise not lawfully using, you may not copy, reproduce, publish, distribute, modify, create derivative works of, rent, lease, sell, transfer, display, transmit, compile or collect in a database, or in any manner commercially exploit such Content in whole or in part. You may not store any Content owned by or licensed to PUPR in any form or medium, including, but not limited to, archival file or computer-readable file. You may not copy, reproduce, publish, distribute, modify, create derivative works of, rent, lease, sell, transfer, display, transmit, compile or collect in a database, or in any manner commercially exploit the design or other features of a Course that do not constitute Content. You may not store any Course owned by or licensed to PUPR in any form or medium, including, but not limited to, archival file or computer-readable file.

Copyright Notice

The materials on this course website may be subject to U.S. and International Copyright Law. The materials on this course website are only for the use of students enrolled in this course for purposes associated with this course and may not be further retained or further disseminated.

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 employees 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 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 employee 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 equipment at PUPR. These rules are in place to protect the employee and PUPR. 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 employees, 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).

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.
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, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their 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. Employees 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 Windows 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 employees 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 employee that are connected to the PUPR Internet/Intranet/Extranet, whether owned by the employee or PUPR, shall be continually executing approved virus-scanning software with a current virus database.
7. Employees 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. Employees 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 employee's host, unless this activity is a part of the employee'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

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).

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Email Confidentiality Disclaimer

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.