Blackboard™ Platform Policies and Procedures

Introduction

This document is designed to establish policies and detail procedures for using the LMS; Blackboard™. Due to the changing nature of the online learning environment, Blackboard™ policy and procedures may change frequently; therefore, it is important that the revision date of the current online policy matches the revision date of any printed documents.

Purpose

The Blackboard™ system is a web-based learning platform and should be used to enhance the learning experience for students. The System is integrated with the student information system, currently known as Banner. Blackboard™ users and courses are integrated through the LMS tool. As users and courses are programmed into Banner, the tool transfers this information to the appropriate course or organization within Blackboard™ system.

Students Users

1. Only students who are enrolled in the current term/quarter in courses using the LMS will have access to Blackboard™ System. Students who have taken courses using Blackboard™ in previous terms/quarters will not have access if they are not currently enrolled in a course using the platform.
2. Once a student enrolls in at least one course in Blackboard™, the student will have access again, using the same username and password as before.
3. In most cases, usernames for Blackboard™ will be the same as the institutional email account username. The institutional account is provided by the Educational Technology Center (ETC) 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, they must visit the ETC office or go online to request an institutional account.
5. Student enrollment is automated between Banner System and Blackboard™ System. Once a student's enrollment is processed in Banner for courses using Blackboard™, the tool will automatically complete that student's enrollment in their respective courses. Self-enrollment may take 24 hours to complete.
6. Students will not have access to their upcoming quarterly courses until Blackboard™ system administrator has made the course available.
7. Students enrolled in Blackboard™ courses will only have access to those courses for three days after the last day of the term/quarter. Any information the student may need to retrieve from the course must be retrieved before the end of the third day after the term/trimester.
8. Students who receive an incomplete grade in a Blackboard™ course must wait until the instructor requests a course extension specifying the reason and dates the course will remain open to one or more students.
9. There may be exceptional circumstances in which external users request access to Blackboard™ System. These requests must be submitted to the Director of VEIL and if approved, these users will be granted Guest access.
10. All users of Blackboard™ System must comply with the established rules and regulations.
11. Instructors can choose to post student work in Blackboard™ course. Students must be informed if their work will be kept on the course site beyond the length of the term/trimester and if others will have access to it. No evaluative comments or grading information may be included in reference to student work left on Blackboard™, if the work includes information that identifies its creator. Students retain rights to their work, including messages posted within the communication area of Blackboard™ system, but the student must retrieve this Blackboard™ course work by the end of the third day after the previous term/quarter.

12. Blackboard™ System Administrator and Course Instructor can track student access and movement within the platform. Through statistical reports, information can be obtained at the request of the instructor, Academic Director, or Dean.

Instructors and Administrative Users

1. Student enrollment is automated between Banner student information system and Blackboard™. Once a student's enrollment in Banner is processed, the tool will automatically complete that student's enrollment.
2. All Blackboard™ instructors must have their course content available to students two weeks prior to the start of the term/quarter.
3. Student information within a course will disappear when a student leaves the course or is removed from Blackboard™ for any other reason during a term.
4. Instructors who request that Instructor's Assistants have access to their course for tutoring purposes may contact the Director of VEIL to have them added to their course.
5. Instructors requesting that students have guest access to their course for purposes of class auditing should contact the Director of VEIL to enroll them in the course.
6. Instructors are solely responsible for retaining copies of Blackboard™ course Gradebook and all student-related data prior to the course file date in the event of grade disputes.
7. Each instructor must maintain a separate Gradebook outside of Blackboard™ for the duration of each course in case the system experiences technical difficulties and Gradebook information is unavailable for an extended period of time.
8. It is important that instructors do not rely on Blackboard™ as a source of important student record keeping and gradebook information.
9. Blackboard™ system administrator can track instructor access and movement within Blackboard™. Through statistical reports, information can be obtained at the request of the Academic Director or Dean.
10. Faculty members and staff who are not currently teaching a course through Blackboard™ can still request an account by contacting the Director of VEIL.

Faculty Development

Any instructor teaching online/hybrid or web-enhanced courses must participate in the Faculty Certification Program in Mastery of Skills for Virtual Media and Technology Supported Instruction. The Instructor Certification Program focuses on mastery of the Learning Modules used to publish and present content that enables instructors to organize related course materials. The Certification is made up of three parts: basic, intermediate, and advanced. These workshops are structured around topics and exercises that encourage interaction and ease the transition from a face-to-face course to an online/hybrid course. Instructors are responsible for course design and content using learning modules.

Basic Certification

This Certification is focused on training faculty in the use of virtual media and technologies to incorporate courses within Blackboard™ platform. Practical aspects of designing exams and assignments on the platform, the use of Blackboard Collaborate Ultra to create virtual spaces and synchronous sessions, and theoretical aspects of designing instructional materials to integrate into an online course such as: learning objectives, instructional material, learning activities and interaction, use of references and citations with APA format and design of courses following the ADA Law are covered.

Intermediate Certification

This Certification is focused on training faculty members in the implementation of tools that promote academic integrity in courses within Blackboard™ platform. The SafeAssign tools, Creation of "Pools" of questions for exams and use of Respondus Lockdown Browser and Respondus Monitor are covered.

Collaboration and communication tools are covered as part of the interaction in a course to enhance the teaching-learning process between students and content, students and

teacher, and students and students. Among these tools are the creation of discussion forums, blogs, journals, and wikis. Also, interaction activities such as creating announcements, publishing teacher contact information, and sending messages and emails through Blackboard™.

Advanced Certification

This certification is made up of five modules that focus on pedagogical approaches that support teaching strategies in virtual and interactive contexts, industry-specific tools and resources, and fundamental mathematics content, situations, and frameworks from a student-centered teaching perspective (does not apply to all academic units). The modules that are presented on in this certification are:

1. Flipped Learning
2. Cooperative Learning
3. Technological Integration Models
4. Interactive Classes Design
5. Evaluation Instruments Design

Blackboard™ Course Copy

The course copy is a tool used for the process of transferring material from one course to another. This is done when the new course structure for the next term/trimester is available. It is the responsibility of the Blackboard™ system administrator to copy course material from one quarter to the next.

Blackboard Administrator

The Blackboard™ System Administrator will post information about:

1. Scheduled Blackboard™ system outages.
2. Announcements of plans for Blackboard™ system upgrades.
3. Creation and modification of Blackboard™ training material.
4. Planning and scheduling of Blackboard™ training workshops.
5. Creation and update of the Blackboard™ policy and procedures.
6. Support Blackboard™ users with technical problems and issues.

VEIL Technical Support

All requests for technical support will be answered within a period of no more than 24 hours, including weekends and holidays. Users of the Blackboard™ platform must include the following information when requesting technical support:

If you are a student:

1. Name and Surname
2. Student ID number
3. Name of the course and Section
4. Professor’s name
5. Detailed explanation of the problem
6. Screenshot - (In case you get a message or error screen)

If you are an instructor or administrator:

1. Name and Surname
2. Name of the course and Section
3. Detailed explanation of the problem
4. Screenshot - (In case you get a message or error screen)

Technical support will be offered through the "ticket" system https://studentservice.pupr.edu, whether for faculty, students and/or administrators.

Blackboard™ System Information

Blackboard™ System may require periodic downtime to apply security updates, patches, system resets, system upgrades, and other scheduled maintenance to it. Advance notice of any scheduled downtime will be given. All routine maintenance for Blackboard™ is scheduled during the early morning hours. It is the instructor's responsibility to maintain an archive of all course material in case of system failure.

Copyright Regulations

Copyright law and fair use guidelines allow instructors to provide access to copyrighted materials using Blackboard™ System. Persons using the PUPR Blackboard™ System are strongly encouraged to respect the property of others by obeying copyright laws and seeking permission, when necessary, before using the work of others.

Family Educational Rights and Privacy Act (FERPA)

The Polytechnic University of Puerto Rico collects and maintains student information that facilitates the educational development of students and the effective administration

of the university, in order to guarantee the rights of privacy and access as stated by the Law of Privacy and Educational Rights of the Family of 1974 (Buckley Amendment, 20 USC 1230, 1232). More information on the FERPA Guidelines: http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

Academic Integrity: Blackboard™ and Respondus

Students must adhere to the following notifications displayed in course announcements on Blackboard:

Academic Honor Promise

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

Terms 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 the Polytechnic University of Puerto Rico and its online courses. With respect to any content posted by you in connection with a course, you represent and warrant to PUPR that you (a) own the copyright to the content, (b) obtained appropriate consent for use of the content, or (c) are legally using and/or publishing the content. With respect to any content to which you (a) do not own the copyright, (b) have not obtained proper consent for use, or (c) are not otherwise legally using, you may not copy, reproduce, publish, distribute, modify, create derivative works from, rent, lease, sell, transfer, display, transmit, compile or compile in a database, or otherwise 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, printed files or computer-readable files. You may not copy, reproduce, publish, distribute, modify, create derivative works from, rent, lease, sell, transfer, display, transmit, compile or compile in a database, or in any way commercially exploit the design or other features of any course. You may not store any course owned by PUPR or licensed to PUPR in any form or medium, including, but not limited to, printed files or computer-readable files.

Copyright Notice

Materials on this course website may be subject to US and international copyright laws. Materials on this course website are only for the use of students enrolled in this course for purposes associated with this course and cannot be preserved or disseminated further.

Information Technology Acceptable Use Policy

Summary

The intentions of the Information Technology (IT) Department to publish an Acceptable Use Policy follow the established culture of openness, trust, and integrity of the PUPR. The IT Department is committed to protecting PUPR employees and the Institution from illegal or harmful actions by individuals, either knowingly or unknowingly.

Systems related to the Internet/Intranet/Extranet, including, but not limited to, computer equipment, software, operating systems, storage media, network accounts that provide email, WWW and FTP browsing, are the property of PUPR. These systems will be used for commercial purposes in the interest of the University during normal operations.

Effective security is a team effort that involves the participation and support of all PUPR employees and affiliates who deal with information and/or information systems. It is the

responsibility of each user of this equipment to be aware of these guidelines and to conduct their activities accordingly.

Objective

The purpose of this policy is to outline the acceptable use of computer equipment at the PUPR. These rules exist to protect the employees of the PUPR. Inappropriate use exposes PUPR to risks that include virus attacks, compromise of network systems and services, and legal problems

Scope

This policy applies to PUPR employees, contractors, consultants, temporary employees, and other workers, including all personnel affiliated with third parties. This policy applies to all equipment that the PUPR owns or leases, either directly or indirectly (grants).

Policy

General Use and Ownership

1. Although the administration of the PUPR network wants to provide a reasonable level of privacy, users should be aware that the data created in the institutional system remains the property of PUPR. Given the need to protect the network of the PUPR, the administration cannot guarantee the confidentiality of the information stored in any device on the network that belongs to the PUPR.
2. Employees are responsible for exercising good judgment as to the reasonableness of personal use. Each department is responsible for creating guidelines for personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should abide by departmental personal use policies and, if there is any uncertainty, should consult their supervisor or manager.

3. IT recommends that all information that users consider sensitive or vulnerable be encrypted.
4. For network security and maintenance purposes, authorized persons can monitor devices, systems, and network traffic at any time within PUPR.
5. PUPR reserves the right to audit networks and systems periodically to ensure compliance with this policy.

Security and Privileged Information

1. The user interface for the information contained in the systems related to the Internet/Intranet/Extranet must be classified as confidential or non-confidential, as defined by the confidentiality regulations of the PUPR. Some examples of confidential information include, but are not limited to, private companies, competitor-sensitive business strategies, trade secrets, specifications, customer lists, and research data. Employees must take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords safe and don't share accounts and/or account information. Authorized users are responsible for the security of their passwords and accounts. System level passwords must be changed quarterly, user level passwords must be changed every six months.
3. All personal computers, laptops, and workstations must be secured with a password-protected screen saver with automatic activation timed for 10 minutes or less, or by logging off (via control-alt-delete to Windows users) when the node is going to be unattended.
4. Since the information contained in laptops is particularly vulnerable, special care must be exercised.
5. All employees' messages originating from a PUPR email address to stakeholders must contain the official disclaimer stating that the opinions expressed are strictly their own and not necessarily those of PUPR, unless the message is carried out within the scope of the functions of the company.

6. Unless department or group policy prevails, all nodes used by the employees that are connected to the PUPR Internet/Intranet/Extranet, whether owned by the employee or PUPR, will be continuously running the PUPR software. Virus detection with an updated virus database.
7. Employees should exercise extreme caution when opening email attachments received from unknown senders that may contain viruses, email bombs or Trojan horse code.

Unacceptable Use

The following activities are, in general, prohibited:

1. Employees may be exempt from these restrictions in the performance of their legitimate job responsibilities (for example, system administration personnel may need to disable a node's network access if the node is disrupting services of production).
2. In no case is a PUPR employee authorized to engage in an activity that is illegal under local, state, federal, or international law, while using PUPR-owned resources.
3. The lists that follow are not exhaustive but are intended to provide a framework for activities that fall under the category of unacceptable use.

System and network activities

The following activities are strictly prohibited:

1. Violate 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, installing, or distributing "hacked" or other hacked products such as software whose uses are not duly authorized by the UPPR.
2. Making unauthorized copying of copyrighted material, including, but not limited to, digitizing, and distributing photographs from copyrighted magazines, books or other

resources, copyrighted music, and installing any software copyrighted for which PUPR or the end user lacks an active license, is strictly prohibited.

3. Exporting software, technical data, encryption software or technology, in violation of international or regional export control laws, is illegal. The IT department should be consulted prior to exporting any questionable material.
4. Introducing malicious programs onto the network or server (for example, viruses, worms, Trojan horses, email bombs, etc.)
5. Reveal your account password to others or allow other people to use your account. This includes family and other household members when working from home.
6. Using a PUPR computer asset to actively participate in the acquisition or transmission of material that is in violation of sexual harassment laws or workplace hostility laws in the user's local jurisdiction. See Title VII of the Civil Rights Act of 1964, as amended, the Age Discrimination in Employment Act of 1967, and the Americans with Disabilities Act of 1999.
7. Make fraudulent offers for products, items, or services from any PUPR account.
8. Cause security breaches or communication interruptions in the network. Security breaches include, but are not limited to, accessing data that the employee is not intended to receive or connecting to a server or account for which the employee is not expressly authorized to access, unless these responsibilities are within the exercise of regulate their duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and information routing code forged for malicious purposes.
9. Port scanning or security scanning is expressly prohibited, subject to proper management, prior notice, and approval from the IT Department.
10. Perform any form of network monitoring that intercepts data not intended for the employee's node unless this activity is part of the employee's normal job.
11. Circumvent the authentication or security of any node, network, or account.
12. Interfere with or deny service to any user other than the employee's node (e.g., denial of service attack).

13. Use any program or script/command or send messages of any kind, with the intention of interfering with or disabling the session of the user's terminal, through any means, either locally or through of the Internet/Intranet/Extranet.

Email and communication activities

1. Sending unsolicited mail messages, including sending "junk mail" or advertising material to individuals who did not specifically request such material.
2. Any form of harassment or violation of federal and state laws through email, telephone, whether through the language, frequency, or size of the messages.
3. Unauthorized use or falsification of email header information.
4. Request email to move (forward) any other email address, for an account other than the sender's, with the intent to harass or gather responses.
5. Create or send "chain letters", "Ponzi" or other pyramid schemes of any kind.
6. Use unsolicited email from PUPR networks on behalf of other Internet/Intranet/Extranet service providers or to advertise any service hosted by PUPR or connected via the PUPR network.
7. Post the same or similar non-commercial messages to a large number of Usenet newsgroups.

Bullying (Cyber Bullying)

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

1. Using institutional resources in order to annoy, harass, terrorize, intimidate, threaten, offend, or annoy another person through the transmission of obscene language, images or other materials or threats of bodily harm to the recipient or others.
2. Using institutional resources to contact another person with the intent to harass or annoy, if no actual message is being communicated, and/or where there is no

purpose of legitimate communication, and in which the recipient has expressed his or her desire for communication to cease.

3. Using institutional resources to contact another person regarding a matter that one does not have the legal right to communicate once the recipient has provided reasonable notice that he or she wishes such communication to cease.
4. Use institutional resources to disturb or harm members of the academic community.
5. Using institutional resources to invade privacy, academic or otherwise, or threaten to invade the privacy of another.

If you are offended by a post, please consider the following before responding:

- Does your publication contribute positively to academic discussion?
- How would you respond if you were in a face-to-face situation?
- Would this situation be better resolved by the intervention of your instructor rather than the individual involved?
- In the event of a post, you have the option of contacting your instructor privately instead of escalating the situation in a public online setting.

Notice of Confidentiality

This is a privileged and confidential communication from the Polytechnic University of Puerto Rico (the sender and the person to whom it is addressed). Any use of the content of the message by a person to whom the message is not addressed is illegal and is strictly prohibited. No person may divulge, copy, or alter the content of this message. If you received this communication in error, please destroy it together with any attachments that may have been included.