GENERAL POLICY FOR THE USE OF PASSWORDS OF THE PONTIFICAL CATHOLIC UNIVERSITY OF PUERTO RICO

I. Introduction

A. Justification

All members of the university community of the Pontifical Catholic University of Puerto Rico (hereinafter *University* or PCUPR) require credentials to access equipment, programs, applications and other technological resources. Each credential includes a username and password. The selection of a password is a fundamental aspect of information security. A poorly selected password can result in unauthorized access to private and confidential information and in the misuse of PCUPR's information technology resources. Professors, students, non-teaching staff and any person who has access to PCUPR's information technology resources (hereinafter *Users*) have the responsibility to follow the appropriate standards, as described below, to select and protect your passwords.

B. Objectives

The General Policy for the Use of Passwords of the Pontifical Catholic University of Puerto Rico has the objective of providing the standards for the creation of strong passwords. It also intends to establish the rules and procedures for the protection and frequency of changing passwords.

C. Scope

The General Policy for the Use of Passwords of the Pontifical Catholic University of Puerto Rico applies to all Users who have or are responsible for an account or form of access that requires a password. This policy applies to users of institutional computers, *WiFi* service, institutional email, G Suite for Higher Education applications, Pioneer Access Portal, Banner System, Moodle Platform and Ellucian Go. It also applies to all information technologies resources that belong to or are managed by the Pontifical Catholic University of Puerto Rico, or other resources provided by the University through contracts or agreements.

II. Policy

A. Password Creation

1. Every password created by the Users or by the Administrators of any system, equipment or technological service must have at least 8 characters.

2. The types of characters required to create the password will depend on the number of these:
    i. If the password is 8 to 11 characters long, it must contain uppercase letters, lowercase letters, numbers, and special characters (@#$%()^&*/=+*).
    ii. If the password is 12 to 15 characters long, it must contain uppercase letters, lowercase letters, and numbers.
    iii. If the password is 16 to 19 characters long, it must contain an uppercase letter and a lowercase letter.
    iv. If the password is 20 or more characters long, you can use any character you want.

3. It is strongly recommended to use a password phrase (e.g. I used to like to dance but not anymore). The advantage of using a phrase as a password (Passphrase) is that it is more complex, but easier to remember.
4. Your password cannot be a name, username, company name, or a full dictionary word. It should also not include names of relatives, pets, and coworkers. It must not have data on the date of birth, physical or postal address or telephone numbers.
5. Passwords to access institutional technological services must be unique.

B. Password Protection

1. The password cannot be shared with anyone, including co-workers and supervisors.
2. Do not discuss passwords in front of others.
3. Do not disclose the password by email, chat, text message or any means of electronic communication.
4. Passwords should not be written down or physically stored anywhere in the office.
5. Passwords should not be stored in unencrypted electronic formats (e.g. IPhone Notes or Google Keep). Use encrypted Password Management services (e.g. Dashlane or LastPass).
6. When using PUCPR's technological services, do not enable the automatic login function, both on institutional computers and on cell phones and tablets.
7. Institutional passwords should not be used to access personal accounts or services.
8. Do not use the *Remember Password* function in web pages and applications.

C. Password Change

1. Users must change passwords every 3 months.
2. Administrators of systems, equipment or technology services must change passwords every 3 months.
3. Previously used passwords cannot be used again.

III. Non-Compliance and Disciplinary Actions

Users who fail to comply with the provisions of this Policy assume all responsibility, and relieve the PCUPR of it, for the damages suffered by them, or caused to third parties, as a result of such non-compliance.

Users are required to report in writing to the Executive Director of the Office of Telecommunications and Information Technologies (director_tti@pucpr.edu) any violation of this Policy to avoid its repetition or repercussions to other users. Any violation of this Policy is subject to legal consequences as they arise from state or federal legislation and/or disciplinary sanctions as established by University regulations.

IV. Amendments

This Policy may be amended, from time to time, by the Administrative Board of the PCUPR, which will notify the Users of the changes adopted by the means it deems appropriate.

This policy was approved by the Administrative Board on February 11, 2019.