INFORMATION SECURITY PROGRAM

Introduction

Columbia Central University (CCU) as a means to protect, manage and conserve the integrity of our students information, being their privacy the most important thing, establishes the following internal safeguards in this program.

Legal Base

The Information Security Program CCU is based on the compliance with different regulations: state, federal and institutional. These are: Student privacy protection policy (FERPA & FTC), Policy prohibiting the use and disclosure of the social security number (Act 186) and the Policy on the acceptable use of technology, all of which are published in the Institutional Policies Manual and on the webpage www.columbiacentral.edu, Student Consumer Information.

Administrative Security

Every employee is responsible of managing and making good use students' personal information as well as of establishing security measures to safeguard the confidentiality and integrity of the information they manage. Every employee becomes custodian of the documents they were trusted with, and must avoid their loss, alteration and destruction.

The information that is shared or paired with other agencies, such as the Selective Service, Veterans Administration, Social Security and National Student Loan Data System (NSLDS), among others, will be with the purpose of helping our students and this information is of private nature.

Physical security

The Registrar's Office is custodian of active and inactive student records. These records contain diverse documents, such as: admission application and admission documents, enrollments, withdrawals and any other document necessary up until degree conferment. The records are filed in a locked vault, and transcripts up to 2004 are kept in fireproof file cabinets in a vault with fire-suppression system. After that year, transcripts are stored in the Columbia System, which is a Microsoft SQL (Server Query Language) database system; transcripts are stored for life.

The Registrar's Office will conserve the records for at least seven (7) years, after the last official academic activity.

The Financial Aid files will be conserved in the vault for six (6) years after their last year of study. After this, they will be destroyed as established in the Federal Student Aid Handbook.

As a security measure, computer screens will not be visible to those who visit the offices, and student information, including accounts, grades and others, will not remain on screen; if they are on screen, they should have a screensaver with a password.

An employee, before leaving the office, should take security measures with student documents remaining on his desk, such as placing the documents in drawers, or shutting the door and turning the lights off.

If there is a student from the work-study program assisting, he/she will sign a non-disclosure statement before being employed.

In the same manner, all personnel with access to student information, including employees and faculty, will protect the privacy that this entails; making good use of the information and will not use or leave screens in plain view of unauthorized people. If any person suspects or knows of any employee or faculty member who is misusing the information, he/she should notify the Student Affairs representative or the Chancellor, who will act as necessary.

Technical security

The information in the Columbia System will be maintained and stored through a daily back-up conducted automatically online, in the Microsoft Azure cloud and physically. In case of a disaster, an attack, intromission or a system failure, the technical personnel will reinstall the system (after repairing or replacing servers if necessary) using the most recent back-up. As a security measure, access to the

Computer Room, where the servers are located, will be limited to the administrator and technical personnel who legitimately work with said servers. Security codes in the computers and Columbia System will be changed every ninety (90) days.

Prepared by:	José A. Rivera, BBA Information System Administrator
Date:	February 27, 2017
Aproved by:	Daritza Mulero, MBA President
Date:	February 27, 2017
Effective date:	February 27, 2017