USE OF INFORMATION TECHNOLOGY RESOURCES

GUIDELINES FOR USE OF INFORMATION TECHNOLOGY RESOURCES

PCOM Information Technology Services (ITS) resources are provided to students to enhance their learning experience. Utilization of these resources for personal gain or illegal or inappropriate activities is prohibited.

The following are examples of prohibited activity:

- Accessing (e.g., read, write, modify, delete, copy, move) another user's files or electronic mail without the College's approval

- Unauthorized use of network or computer resources
- Attempts to circumvent information security protocols or exploit security loopholes (e.g. bypassing browser configurations; network data capture, etc.)
- Violation of College policies and State, Federal and local laws

Use of the PCOM computer network is for educational and informational purposes. Abuse or inappropriate use of the PCOM Network will be subject to disciplinary action. All students are responsible for using the PCOM computer labs in a professional, efficient, ethical and lawful manner.

Use of the network and PCOM systems is a privilege, which may be revoked at any time for misuse. PCOM information systems are to be used only for assigned purposes and are not to be used for commercial purposes or non-College-related activities. Fraudulent, harassing or obscene messages and/or materials are not to be sent, printed, requested or stored.

All software is licensed to PCOM and may not be copied or distributed. The ITS Department should be contacted regarding licensing, distribution and installation of non-standard software necessary for the support of special projects. Contact the PCOM ITS Department at 215-871-6110 or by email at support@pcom.edu with questions about PCOM's information technology policies.

EMAIL POLICIES

The College email system should be used as the primary source of communication for PCOM users, including students, faculty, staff and administration.

Students are expected to check their PCOM email account daily as this will serve as the official channel for all college-related notifications and updates. Personal email accounts will not to be used for PCOM-related communication.

Students may not use the PCOM group email functions without the permission of the Office of Student Affairs on their respective campus.

Inappropriate use of email, examples of which are described below, is prohibited and will result in disciplinary action:

- The creation and exchange of messages that are harassing, obscene or threatening, including messages containing offensive comments about race, gender, age, sexual orientation, pornography, religious or political beliefs, national origin, or disability.

- The unauthorized exchange of proprietary information or any other privileged, confidential, and sensitive information.

- The exchange of advertisements, solicitations, chain letters and other unofficial, unsolicited email.

- The creation and exchange of information in violation of any laws, including copyright laws, or College policies.

- The misrepresentation of the identity of the sender of an email.

- The use or attempt to use the accounts for political appeals, editorializing, religious messaging or partisan (including issue-partisan) lobbying.

- The use or attempt to use the accounts for personal financial gain in connection with outside (non-College) consulting, business or employment, except as authorized and approved by the College administration.

PCOM ACCOUNT SECURITY

To enhance account security, students are required to update their network password at least once every 180 days. PCOM students can use the ITS Portal at https://reset.pcom.edu/to reset their network password. Users can log in using the network username and current password that they received via email, and then click on "Change Password". Please contact the ITS Service Desk at 215-871-6110 for assistance with password lockouts.

Multi-factor authentication is required for access to all PCOM applications including email. New students will receive instructions to enroll in Duo and Google Authenticator.

To report a Cybersecurity incident contact the ITS Service Desk at 215-871-6110 or support@pcom.edu. For matters that require immediate attention, contact the Chief Information Security Officer at 215-871-6125 or marisani@pcom.edu.

RECORDINGS FOR EDUCATIONAL PURPOSES

Educational course activities, including but not limited to lectures, webinars, and labs may be audio/video recorded and made available to other students in this course. As part of your participation in the course activity, you may be recorded. Pursuant to the Family Educational Rights and Privacy Act (FERPA), the sharing of recorded activities with other students in the course does not require your written consent. If you do not wish to be recorded, please notify the instructor in advance to discuss alternative arrangements.

Under FERPA, any additional release of recordings containing non-directory student educational records or personally identifiable information contained therein requires written consent of a student before it may be disclosed to a third party, unless an exception to this general requirement of written consent applies.

COMPLIANCE

In adhering to these Guidelines, each student contributes to a respectful, secure, and productive learning environment. Non-compliance with the policies outlined in this handbook can have serious consequences, including but not limited to: a warning, disciplinary action, loss of access to PCOM's Information Technology resources, and, in some cases, suspension or expulsion from the College. Moreover, certain actions may also have legal consequences under local, state, or federal laws. We urge

each student to recognize their responsibilities and to use the College's Information Technology resources in a manner that respects the rights and privileges of all PCOM community members.