COLLEGE POLICY 371
COLLEGE COMPUTER USE AND DATA SECURITY POLICY

I. Introduction

The College provides access to technology hardware, software, Internet, and network accounts in support of the educational mission. This policy balances access for faculty, staff and students via College-owned or personally owned systems in accordance with state, federal and industry compliance requirements.

II. Policy

A. AntiVirus Use

All computers connecting to College's network systems physically, wirelessly or remotely must have updated anti-virus software installed, configured and activated. To protect the College's network systems, computers detected with an infection may be disconnected from the network until the infection is removed.

All inbound e-mail services must be directed through the College's spam and anti-virus scanners at the Internet gateway. Once e-mail is scanned, the anti-virus scanners will relay the e-mail to the respective location for delivery.

B. Internet Usage

1. Resources available on the Internet are used to support the College's educational mission. In interacting online, a user's behavior is subject to the College Code of Conduct and Board Policies 071, Statement of Individual Rights, and 074, Statement of Practices Constituting Unacceptable Conduct. Use of the Internet, including email, to create, display, or transmit language and/or materials which violate local, state or federal laws or regulations is strictly prohibited. Such use includes, but is not limited to, the violation of applicable laws regarding copyright and trademark infringement, fraud, forgery, harassment, discrimination, obscenity, libel or slander.

2. Access to the Internet is a privilege and not a right, and is to be available to the entire College community of users. The College reserves the right to terminate any network session at any time. Users, NOT the College or its staff, are responsible for the Internet information selected and/or accessed.

3. The College does not generally monitor Internet use and is not responsible for its content, and consequently has no control over information accessed, either on workstations on campus, or remotely. The College assumes no responsibility and shall have no liability

for any direct, indirect or consequential damages arising from the use of information found on the Internet, or any communications sent through College Internet connections.

C. E-Mail Privacy and Monitoring

1. Individuals should have no expectation of privacy in anything they store, send or receive on the College's email system. However, with the exception of automated scans which monitor email communications for *sensitive content**, the College does not monitor the content of electronic mail as a routine procedure. The College reserves the right to inspect, copy, store, or disclose the contents of electronic mail messages, but will do so only when it believes these actions are appropriate to: prevent or correct improper use of College E-Mail Facilities; ensure compliance with College policies, procedures, or regulations; satisfy a legal obligation; or ensure the proper operations of College E-mail facilities or Data Network. *Reference: Administrative Procedure 651, "Disclosure of Information About Students."

2. E-mail is stored electronically in the users' account for 366 days. Upon deletion of an e-mail, it will be preserved for no longer than 7 days in the users' "trash". Electronic calendars are stored for one (1) year. Once e-mail is 367 days old, it will automatically be moved to the user's archive within Outlook. Archives will be kept for one year for adjunct faculty and student workers and three years for all other staff and faculty. Should it become necessary to put a "legal hold" on anyone's e-mail, the individual will not be able to delete or remove items from his/her mailbox, including archives, until such time that the legal hold is removed. A legal hold is put on a person's account at the direction of Human Resources and/or legal counsel in the event of potential litigation.

3. Disclaimer: The College makes no warranties of any kind, whether expressed or implied, with respect to the College E-mail services it provides. The College will not be responsible for damages resulting from the use of College E-mail, including, but not limited to, loss of data resulting from delays, non-deliveries, missed deliveries, service interruptions caused by the negligence of a College employee, or by User error or omission. The College specifically denies any responsibility for the accuracy or quality of information obtained through College E-mail except material represented as an official document.

D. Wireless Access

The College grants wireless access to the Internet and network resources as a privilege and must manage them responsibly to maintain the integrity and availability of all wireless information assets. Only wireless access points installed and managed by Information Technology Services (ITS) will be allowed on the College's wireless network.

E. Removable Media

College faculty and staff are responsible for the secure and responsible use of removable media. The College reserves the right to disable or restrict access to USB ports and writable CD and DVD drives on College-owned and maintained systems.

F. Remote Access

Access of the College's network resources remotely shall follow the same policies and procedures as an on-site connection to College network resources.

G. Security and Confidential Information

1. The College, through its employees, will treat all of its information pertaining to students and employees as confidential, disclosing that information only when authorized by the student or employee in question, approved by the appropriate College Official, or required by local, state or federal law. The data stored on the College's network systems remains the property of the College.

2. **Family Education Rights and Privacy Act Provisions (FERPA)** -- Employees at the College may have access to education records which contain personally identifiable information, the disclosure of which is prohibited by the Family Education Rights and Privacy Act of 1974. Disclosure of this information to any unauthorized person (including a parent or a spouse) is contrary to College policy, Reference Administrative Procedure 651, "Disclosure of Information About Students."

3. **Software Copyrights** -- It is the policy of the College to honor the copyrights of all software packages used by or licensed to the College and to recognize the intellectual property rights of the owner. All software run on computers owned or controlled by the College must be purchased and used in accordance with College policies and procedures.

4. **Business Records** -- Any and all records generated by the College, including but not limited to personnel records, payroll records, business and other related records are considered to be confidential. Willful or intentional unauthorized disclosure of such information violates College policy.

5. **System Tampering** -- It is a violation of College policy to intentionally disrupt the performance of the College's computer system or the College network; introduce computer viruses; read, execute, modify or delete any file belonging to someone else without permission; or damage or remove without permission from ITS Department any hardware that supports the College's computer system or College network.

H. System Maintenance – Authorized College staff may monitor equipment, systems and network traffic at any time. Personal privacy of information stored on the College's network systems is not guaranteed. Information stored on the College's network systems may be

copied, archived, or deleted. Electronic files not accessed may be removed to off-line storage and eventually erased.

I. Incident Response

HACC recognizes the importance of rapidly and methodically responding to data/network security incidents in order to protect and preserve the confidentiality, integrity and availability of College assets and data. HACC educates users about the College's response and employee roles in assisting in the protection of College assets and assuring the continuity of business operations during orientation.

Adopted: August 4, 1998 (Vol. 36, Res. 15)
Amended: June 6, 2000 (Vol. 37, Res. 122)
Amended: April 3, 2012 (Vol. 49, Res. 100)
Amended: August 7, 2012 (Vol. 50, Res. 14)