HEARTLAND COMMUNITY COLLEGE

SECURITY & APPROPRIATE USE POLICY

(REVISED AUGUST 2009)

Contents

1.0 INTRODUCTION 3
2.0 DEFINITIONS 3
2.1 Authentication 3
2.2 Authorization 3
2.3 IT 3
2.4 Individual Storage 3
2.5 Information 4
2.6 Login Name 4
2.7 Single Sign-On 4
2.8 System Administrator 4
2.9 Technology Resource 5
2.10 User 5
2.11 User Account 5
3.0 EMPLOYEE ACCESS TO TECHNOLOGY RESOURCES AND INFORMATION 5
3.1 Eligibility for Access 6
3.2 Sharing of System Accounts 6
3.3 Position Changes 6
3.4 Disabling User Accounts 6
4.0 APPROPRIATE USE OF TECHNOLOGY RESOURCES 6
4.1 General Restrictions 7
4.2 Other Applicable College Policies 7
4.3 Physical Misuse of Resources 7
4.4 Use of Resources and Information for Profit 7
4.5 Software 7
4.5.1 Software Licensing 7
4.5.2 Software Application Availability 8
4.5.3 Software Installation/Removal 8
4.5.4 Software Reproduction 8
4.6 Hardware 8
4.6.1 Hardware Installation/Removal 8
4.6.2 Standard Media Device Use 8
4.7 Electronic Communications 9
4.7.1 Responsibilities 9
4.7.2 Requirements 9
4.7.3 Restrictions 9
4.8 Internet Use 10
4.8.1 Downloading/Uploading 10
4.8.2 Peer-to-Peer File Sharing 11
4.8.3 Pornography 11
4.9 Network Bandwidth Use 11
4.10 Duplication/Reproduction of Copyrighted Materials 11
4.10.1 IT Duplication Requests 11

4.10.2 Duplication/Reproduction of College-Owned Information 12
4.10.3 Duplication/Reproduction of Personally-Owned Information..... 12
4.10.4 TEACH 12
4.11 Personal Use..... 12
4.12 Upholding the Mission..... 12
5.0 EMPLOYEES' ROLE IN INFORMATION SECURITY 12
5.1 Passwords..... 12
5.1.1 Password Sharing..... 13
5.1.2 Failed Password Attempts..... 13
5.2 FERPA 13
5.2.1 Student Information Maintenance..... 13
5.2.2 Directory Information 13
5.2.3 Personally Identifiable Information 14
5.2.6 FERPA-Related Requests and Demands from Students..... 15
5.3 GLBA..... 16
5.3.1 Heartland Community College GLBA Compliance 16
5.4 Payment Card Industry 17
5.3.1 Heartland Community College PCI DSS Compliance 17
6.0 PRIVACY 18
6.1 ECPA 18
6.2 System Maintenance 18
6.2.1 Deleted Files 18
6.2.2 Archive and Backup Files..... 19
6.3 Access without Consent..... 19
6.3.1 Emergency Entry 19
6.3.2 Reasonable Cause 19
6.3.3 Temporary Access Request..... 19
6.3.4 File Ownership Transfer 19
6.4 Employment Termination 19
7.0 CONSEQUENCES FOR POLICY VIOLATIONS..... 20
8.0 POLICY DEVELOPMENT AND MAINTENANCE..... 20

Effective August 1, 2009, this policy replaces any prior policies related to technology resources and information.

1.0 INTRODUCTION

Heartland Community College (HCC) strives to remain a technologically forward institution. As such, the College is obligated to safeguard its technological infrastructure by establishing security and appropriate use guidelines for all users of HCC technology resources. The need for such a policy originates from access to both digital information and physical resources. Each member of the College community is afforded a level of access that is appropriate for the tasks they perform. Access is a privilege. It is accompanied by a responsibility to conduct activities within the parameters of this policy in an effective, ethical, and lawful manner. Policy violations will be addressed in accordance with Section 7.0 herein.

The misuse of any technology resource as described herein is not limited to the unauthorized or illegal use of that resource. Simply having access to a particular resource does not necessarily imply all usage of that resource is appropriate. Similarly, legality does not necessarily constitute appropriateness.

2.0 DEFINITIONS

Below is an alphabetical list of terms and their definitions as deemed appropriate for the purposes of this document.

2.1 Authentication

"Authentication" refers to the process a technology resource carries out in order to securely identify a user and verify that that user is who he or she claims to be. Authentication can occur in a number of ways with the most common method being a unique user name paired with a password. Other less common methods for authentication include biometric scans and smart cards with magnetic strips or bar codes.

2.2 Authorization

"Authorization" refers to the specific technology resources and the amount and type of information in each of those resources that a user is allowed to see and/or use. Authorization, also called "access", for each user is unique and is assigned based upon an individual's requirements for adequately, effectively, and efficiently performing the tasks of his or her official position.

2.3 IT

The abbreviation "IT" refers to the Information Technology Department and/or its members.

2.4 Individual Storage

"Individual storage" refers to electronic file storage on a network drive that is named and reserved for use by one specific employee. Storage areas assigned to individual employees are used for storing files that are not typically needed by other College employees. Information residing in individual storage is backed up by the College. While

commonly referred to as "personal storage" or the "home directory," individual storage is considered to be property of the College, regardless of its content.

2.5 Information

"Information" refers to any data owned by the College. This includes any data stored on or used by any College-owned or College-licensed technology resource, and it includes any College related data such as student grades and IDs, even if that data were being stored on or used by equipment that is not College-owned. For example, in this document the term "information" may refer to student grades or other data being stored on personally-owned hardware such as digital assistants, laptops, home computers, and portable storage devices.

2.6 Login Name

"Login name" refers to a unique alphanumeric identifier that is assigned to each employee. Many technology resources at the College require employees to enter a login name and password in order to gain access to the resource. Once a user has authenticated using a login name and password, authorization to view and/or use specific information within the confines of the technology resource currently being accessed is granted based on the login information. For example, an employee who uses his or her login name and password to be admitted into the e-mail system will, upon entering the system, have access only to his or her specific mailbox and any authorized shared mailboxes.

2.7 Single Sign-On

"Single sign-on" refers to the ability of a user to access multiple technology resources with one successful authentication to a primary account, which at HCC is a user's network account. For example, a successful sign-on to myHeartland also opens access to individual storage, IRIS, WebCT/Blackboard, and email account without the need to re-enter a login name and password for every system.

2.8 System Administrator

"System administrator" refers to certain employees in the Information Technology Department whose official positions at the College include duties related to network and telecommunication systems. These duties include, but are not limited to, troubleshooting and maintaining the College's network, setting up and maintaining user accounts, and assigning and monitoring file storage space such as individual, voice mail, and e-mail storage.

2.9 Technology Resource

"Technology resource" refers to all College-owned or College-licensed electronic or digital hardware and software products or systems, including, but not limited to, the following:

- network services (such as shared and personal file storage, Internet access, e-mail, and printing services)
- mission critical systems (such as PeopleSoft, SpeedScan, Compass, WebCT/Blackboard)
- telecommunication systems (such as telephone, cellular phone, voice mail, and fax systems)
- desktop equipment (such as computers and peripherals in offices, classrooms, and common areas)
- supplementary technology devices (such as scanners, digital cameras, video cameras, projectors, document cameras, TVs and VCRs, ITV systems, satellite, and public display systems)
- mobile equipment (such as laptops and other personal computing devices)
- retail software (such as Windows and Microsoft Office)
- specialized applications (such as Peachtree, MathType, and Photoshop, as well as access to research databases such as FirstSearch)

Note: This list is representative. It cannot be exhaustive as technology resources at the College are constantly changing. This policy applies to all technology resources regardless of whether or not an individual item is specified in this list.

2.10 User

"User" refers to anyone who accesses or uses any College-owned or College-licensed technology resource. Such persons include, but are not limited to, students, employees, community members, vendors, contractors, and subcontractors. A personal network or other user account is not required to be considered a user. Also, neither the location of the user nor the location of the resource is of consequence. Persons accessing systems remotely, as is possible with WebCT/Blackboard or library databases, are also considered users and are required to operate within the parameters of this policy.

2.11 User Account

"User account" refers to the information stored by a technology resource that identifies the user for authentication purposes. For example, the user account stores the password needed to authenticate a login name. Typically a user account also stores information on what resources a user has authorization to view and/or use within that particular system. For example, a user's network account allows access to the HCC network as well as specific drives on that network, and a WebCT/Blackboard account allows access to an individual's specific online classes.

3.0 EMPLOYEE ACCESS TO TECHNOLOGY RESOURCES AND INFORMATION

Many technology resources at Heartland Community College require user authentication and authorization via a personal account. The rules and responsibilities described in this document apply to both network accounts and accounts in all other systems.

3.1 Eligibility for Access

All employees are eligible to receive a network account, e-mail account, and individual storage space on the network. Accounts that provide access to other systems such as PeopleSoft or SpeedScan are granted based upon the responsibilities of the employee's official position and/or upon the request of the employee's supervisor. Supervisors may submit requests for changes to an employee's access rights to the IT department.

3.2 Sharing of System Accounts

Login names are non-transferable. A login name is to be used only by the employee to whom it is assigned. Similarly, passwords, by definition, are secret and may not be shared with any other person under any circumstances. Allowing another individual to use a login name and password, either knowingly or negligently, is a violation of the security and appropriate use policy. Policy violations will be addressed in accordance with Section 7.0 herein.

Note: Employees who request assistance from IT while using the login name and password of another user will be denied assistance. Additionally, violation of the security and appropriate use policy will be documented and reported to the Director of Technology Support Services.

3.3 Position Changes

Reassignment of authorizations resulting from internal employment changes are managed on a case-by-case basis. If an employee moves to a different department, his or her login name and e-mail address will remain the same. However, all other access that was originally granted based on the duties of the employee's prior position will be suspended. It is the responsibility of the employee's new supervisor to submit a new request for authorizations appropriate to the new job duties.

3.4 Disabling User Accounts

A request to disable account access to College technology resources may be put forth by an employee's supervisor, the Director of Human Resources, or a member of the Cabinet. Such requests will be carried out by a College system administrator. Also, a system administrator, at his or her own discretion, may disable an employee's account in order to protect the integrity of the College network.

User accounts for terminated employees will be disabled upon Human Resources notification to IT of such termination.

4.0 APPROPRIATE USE OF TECHNOLOGY RESOURCES

Information technology plays an integral role in allowing employees to accomplish their assigned duties. There is an ever-growing array of computing services that empowers employees to create, access, evaluate, update, distribute, store, and report on information using a variety of media and formats. Understanding that a College employee may be severely hindered in the ability to perform his or her duties if he or she lacks access to appropriate technology resources, Heartland Community College provides such resources in support of the various activities of the

institution. These resources are intended for the sole use of Heartland employees, students, and other authorized users. The use of these technology resources is a privilege and demands individual responsibility for security and appropriateness.

It is impossible to identify every situation that pertains to proper or improper use of technology resources. The list below describes some general guidelines regarding prohibited activities, and focuses on some of the more significant responsibilities an employee accepts when he or she chooses to use a College-owned or College-licensed technology resource.

4.1 General Restrictions

Use of technology resources shall be within the spirit or principles of this policy. No one shall attempt to circumvent or undermine the intent of this policy. Discovering and operating within a loophole of the policy constitutes unacceptable behavior and will be considered a policy violation. Policy violations will be addressed in accordance with Section 7.0 herein.

4.2 Other Applicable College Policies

Many information technology functions parallel familiar activity in other formats making existing College policies important in determining what use is appropriate. For example, the College's copyright policy applies not only to hard-copy documents, but also to electronic documents. Also, the College's harassment policy applies not only to face-to-face harassment, but to harassment via electronic means as well. For statements defining other applicable College policies, consult the Employee Handbook.

4.3 Physical Misuse of Resources

General physical misuse of technology resources such as any unauthorized loan, unauthorized removal of equipment from campus, theft, damage, or destruction is strictly prohibited.

4.4 Use of Resources and Information for Profit

Using HCC technology resources for commercial purposes including, but not limited to, the promotion or day-to-day operation of "for profit" and/or privately-owned businesses or commercial ventures is strictly prohibited. This includes any use of College-owned information or equipment for solicitation purposes.

4.5 Software

4.5.1 Software Licensing

It is the responsibility of the IT department to ensure that the College remains in legal compliance with all software licenses, subscriptions, and contractual agreements regardless of the budget from which a software resource was funded. Consequently, IT is responsible for storing and maintaining application software, as well as for understanding and ensuring College compliance with software license agreements.

4.5.2 Software Application Availability

All College computers are equipped with a set of standard software applications including, but not limited to, programs such as Microsoft Windows, Microsoft Office, and Internet Explorer.

Additional applications may be available upon request. Procedures for requesting additional applications are maintained within IT.

4.5.3 Software Installation/Removal

The IT department is responsible for installing and removing all software applications. Employees are prohibited from loading applications or utilities on any workstation unless given specific authorization from IT. Similarly, employees are prohibited from removing applications or utilities from a workstation without IT authorization. The IT department retains the right to remove any personal or other non-College-owned applications downloaded from the Internet or otherwise installed on a workstation, regardless of whether or not previous authorization was granted. Removal of software may be necessary in a variety of situations such as restoring functionality of College systems, resolving policy violations, or ensuring compliance with licensing requirements.

4.5.4 Software Reproduction

Reproduction or duplication of College-owned or College-licensed software using any type of media or through any type of electronic transmission without prior authorization from IT is prohibited.

4.6 Hardware

4.6.1 Hardware Installation/Removal

The IT department is responsible for acquiring, installing, moving, and removing all hardware devices in all campus common areas such as classrooms, computer labs, and office areas.

In assigned office spaces, employees outside of the IT department may only connect or disconnect hardware devices with prior authorization from IT. Authorization for many peripheral devices such as mice and keyboards can be obtained by calling the IT hotline. Personal devices connected to College resources must be identified as such, preferably with a label identifying the owner. Whether or not authorization was originally granted, the IT department retains the right to disconnect any personally-owned equipment connected to College resources.

4.6.2 Standard Media Device Use

Employees may use College-owned or personal media and memory devices such as diskettes, USB drives, CD-ROMs, etc. with any College-owned equipment without prior authorization from IT. However, these devices may not be used to copy, transfer, or remove sensitive or protected information from College-owned or

College-licensed technology resources unless such activity is authorized by the employee's supervisor.

4.7 Electronic Communications

The following policy guidelines apply to all forms of electronic communication used by College employees when communicating using College-owned or College-licensed technology resources. Electronic communication methods include, but are not limited to, phones, voice mail messages, e-mails, instant messaging, online newsgroups, faxes, radios, and College-owned cell phones. Except as otherwise excluded by law or collective bargaining language, all devices, files, messages and storage associated with such electronic communications are the property of the College regardless of their content.

Note: The College recognizes issues surrounding intellectual property rights and will make every effort to respect the rights of the individual. In situations where ownership of content is in question, the College will abide by the law and established legal precedence with regard to those issues.

4.7.1 Responsibilities

The e-mail system is the primary means by which College information is disseminated. All employees are required to check their e-mail for distribution of such messages at least one time per week unless on an official leave.

4.7.2 Requirements

A general e-mail confidentiality notice is automatically appended to all e-mail messages sent via the College's e-mail system. This notice identifies Heartland Community College as the owner of the information and provides instructions for recipients who have received a message in error. Employees may not block, hide, or cancel this notice.

4.7.3 Restrictions

Etiquette commonly used for traditional written communications should be used as a guideline for electronic communications. Every employee should be continually aware that he or she represents Heartland Community College with every communication he or she sends. Inappropriate communications are prohibited. Instances of inappropriate electronic communications include, but are not limited to, the following:

4.7.3.1 Fraudulent Communications

Any electronic communication sent under an assumed name or modified address, or with the intent to obscure the origin, date, or time of the communication is considered fraudulent and is prohibited.

4.7.3.2 Harassing Communications

Any electronic communication that constitutes harassment as defined by the Heartland Community College harassment policy is prohibited.

4.7.3.3 Mass Communications

Employees may not knowingly create or send unapproved communications that will generate excessive network traffic. Examples of this type of communication include chain letters, unwelcome e-mails, e-mail bombs, viruses, hoaxes, and/or other mass communications that may potentially degrade the performance of the network infrastructure.

4.7.3.4 Confidential Personnel Communications

In keeping with the College's policies and collective bargaining agreements, disciplinary activities are to take place in-person between a supervisor and his or her subordinate. Employees are prohibited from using direct e-mail communications and/or voice mail to address confidential disciplinary issues with other employees. Similarly, employees are asked to refrain from criticizing others using e-mail and/or voice mail.

The e-mail system may be used to transmit files or documentation related to disciplinary activity as long as such files are sent as attachments and the original files or documentation are stored elsewhere (i.e., the information should not exist solely in the e-mail system).

Note: Due to the confidential nature of such communications, employees are encouraged to submit claims of harassment or other policy violations using methods other than e-mail. However, if such a claim is submitted via the e-mail system, the claim will be addressed, regardless of the method of communication.

4.7.3.5 Copyright

Electronic communications are prohibited from including any information that violates the College's copyright policy or any state or federal copyright law.

4.8 Internet Use

Information available via the Internet may be distracting, objectionable, or even disturbing. Since many technology resources may be visible and/or audible to others, sensitivity in viewing and/or listening to such material is required. Users who disturb or distract others may be asked to stop their activities or leave a particular area.

4.8.1 Downloading/Uploading

Downloading is when data is transferred from a main source to a device such as a desktop computer. Conversely, uploading is when data is transferred from a device such as a desktop computer to a main source such as a server. Using College-owned resources to download or upload copyrighted material outside of Fair Use rules without obtaining a copyright release is prohibited. Copyrighted material may include, but is not limited to, audio files, graphics, video files, and electronic publications.

4.8.2 Peer-to-Peer File Sharing

Peer-to-peer (P2P) file sharing occurs when files stored on one computer are sent directly to another computer across the Internet. In a P2P network, each computer functions as a client and a server, with each having equal privileges to download and/or upload files to other computers on the network. Although P2P file sharing is legal; sharing, distributing, or downloading copyrighted material typically is not.

College-owned technology resources may not be used in a P2P network to illegally transfer copyrighted materials. Further, P2P software shall not be installed on any college owned computer in accordance with section 4.5.3 herein.

4.8.3 Pornography

Employees are prohibited from using College-owned or College-licensed technology resources for accessing images, sounds, or messages that are pornographic in purpose. Legal, sexually explicit literary/artistic expressions and materials that are relevant and appropriately related to course subject matter or curriculum are not considered to be pornographic in purpose.

4.9 Network Bandwidth Use

Large-scale distribution of such things as MP3 music or video files or the use of streaming audio or video can cause excessive network loading that may cause a significant decrease in network performance and affect all users. Therefore, no one may knowingly or recklessly download or distribute such data, digital audio or video files, or audio or video streams.

Employees who believe they need to perform these types of actions within the confines of their job responsibilities must contact IT for assistance in completing the task in a manner that will not negatively impact other users.

4.10 Duplication/Reproduction of Copyrighted Materials

Typically, copyrights belong to the original author(s) of a work, regardless of whether a work is published or unpublished. In general, a copyright release is required to legally duplicate or otherwise reproduce copyrighted material. This requirement pertains to all works regardless of the medium on which the work is stored. Some examples of storage media used at HCC that may contain copyrighted material are VHS and 8mm tapes, CDs, DVDs, diskettes, zip disks, and USB devices.

4.10.1 IT Duplication Requests

Requests submitted to IT for duplication of files from one medium to another will be individually evaluated and granted only when the request is acceptable within the confines of the College's copyright policy. For example, at the request of the recording instructor, it is appropriate for IT to copy recordings of classroom presentations from 8mm tapes to VHS tapes to facilitate future viewing of such recordings.

4.10.2 Duplication/Reproduction of College-Owned Information

Duplication and/or reproduction of College-owned copyrighted material in any form without proper authorization and release is prohibited. Neither authorization nor release will be granted for requests that are not in accordance with the College's copyright regulations or that go against federal or state law.

4.10.3 Duplication/Reproduction of Personally-Owned Information

College-owned technology resources, including media, may not be used for the duplication and/or reproduction of personally-owned copyrighted material (i.e., simply having purchased a music CD or movie DVD does not give the purchaser any legal right to copy it).

4.10.4 TEACH

The Technology, Education, and Copyright Harmonization Act, also known as the TEACH Act, was created to allow distance education instructors and students to take advantage of the copyright exceptions granted to classroom educators under the doctrine of Fair Use. There are some differences in how copyrighted material may be used in a classroom versus in distant learning situations. Employees who wish to take advantage of the allowances provided by the TEACH Act to transmit copyrighted materials to online course participants must contact IT for assistance in technologically enforcing the regulations specified in the TEACH Act.

For more information about the provisions of the TEACH Act and Fair Use, consult with the Director of Library and Information Services.

4.11 Personal Use

Limited, reasonable personal use of College resources is permissible. However, such use cannot interfere with the employment responsibilities of the employee, must comply with the guidelines established herein, and is conducted at the employee's own risk, without an expectation of privacy.

4.12 Upholding the Mission

College technology resources shall not be used in any manner that violates or conflicts with the College's mission and/or its policies.

5.0 EMPLOYEES' ROLE IN INFORMATION SECURITY

The information owned by the College is one of its most valuable assets. It is the responsibility of all users to guard against misuse of this asset. Each person granted access to information must comply with the data security, confidentially requirements, and applicable laws described below.

5.1 Passwords

Upon creation of a user account an initial password is assigned to that account. Initial passwords are considered non-private and must be changed by account owners as soon as possible. Account owners are required to create passwords that comply with the College's password policy. The documented password policy is available to employees via the College's Web site. Account owners are responsible for protecting their

passwords from discovery by others and must immediately change any password that has been compromised.

5.1.1 Password Sharing

An account owner may not, under any circumstances, share any password with any other person. Similarly, a person may not, for any reason, ask an account owner to reveal his or her password. If an employee finds it necessary to write down login names and passwords for future reference, the document must be kept in a secure location.

5.1.2 Failed Password Attempts

Many user accounts have security protocols that will automatically disable an account after a specific number of failed login attempts. When a College account becomes disabled, the account owner must contact IT to have the account reactivated.

5.1.3 Security Compromise

In the event that there is suspicion of a hacking attempt or reason to believe a password has been compromised, a system administrator is authorized to and may, without prior notice, disable an employee's account access.

If an employee encounters a gap in security, he or she must report it to IT immediately. Exploitation of any security gaps is strictly prohibited.

5.2 FERPA

The Family Educational Rights and Privacy Act, more commonly known as FERPA, is a federal law that declares the rights of students to view their personal educational records while protecting the privacy of those records. This law applies to all public and private institutions that receive funding from the U.S. Department of Education. In short, failure to comply with FERPA regulations has both legal and funding implications for the College.

5.2.1 Student Information Maintenance

The Student Services Department has ownership and authority over the primary repository of student data at Heartland Community College. To acquire access to student records systems an employee must complete FERPA compliance training and sign an Ethical Standards agreement. The Director of Admissions and Records along with the Dean of Student Affairs and Enrollment Services will evaluate all requests for access to student information systems and will either approve or deny individual requests on a case-by-case basis.

5.2.2 Directory Information

Under FERPA the College is allowed to disclose directory information without the prior consent of students. Directory information at Heartland Community College consists of the following information:

- Name, address, and telephone number
- Major field of study

- Dates of attendance
- Enrollment status (part-time, full-time, hours completed)
- Degrees, honors, and certificates received or anticipated
- Participation in activities and sports
- Most recent previous school attended
- Login name
- Height/weight (athletes only)
- Photo (athletes only)
- E-mail addresses

5.2.2.1 Directory Information Suppression

A student has the right to suppress the release of his or her personal directory information. To request that personal directory information not be publicly disclosed, a student must submit a completed Public Directory Information form to Student Records prior to the end of the second week of class. These forms are available in Student Services.

Note: Once a student has a signed request to suppress his or her directory information on file, he or she would then need to submit, in writing to the Student Records Office, authorization for each individual disclosure of any information in the future.

5.2.2.2 Solomon Amendment

Pursuant to the Solomon Amendment, the College must supply specific student directory information to any military representative who requests such information for recruitment purposes. Exceptions are made for individuals with signed Public Directory Information forms on file. Military representatives will not be given directory information for those who have requested that such information be publicly withheld.

5.2.3 Personally Identifiable Information

According to FERPA regulations "personally identifiable information" is defined as information that includes, but is not limited to:

- the student's name
- the name of the student's parent or other family member
- the address of the student or the student's family
- a personal identifier, such as the student's Social Security number or student ID number
- a list of personal characteristics that would make the student's identity easily traceable
- other information that would make the student's identity easily traceable

5.2.3.1 US Patriot Act of 2001

In accordance with the US Patriot Act of 2001:

- The U.S. Attorney General may submit a written application to a court for an ex parte order requiring Heartland Community College to collect and produce education records that might otherwise be protected by FERPA.
- Under the US Patriot Act, College personnel are prohibited from disclosing to any other person that the FBI has sought or obtained records, except for to those persons necessary to produce the requested records.
- The College is provided immunity as a provider of electronic communications services if it furnishes information or assistance in accordance with a court order or a request for emergency assistance under the Foreign Intelligence Surveillance Act, as amended.

5.2.3.2 Disclosure of Personally Identifiable Information

Personally identifiable information may be disclosed internally to those who have legitimate educational interests, including the interests of students for whom consent would otherwise be required. Legitimate educational interest exists when disclosure of information is necessary for the completion of an employee's official duties, and access to the information is consistent with the purpose for which it was granted. For example, legitimate educational interest exists when a division secretary distributes class rosters, which contain student IDs, to faculty members.

Disclosure of any student information by non-Student Services personnel to any organizations or persons, including students, is prohibited. Employees outside of Student Services are required to forward such requested to the Director of Admissions and Records or to the Dean of Student Affairs and Enrollment Services.

5.2.3.3 Grade Posting

Employees are prohibited from posting grades or evaluative data in public areas using personally identifiable information, in whole or in part. Public areas include, but are not limited to, classrooms, computer labs, collaborative study areas, hallways, department reception areas, conference rooms, or on office doors.

Instructors are allowed to post the grades of students if done without using personally identifiable information. To clarify, FERPA prohibits an instructor from posting grades by social security numbers, student ID numbers, or names because these types of information are personally identifiable or easily traceable to the students. However, FERPA does not prevent an instructor from assigning individual numbers to students for the purpose of posting grades as long as those numbers are known only to the student and the faculty member.

5.2.6 FERPA-Related Requests and Demands from Students

Employees are required to direct students who inquire about FERPA regulations to Student Services. Employees outside of the Student Services department are prohibited from responding to a student's questions relating to FERPA. Likewise,

employees outside of the Student Services department are not allowed to carry out a FERPA-based request.

5.3 GLBA

The Gramm-Leach-Bliley Act, also known as the GLBA, declares the need for financial institutions to safeguard the confidentiality of financial information such as names, addresses, phone numbers, bank and credit card account numbers, and social security numbers. Because colleges participate in financial activities, colleges are required to adhere to the conditions established under the GLBA.

5.3.1 Heartland Community College GLBA Compliance

Heartland Community College employees will comply with the GLBA by adhering to the following privacy practices and specific rules:

5.3.1.1 Information Security Program Coordinator

The Director of Technology Support Services will serve as the Heartland Community College Information Security Program Coordinator. The Information Security Program Coordinator is responsible for overseeing institutional compliance with this Security and Appropriate Use Policy.

5.3.1.2 Information Privacy Policy

The College's Information Privacy Policy document is publicly available on the College's Web site. The posted document is refreshed within 30 days of any updates to the policy.

Employees who handle information referenced in the Information Privacy policy are required to complete annual information privacy sensitivity training.

5.3.1.3 Information Privacy Practices

College employees will ensure the privacy of financial data in the following ways:

- Conversations with individuals who are verbally disclosing financial information will take place in an office or other area that affords privacy.
- Financial data such as credit card numbers will not be transmitted through e-mail.
- All paper documents that contain financial information will be handled with caution during day-to-day operations of the College. Such documents will be removed from view or physical access in the presence of other students, employees or contributors.
- When paper retention policies do not apply, documents with financial information that are duplicates of electronically stored information will be permanently destroyed by shredding or other means.
- All documents or other tangible items containing financial information related to students, employees, and contributors will be stored nightly in locked cabinets.

- All financial information such as credit card information provided over the phone typically for the purpose of tuition and fees payment or contribution shall be destroyed immediately upon completion of the related transaction.

5.3.1.4 Employee Accountability

During performance evaluations, employees will be evaluated on their consistent compliance with GLBA rules as part of their required job duties. If a pattern of compliance violations exists, the failure to comply with the rules will be noted in the employee's annual evaluation. Supervisors may require employees to attend additional compliance training sessions.

5.3.1.5 Vendor Compliance

Service providers who may have access to any financial data – either in print, digital, or audio format – must sign the "GLBA Service Provider Compliance Contract." Service providers must then internally implement and maintain practices that adhere to the compliance program. The Information Security Program Coordinator or designee will regularly monitor the activities of service providers.

5.4 Payment Card Industry

The Payment Card Industry Data Security Standard (PCI DSS) is a set of standards created by the major credit card brands including Visa, MasterCard, American Express, Discover, and Japan Commercial Bank. The objective of these standards is to protect personal credit card data, also called cardholder data. All merchants that process, store, or transmit credit card data must comply with the PCI DSS. The standards specify how merchants are required to handle cardholder data, whether it is in paper or electronic form.

5.3.1 Heartland Community College PCI DSS Compliance

Heartland Community College will comply with the PCI-DSS in the following ways:

- Employees will not store any credit card number, expiration data, CVV2 number, PIN, or Magnetic Stripe data in any system on any College-owned device.
- All online credit card payments will be conducted using a 3rd party vendor that is PCI DSS certified and uses secure transaction technology.
- No credit card transactions will be conducted on the College's data network. All card readers will be on analog phone lines that are separate from the College's data network.
- All credit card transactions done using paper forms will be managed securely. All paper records will be stored in secure, locked cabinets with limited access.
- All employees that handle credit card information will be trained in the safe handling of card holder data. Training, along with refresher courses, will be conducted annually.
- Policies and procedures pertaining to the PCI DSS will be evaluated and updated annually.

6.0 PRIVACY

All information that resides on any College-owned or College-licensed technology resource is the property of Heartland Community College, subordinate to recognized copyrights and legal statutes. Nonetheless, the College respects the privacy of the individual. It is not the practice of College administrators or IT personnel to access the files created and/or stored by others. However, the College reserves the right to monitor its computing resources and may do so at anytime without prior notification.

Although privacy is valued, it must be balanced with the requirements of assuring system integrity and/or enforcing institutional policies. These necessities may result in a system administrator accessing files with or without consent of an employee. Maintaining the integrity of College resources outweighs privacy and confidentiality interests. Consequently, employees do not have a right to privacy while accessing and/or using any technology resource, including e-mail.

In order to fully understand the scenarios in which a system administrator may access an employee's files with or without the consent of the employee, employees should familiarize themselves with the policy components below.

6.1 ECPA

According to the Electronic Communication Privacy Act, also known as the ECPA, electronic communications may be intercepted when at least one of the communicating parties has given prior consent. Under the Heartland Community College Security and Appropriate Use policy described herein, users of any College-owned or College-licensed technology resource are, by nature of such use, granting consent to the College to monitor and/or intercept any electronic communications.

6.2 System Maintenance

System administrators regularly scan volumes of data on network devices for routine maintenance purposes. As a byproduct of maintenance, a system administrator may see the contents of files and e-mail messages.

System administrators are required to report any illegal activity that is discovered, or any information that indicates a violation of policy to the Chief Information Officer, who will review the report with a Cabinet member. Uncovered policy violations will be addressed in accordance with Section 7.0 herein.

6.2.1 Deleted Files

Deleting a file does not reliably or permanently remove a file from a system. This is true of computer files and voice mail files. The file may reside in an archive or backup storage, potentially indefinitely. If a file is not in storage it may be accessible by using recovery tools. Files that are retrieved through any of these methods are potentially subject to examination during routine system maintenance.

6.2.2 Archive and Backup Files

Computer files and e-mail systems are backed up on a regular basis. Some systems may be configured to create archives with or without the knowledge of the employee. The contents of these files are potentially subject to examination during routine system maintenance.

6.3 Access without Consent

Any access that occurs without consent must be authorized by the Chief Information Officer or a member of the Cabinet. A system administrator or designee will log all instances of access without consent. The employee will be notified of College access to files without consent. Depending on the circumstances such notification may occur before, during, or after the access. Situations that may result in file access without consent include, but are not limited to, the following:

6.3.1 Emergency Entry

Emergency entry may be necessary to preserve the system infrastructure, system integrity and facilities, or to preserve public safety. For example, if a virus exists in the network, a system administrator may need to access file storage assigned to individual employees in order to eradicate the virus.

6.3.2 Reasonable Cause

Heartland Community College reserves the right to examine files should it determine reasonable cause exists that an individual has violated internal policy or state or federal law. When an employee other than a system administrator is more qualified to research a specific violation, the Chief Information Officer, in consultation with a Cabinet member, may authorize temporary access to another Heartland Community College administrator so that he or she may research the alleged violation.

6.3.3 Temporary Access Request

During a period of leave, a supervisor may request temporary access to a specific subordinate's files and/or directories when this access is important to maintaining day-to-day operations, when a high-priority and time-sensitive project requires access, or when necessary to support the overall mission of the College. The Chief Information Officer has the discretion to grant or deny such requests.

Upon return from leave, the employee will be notified that temporary access was granted to his or her supervisor, and the temporary access will be terminated.

6.3.4 File Ownership Transfer

If an employment relationship is terminated, a supervisor may request permanent access to a former subordinate's files and/or directories.

6.4 Employment Termination

When employment is terminated, terminated employees are prohibited from removing any files, other than personal files, from the College. All files, whether related to the day-to-day operations of the College or to special projects to which the employee was

assigned; or which were created, copied, or edited as part of the duties of the employee's position are College-owned, and, with the exception of strictly personal files, may not be removed by a person whose employment at the College has been terminated

7.0 CONSEQUENCES FOR POLICY VIOLATIONS

Heartland Community College considers any violation of security and appropriate use guidelines to be a serious offense. Violators of this policy will be subject to disciplinary action in accordance with the College's progressive discipline policy, up to and including discharge. In addition to College discipline, violators of this policy may be subject to criminal prosecution, civil liability, or both for unlawful use of any technology resource.

8.0 POLICY DEVELOPMENT AND MAINTENANCE

This policy document is available to all employees. Employees may access the document via the College's public drive or may request a printed copy from the Information Technology Department or the Human Resources Department.

This policy will be reviewed periodically as determined by the Chief Information Officer. Concerns or questions about the policy may be directed to the Director of Technology Support Services, the Chief Information Officer, or the Vice President of Business Services.