INFORMATION SECURITY POLICY
Heartland Community College – Information Technology
Version 2.0 – 10/01/2013
# Table of Contents

1.0 INTRODUCTION .................................................................................................................. 3

2.0 INFORMATION SECURITY PROGRAM COORDINATOR .................................................. 3

3.0 PURPOSE OF THE INFORMATION SECURITY POLICY ................................................... 3

4.0 TYPES OF INFORMATION ................................................................................................. 3
   4.1 Confidential and Sensitive Information (CSI) ................................................................. 3
   4.2 Public Information ............................................................................................................ 4

5.0 RESPONSIBILITIES .............................................................................................................. 4
   5.1 Employee Responsibilities ............................................................................................... 4
   5.2 Administrator Responsibilities .......................................................................................... 5

6.0 DILIGENCE .......................................................................................................................... 5
   6.1 Diligence Concerning the Gramm-Leach-Bliley Act ......................................................... 5
      6.1.1 Mitigation of Risks ..................................................................................................... 5
   6.2 Diligence Concerning Credit Card Information .............................................................. 6
      6.2.1 Electronic Storage ..................................................................................................... 6
      6.2.2 Electronic Transmission ............................................................................................ 7
      6.2.3 Hard Copy Storage .................................................................................................... 7
      6.2.4 Hard Copy Transportation ......................................................................................... 7
      6.2.5 Hard Copy Retention and Destruction ....................................................................... 7
   6.3 Diligence Concerning Identity Theft ................................................................................ 8
      6.3.1 Identification Verification Procedures ......................................................................... 8
      6.3.2 Red Flag Response Procedures ................................................................................ 8
   6.4 Diligence Concerning the Family Educational Rights and Privacy Act ............................ 9
      6.4.1 Student Information Maintenance .............................................................................. 9
      6.4.2 Personally Identifiable Information .......................................................................... 9
      6.4.3 Directory Information ............................................................................................... 10
      6.4.4 Grade Posting .......................................................................................................... 10
      6.4.5 FERPA-Related Requests and Demands from Students .......................................... 10
      6.4.6 Other FERPA-Related Legislation ............................................................................ 10

7.0 VENDOR AGREEMENTS ................................................................................................... 11

8.0 UPDATING THE INFORMATION SECURITY POLICY ...................................................... 11

9.0 TRAINING AND COMMUNICATION .................................................................................. 11

APPENDIX A: IDENTITY THEFT RED FLAGS ........................................................................... 12
1.0 INTRODUCTION
The primary goal of Heartland Community College’s (HCC’s) Information Security Policy is to ensure that all Confidential and Sensitive Information (CSI) maintained by the college is protected in a manner that is in compliance with all relevant legislation, industry best practices, and the values of the College.

Other goals of the Information Security Policy are to:

- Define what information is considered to be confidential and sensitive.
- Define what information is considered to be public.
- Outline employee responsibilities when working with CSI.
- Provide a process for reporting security breaches or other suspicious activity related to CSI.
- Provide guidelines on how to communicate information security requirements to vendors.
- Summarize the laws and other guidelines that impact the Information Security Policy.

2.0 INFORMATION SECURITY PROGRAM COORDINATOR
The Director of Technology Support Services is the coordinator of the Information Security Program at Heartland Community College. The Director of Technology Support Services is responsible for working with Administrators from all areas of the College to implement information security practices in accordance with all legal requirements and industry best practices. The Director of Technology Support Services reports to the Chief Information Officer (CIO) of Heartland Community College. The CIO reports to the Cabinet. The Cabinet and the Heartland Community College Board of Trustees are ultimately responsible for all policies at Heartland Community College.

3.0 PURPOSE OF THE INFORMATION SECURITY POLICY
The purpose of the Information Security Policy is to define the guiding principles that all College employees must follow when working with Confidential and Sensitive Information. Each department that works with CSI will be required to implement department specific procedures to ensure that they are operating within the guidelines.

4.0 TYPES OF INFORMATION
Heartland Community College owns or is entrusted with a vast amount of information about its students, employees, and other business partners. This information may be in electronic form, stored on network servers, PC workstations, or magnetic or optical storage media. It may also be in hard copy (paper) form stored in file cabinets.

4.1 Confidential and Sensitive Information (CSI)*
The following types of information are considered by Heartland Community College to be Confidential and Sensitive Information:

- Social Security Number (SSN)
- Social insurance number (Medicare number)
- Date of birth
- Driver’s license number
- Customer identifiers
- Employee ID (EMPLID)
- Library ID
- Debit/Credit card number (Personal account number, Expiration date, CVV code)
• Bank account numbers
• Tax ID
• Passwords
• Medical records
• Doctor names
• Insurance policy information (Insurance claim information)

CSI can be found in many places at Heartland Community College. Records containing this information may be referred to as “Covered Accounts”. The following are some of the primary locations for CSI:
• Student records – PeopleSoft (credit/non-credit students)
• Student records – ImageNow
• Student records – Paper
• Employee records – PeopleSoft (HR, Payroll)
• Employee records – Paper (HR, Payroll)
• Student payment/billing information (credit card, bank account number)
• HCC financial accounts (checking/savings accounts, investment accounts, credit/debit card accounts)
• Medical records (employees and students)

*While all of these items are explicitly considered to be CSI, there may be other items

4.2 Public Information
Public information, often called “Directory Information”, may be shared with the general public. Students wishing to have their Directory Information withheld from the public must fill out a form in Enrollment Services. Heartland Community College considers the following information to be Directory Information:
• First name, middle name, last name
• Local address
• Local telephone number
• HCC e-mail address
• Photograph of athlete
• Dates of attendance at HCC
• Major field of study
• Participation in officially recognized activities, organizations, and athletic teams
• Weight and height of members of athletic teams
• Degrees, certificates, honors awarded or anticipated
• Enrollment status (part-time, full-time)
• Institutions previously attended
• Student login name

5.0 RESPONSIBILITIES

5.1 Employee Responsibilities
Most HCC employees will come in contact with CSI at some point while performing their job duties. While some employees will work with CSI more often than others, all employees need to be aware of their responsibilities when handling CSI.
• Employees may not divulge, copy, release, review, or destroy any CSI unless properly authorized as part of their official job duties.
Properly authorized employees must destroy CSI that is no longer needed. This includes shredding documents and having digital storage devices permanently erased.

Employees must protect CSI regardless of its location or format (electronic or paper).

Employees must safeguard all types of access (i.e., keys, ID cards, and passwords) to CSI.

Employees are required to report any suspicious activity regarding CSI to their supervisor as soon as possible.

5.2 Administrator Responsibilities
In addition to the employee responsibilities stated above, College administrators have additional responsibilities regarding the use of CSI in their respective departments. College administrators are required to:

- Know what types of CSI are available in their department.
- Develop procedures that support safeguarding CSI in their department as outlined in this policy.
- Ensure employees are trained on departmental procedures and are following them.
- Report any suspicious activity regarding CSI to the CIO or the Director of Technology Support Services.

6.0 DILIGENCE

6.1 Diligence Concerning the Gramm-Leach-Bliley Act
The Gramm-Leach-Bliley Act (GLBA) has two rules that impact financial institutions; the Privacy Rule and the Safeguards Rule. Colleges and universities are considered to be financial institutions under GLBA. Colleges and universities are considered to be compliant with the Privacy Rule if they are compliant with FERPA (see section 6.4). In order to be considered compliant with the Safeguards Rule, financial institutions must:

- Conduct ongoing risk assessments of all areas of operation where CSI is used.
- Design and implement a safeguards program to protect all CSI owned or entrusted to the College. This includes regular monitoring of these safeguards.
- Select appropriate service providers when those service providers work with the College’s CSI.
- Regularly evaluate and adjust the Information Security Program in light of changes in the College environment.
- Provide ongoing training to employees on the proper handling of CSI.

6.1.1 Mitigation of Risks
Heartland Community College continuously assesses the potential risks (internal and external) to its Confidential and Sensitive Information. The College has taken the following steps to mitigate these risks:

- A network firewall has been implemented and is continuously monitored and adjusted.
- Anti-virus software is running on all workstations and servers and is regularly updated. The updates are controlled at the network domain level.
- Microsoft updates are performed regularly on all server and workstation operating systems as well as Microsoft Office applications.
An enterprise spam filtering software solution is in place to drastically reduce the amount of spam e-mail that enters the College’s e-mail system.

Administrative access is restricted on workstations located in public/shared areas.

File level access rights are controlled on all network shared drives. File shares are available as follows:

- I: drive – user’s home directory. Only the user has access to this share.
- M: drive – department share. Access is granted based on the employee’s department of employment.
- S: drive – cross functional teams. Access is granted based on team lead approval to individuals participating in various cross-functional teams.
- Z: drive – Public area (read only). Hosts organizational documents such as policies, phone lists, etc. that employees can view, but not edit.

*Note: System Administrators have access to all file shares on all servers.*

Employees are required to change their password every 120 days using Microsoft’s complex password requirements.

A self-service password reset tool called Password Station is used by students and employees to change their own password from on-campus or off-campus.

Off-campus access to Heartland Community College network resources is limited to Cisco’s Virtual Private Network (VPN) software, Citrix Access Gateway, SharePoint, and/or the myHeartland portal.

### 6.2 Diligence Concerning Credit Card Information

Heartland Community College accepts credit card and debit card payments for tuition, donations, and other financial transactions. Any merchant that accepts credit card payments is subject to the security requirements outlined in the Payment Card Industry Data Security Standards (PCI-DSS). All HCC employees that work with credit card transactions must adhere to the following security requirements.

#### 6.2.1 Electronic Storage

HCC does not store any cardholder data electronically. Cardholder data includes:

- The Primary Account Number (PAN) – 16 digit credit card number on the front of the card.
- The expiration date of the credit card.
- The service code, Card Validation Code, or value (CVC, CVC2, CVV2, etc.) – the 3 digit number found on the back of the card used for on-line transactions.
- Personal Identification Number (PIN) – the number used for ATM transactions.
- Any magnetic stripe information – which includes all of the above information.

Employees must never enter cardholder data into any electronic software system such as PeopleSoft or any other type of database, spreadsheet or other electronic file. Credit Card data may not be stored on any laptop computer, any Personal Digital Assistant (PDA) device, any removable storage media such as a thumb drive, any office or public workstation, or any network drive.
6.2.2 Electronic Transmission
Heartland Community College does not electronically transmit credit card information over its data network.
- All on-line credit card transactions are handled by a third party service provider. These providers are responsible for providing a secure web site to handle the transactions as well as storing the credit card data securely.
- All “card present” transactions are handled using stand-alone terminals connected to analog phone lines.
- Any faxed-in applications (Continuing Education only) are received on a fax machine that is connected to an analog phone line.
- HCC employees are prohibited from sending credit card information using electronic communication methods such as e-mail, chat, or instant messaging.

6.2.3 Hard Copy Storage
Heartland Community College does receive and work with paper forms that may contain credit card information. Paper forms that contain credit card information must be safeguarded as follows:
- All paper forms containing credit card information must be physically secured in a lockable file cabinet in a lockable room. Access to this room and the file cabinet must be limited to employees with a legitimate business need to access them.
  - The room may be unlocked during normal business hours, but must be locked otherwise.
  - Any file cabinet containing credit card information must be locked at all times. A cabinet should only be unlocked when an employee is accessing it to store or retrieve records.
- Credit card information must not be hand-written on paper such as “post-it notes” or other types of note pads.
- Hard copy forms containing credit card information must not be left unattended on desktops in offices.
- Hard copy forms containing credit card information must not be stored in personal desk drawers (even locked drawers) over night. It is acceptable to store credit card information in a locked desk drawer during the work day when you are away from your desk.

6.2.4 Hard Copy Transportation
Heartland Community College employees are permitted to transport hard copy forms containing credit card information to other areas on campus. For example, credit card receipts need to be taken to the Business Office. Continuing Education applications containing credit card payment information that have been sent via U.S. Postal mail are required to be delivered to the appropriate department. When such transportation is required, only employees authorized by the Department Supervisor are allowed to transport the credit card information.

6.2.5 Hard Copy Retention and Destruction
Hard Copy forms containing credit card information will be kept for a period of no longer than one academic semester. After one academic semester, these records will be destroyed using a cross cut shredder. Only employees authorized by the
Department Head will be allowed to shred credit card information, and a record must be kept of the dates that these forms were shredded as well as the employee responsible for shredding them.

6.3 Diligence Concerning Identity Theft
The Red Flags Rules of the Fair and Accurate Credit Transactions Act of 2003 (FACTA) require financial institutions to implement procedures to detect, prevent, and mitigate potential identity theft incidents. Procedures required in order to comply with the Red Flag Rules are:

6.3.1 Identification Verification Procedures
Identification verification procedures are necessary for employees to form a reasonable belief that they know the identity of the individual opening a new covered account or requesting access to an existing covered account. Each department where CSI is handled must define and implement a procedure that will allow HCC employees to verify the identity of anyone opening a new account or anyone requesting access to an existing account.

6.3.1.1 Opening a New Account
Heartland Community College may open new covered accounts for someone requesting such an account either in person or by mail, fax, or on-line. Whenever possible, identification will be verified in-person using a valid State Issued Driver’s License or State Issued Identification Card. When new accounts are opened and the individual is not present, a welcome letter will be sent via U.S. Postal Service. This letter will serve as verification of the individual’s identification.

6.3.1.2 Accessing Information Stored Electronically
Information stored electronically will be secured using various network and application specific authentication and authorization policies. This includes the use of login names and passwords and access rights that are maintained by the Information Technology Department with guidance from other departments within Heartland Community College.

6.3.1.2 Accessing Information Stored in Hard Copy Format
Covered Account information stored in hard copy format will be physically protected by the department storing the information. Access to this information will be granted based on the position held at the College or on the legitimacy of the need for the information.

6.3.2 Red Flag Response Procedures
Nearly all HCC employees have the potential to help detect or prevent identity theft from occurring regardless of their position at the College. Front line employees are typically from the Professional-Technical or Classified job classifications. These employees are the most likely to have direct contact with customers. Face-to-face, phone, fax, and e-mail contact are all considered forms of direct contact with a customer. Supervisors may be Professional-Technical or Administrative employees. These employees have a responsibility to supervise the activities of one or more other employees. Administrators are employees in the Administrative job classification. Administrators typically are responsible for managing a department or
a specific group within a larger department. It is the responsibility of all HCC employees to detect and prevent potential cases of identity theft.

6.3.2.1 Red Flag Detection and Verification
All red flags detected will be escalated to an employee in a supervisory position. The decision to notify any third parties including law enforcement of a potential identity theft incident will be made by the CIO or the Vice President of Business Services.

6.3.2.2 List of Red Flags
A list of relevant red flags can be found in Appendix A of this policy.

6.4 Diligence Concerning the Family Educational Rights and Privacy Act
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.

6.4.1 Student Information Maintenance
The Enrollment 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 Dean of 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.

6.4.2 Personally Identifiable Information
According to FERPA regulations, educational agencies or institutions are not permitted to release educational records, including personally identifiable information from those records, without prior written consent. According to FERPA, "personally identifiable information" is defined as information that includes, but is not limited to, the following:

- Student’s name
- Name of the student’s parent or other family member
- 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

In exception, personally identifiable information may be disclosed without prior written consent 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.
Disclosure of any student information by non-Enrollment Services personnel to any organizations or persons, including students, is prohibited. Employees outside of Enrollment Services should direct such requests to the Dean of Enrollment Services.

6.4.3 Directory Information
Under FERPA, the College is allowed to disclose directory information, including that which may be personally identifiable information, without the prior consent of students. Directory Information at HCC consists of the information listed in the 4.2 Public Information section of this document.

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 Enrollment 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.

6.4.4 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. 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. Instructors should post grades in Blackboard. Blackboard provides a secure and private method for instructors to share grade information with students.

6.4.5 FERPA-Related Requests and Demands from Students
Employees are required to direct students who inquire about FERPA regulations to Enrollment Services. Employees outside of the Enrollment Services department are prohibited from responding to a student’s questions relating to FERPA. Employees outside of the Enrollment Services department are not allowed to carry out a FERPA-based request.

6.4.6 Other FERPA-Related Legislation

6.4.6.1 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.
6.4.6.2 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 HCC 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.

7.0 VENDOR AGREEMENTS
When negotiating contracts with third party vendors, Heartland Community College employees must consider whether or not the vendor will need access to any of the College’s CSI. Any vendor that will have access to CSI will be required to abide by this Information Security Policy and any subsequent procedures. Contract language must include acceptance of the Information Security Policy. In cases where vendors will provide services directly related to Confidential and Sensitive Information, they will be required to provide proof of their compliance with all applicable laws.

8.0 UPDATING THE INFORMATION SECURITY POLICY
The Information Security Policy will be reviewed at least one time per year by the Information Security Team, headed by the Director of Technology Support Services. The policy may be reviewed and updated more often if circumstances arise that require significant changes to the policy.

9.0 TRAINING AND COMMUNICATION
The Director of Technology Support Services is responsible for providing annual Information Security Practices training to all Heartland Community College employees. This training will inform employees of their responsibilities when working with Confidential and Sensitive Information at Heartland Community College and update them on policy changes. Additional training will be provided to employees whose primary job duties require them to work with CSI. Procedural training specific to a particular department regarding CSI will be the responsibility of the Department Head.

Source: https://share.heartland.edu/sites/workcenter/378/Series Documents/Policies/Information Security Policy.docx
APPENDIX A: IDENTITY THEFT RED FLAGS
The following identity theft red flags have been identified as risks to the covered accounts at Heartland Community College:

Suspicious Documents
- Documents provided for identification appear to have been altered or forged.
- The photograph or physical description on the identification is not consistent with the appearance of the customer.
- Other information on the identification is not consistent with readily accessible information on file for the customer (such as physical attributes including height, weight, gender, eye and hair color, and/or approximate age).
- Application appears to be altered or forged.

Suspicious Personal Identifying Information
- Personal Identifying Information provided is inconsistent when compared to external information sources – Address does not match any address for the customer, SSN has not been issued.
- Personal Identifying Information submitted is not consistent with other personal identifying information provided by the customer.
- Personal Identifying Information provided is associated with known fraudulent activity as indicated by internal or third party sources. For example – the address on an application is the same as the address provided on a fraudulent application, or the phone number on an application is the same as the number provided on a fraudulent application.
- Personal Identifying Information provided is of a type commonly associated with fraudulent activity as indicated by internal or third party sources. For example – the address on an application is fictitious, a mail drop, or a prison; or the phone number is invalid or associated with a pager or answering service.
- The Social Security Number provided is the same as that submitted by another person.
- The person opening a covered account or the customer fails to provide all required personal information on an application.
- Personal Identifying Information provided is not consistent with personal identifying information currently on file.
- The person accessing the account cannot provide authenticating information to challenge questions.

Unusual Use of/Suspicious Activity Related to Covered Accounts
- Mail sent to the customer is returned as undeliverable although transactions continue to be conducted in connection with the account.
- HCC is notified of unauthorized transactions in connection with the customer’s covered account.

Notice from Customers/Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with a Covered Account
- HCC is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.
Other Red Flags
Any other circumstance that a Heartland Community College employee feels may be suspicious.

- A person asking for information about a customer.
- A person trying to gain physical access to HCC records.
- Inappropriate use of HCC resources in an attempt to gain access to HCC records.