INFORMATION SECURITY POLICY

Heartland Community College – Information Technology
Version 3.0 – 6/24/2020

Table of Contents

Effective June 24, 2020, this policy replaces any prior policies related to information security.

1 POLICY STATEMENT

Heartland Community College (HCC) is entrusted with a great deal of information from students, employees, business partners, the government, and other sources. That information includes Confidential and Sensitive Information (CSI) which is critical to the College's teaching, learning, and to the administrative functions that support that mission. The loss or misuse of CSI can cause substantial injury to the College, its constituents and/or affiliates in terms of financial loss, reputational damage, operational capability, and/or significant embarrassment.

All members of the College community are responsible for protecting the CSI entrusted to them, and for taking affirmative steps to prevent its unauthorized disclosure or loss. This policy sets forth the security guiding principles that all members of the College community must follow to meet that responsibility. Each department that works with CSI will be required to implement department specific procedures to ensure that they are operating within the guidelines.

This policy applies to all College activities, whether on campus or off, and to all CSI regardless of the medium in which it is stored (paper, electronic, etc.) or shared (electronically, verbally, visually, etc.). This policy applies to all staff, faculty and students, and anyone accessing College Systems (defined below) or CSI contained on those systems, such as visitors, vendors, and contractors. Violations of this policy may result in disciplinary action up to and including separation from the College.

2 DEFINITIONS

Information generated, collected by, or entrusted to the College is classified as follows:

2.1 Confidential and Sensitive Information (CSI)*

CSI is data that is protected by federal, state or local law or contractual obligation, or that is specifically designated as confidential by the College. Information also is considered CSI if its loss, misuse or unauthorized disclosure or alternation might cause substantial injury to the College, its constituents and/or affiliates in terms of financial loss, reputational damage, operational capability, and/or significant embarrassment. Examples of CSI include, but are not limited to:

- Student education records (e.g., grades, biographical information, class rosters)
- Employee ID (EMPLID)
- Student ID
- Library ID
- Tax ID
- Passwords
- Social Security Number (SSN)
- Social insurance number (Medicare number)
- Date of birth
- Driver’s license number
- Bank account
- Credit/debit card (Account number, Expiration date, CVV code) or other financial information
- Insurance policy information (Insurance claim information)
- Medical records
- Doctor names
- Payroll records
- Personnel (employment) records
- Customer identifiers
- Donor information

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

The highest levels of security must be applied to restrict access to CSI to only authorized individuals, and to protect against its unauthorized use, disclosure or modification.

2.2 Internal Use Only Information

Internal Use Only Information is the College's default classification and refers to all institutional data that is not classified as either "CSI" or "Public." Information is considered Internal Use if its loss, misuse or unauthorized disclosure or alteration might cause moderate injury to the College, its constituents and/or affiliates. Examples include, but are not limited to:

- Internal directories
- Non-public meeting minutes or memoranda
- Contracts
- Information about financial transactions
- Drafts of official documents

A reasonable level of security must be applied to limit access to Internal Use Only Information, and to prevent its unauthorized use, disclosure, or modification.

2.3 Restricted College Information

Restricted College Information means any information which is classified by the College as either CSI or Internal Use Only (see the definitions above).

2.4 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. HCC considers the following information to be Directory Information:

- First name, middle name, last name
- Address
- 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

Public Information is open to the College community, external entities, and the general public. Examples of Public Information could include, but are not limited to:

- Press releases
- The College website
- Publicly-posted schedules or calendars
- Publicly-posted or published newsletters or magazines

A reasonable level of security must be applied to protect Public Information against unauthorized modification.

2.5 Legitimate Business Function

Legitimate Business Function refers to the business justification, as approved by an appropriate supervisor, for which access to Restricted College Information is approved.

2.6 Mobile Device

Mobile Device means an electronic device, without regard to ownership, that is easily transportable and capable of accessing, storing, or transmitting information. Mobile devices include but are not limited to laptop computers; tablets; netbooks; cell phones; Smartphones (e.g., iPhones, Galaxy); flash or "thumb" drives; magnetic tape; discs; and external hard drives.

2.7 College Systems

College Systems include College-owned or controlled computing devices, data networks, software, databases, services, and facilities. College Systems is a potential source for containing CSI and may be referred to as “Covered Accounts”. The following are some of the primary College Systems locations but are not limited to shared computer drives, network file shares, Cloud storage, third party storage, networkable copiers, College-provided wireless networks (WiFi), and College-provided programs or software such as:

- Employee records – PeopleSoft, Network Drive (HR, Payroll)
- Employee records – Paper (HR, Payroll)
- Employee documentation/correspondence - Office 365
- Medical/Insurance records (employees and students)
- Student records – PeopleSoft (credit/non-credit students)
- Student records – ImageNow
- Student records – Paper
- Student email – Google/Gmail
- Student payment/billing information (credit card, bank account number)
- HCC financial accounts (checking/savings accounts, investment accounts, credit/debit card accounts)
- Donor Records – Raisers Edge

3 REASONABLE EXPECTATION OF PRIVACY

Generally, users of College Systems (defined above) may expect that the usage of HCC information resources, including accessing the Internet or using electronic mail, social media, instant messaging, telephone, or voice mail is not routinely monitored; however it is not completely private. The Appropriate Use Policy notes in the Monitoring section that the normal operation and maintenance of these resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the provision of service. HCC may also specifically monitor the activity and accounts of individual users of HCC information resources, including individual login sessions, the content of individual communications, and the contents of stored information, with or without notice, when:

- The individual has voluntarily made the information accessible to the public, as by posting to a blog or a Web page;
- it reasonably appears necessary to do so to protect the integrity, security, or functionality of HCC information resources or to protect HCC from liability;
- a written complaint has been received, or there is reasonable cause to believe, that the individual has violated or is violating this policy;
- an account appears to be engaged in unusual or unusually excessive activity; or it is otherwise required or permitted by law.

Any such monitoring of communications or stored information, other than what is made accessible by the individual, required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the Chief Information Officer (CIO), the Executive Director of Human Resources, the Dean of Students, or the Director of Network and System Administration, as appropriate. HCC, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications or stored information, to appropriate HCC personnel and/or law enforcement agencies and may use those results in appropriate HCC disciplinary proceedings.

4 SYSTEM ACCESS REQUIREMENTS

Limiting access to College Systems can prevent unauthorized access to those systems and the information they contain. The College therefore provides limited access to those systems based upon a demonstrated business need. Access to College Systems requires the following:

- An authorized relationship with the College (e.g., staff, faculty, students, and in limited circumstances vendors or contractors);
- A Legitimate Business Function as certified in writing by the individual's direct supervisor;
- Approval for access to information domains by the relevant Data Steward; and
- Use of a unique username and password by each individual granted system access (group access and shared credentials may be permitted on an exception basis with the approval of the CIO.) See **Information Security Requirements**, below, for required steps for protecting credentials.

Access is conditioned upon the user's agreement to abide by the foregoing requirements and all applicable College policies.

5 DILIGENCE

5.1 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.

5.1.1 <u>Mitigation of Risks</u>

HCC continuously assesses the potential risks (internal and external) to its CSI. 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 internal network drives and Cloud file space.

  Note: College 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 HCC network resources is limited to Cisco's Virtual Private Network (VPN) software, Citrix Access Gateway, SharePoint, Office365 and/or the myHeartland portal.

5.2 Diligence Concerning Credit Card Information

HCC 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.

5.2.1 <u>Electronic Storage</u>

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 mobile device, any office or public workstation, or any network drive.

5.2.2 <u>Electronic Transmission</u>

HCC 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 or Ethernet network lines.
- HCC employees are prohibited from sending credit card information using electronic communication methods such as e-mail, chat, or instant messaging.

5.2.3 <u>Hard Copy Storage</u>

HCC does receive and works 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 workday when the employee is away from his/her desk.

5.2.4 <u>Hard Copy Transportation, Retention, and Destruction</u>

HCC employees are permitted to transport hard copy forms containing credit card information to the Business Office or the Continuing Education Office. Continuing Education applications containing credit card payment information that have been sent via US Postal mail are required to be charged to the credit card terminals when received and immediately shredded. Employees only can transport credit card information directly to the Business Office or the Continuing Education to be charged to the credit card terminal and then shredded. Hard copy forms containing credit card information will be processed and shredded with a crosscut shredder as soon as the information is processed with the credit card terminal.

5.3 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:

5.3.1 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. College System 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.

5.3.1.1 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 Finance and Administration.

5.3.1.2 List of Red Flags

A list of relevant red flags can be found in Appendix A of this policy.

5.4 Diligence Concerning the Family Education 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.

5.4.1 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.

5.4.2 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:

- 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 Registrar.

5.4.3 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 2.4 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 the Prevent Release of Directory Information form available on the Heartland website. The request remains in effect until the College receives written authorization to revoke the request.

5.4.4 **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 Canvas and will submit midterm and final grades through Faculty Work Center. Canvas and the IRIS-Student Center provide a secure and private method for instructors to share grade information with students.

5.4.5 **FERPA-Related Requests and Demands from Students**

Employees are required to direct students who inquire about FERPA regulations to the Registrar or the Records Office. 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.

5.4.6 **Other FERPA-Related Legislation**

5.4.6.1 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 a submitted Prevent Release of Directory Information form. Military representatives will not be given directory information for those who have requested that such information be publicly withheld.

5.4.6.2 US Patriot Act of 2001

The US Patriot Act of 2001 resulted in amendments to FERPA. In accordance with the US Patriot Act of 2001:

- Heartland is permitted to disclose, without consent or knowledge of the student, protected information from the student’s educational records to the U.S. Attorney General or to his/her designee in response to an *ex parte* order in connection with the investigation or prosecution of terrorism crimes.
- Heartland is not required to record a disclosure of information from a student’s education record when it makes the disclosure pursuant to an *ex parte* order.
- Further, Heartland, if in good faith, produces educational records in compliance with an *ex parte* order, it shall not be liable to any person for that production.
- Finally, 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.

6 RESPONSIBILITIES

All members of the College community share the responsibility for safeguarding College information. The following individuals/offices have a heightened expectation as outlined below:

6.1 Information Security Program Coordinator

The Chief Information Officer (CIO) of HCC is the coordinator of the Information Security Program at HCC. The CIO reports to the Cabinet. The CIO 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.

6.1.1 **Information security practices implemented by CIO, but is not limited to:**

6.1.1.1 Security of Restricted College Information to which users have been granted access, in whatever format (e.g., electronic, paper, verbal).

6.1.1.2 Responsible for the decision to authorize, or not, access to Restricted College Information for which they are the primary College System Administrator in charge of that functional area (e.g., academic records fall under the purview of the Registrar).

6.1.1.3 Information Technology Department: Responsible for the implementation and auditing of functional controls which support the restriction of access to Restricted College Information to individuals with a Legitimate Business Function that has been appropriately approved for such access.

6.1.1.4 Restricted College Information is appropriately handled, stored and destroyed in accordance with applicable College policy.

6.2 The Cabinet and the HCC Board of Trustees

The CIO will provide recommended information security practice and policies for the ultimate approval made by the Cabinet and the HCC Board of Trustees. The Cabinet and the HCC Board of Trustees are ultimately responsible for all HCC policies.

7 INFORMATION SECURITY REQUIREMENTS

Every staff and faculty member is responsible for completing the College's mandatory online Privacy and Information Security Training. All members of the College community, and anyone accessing College Systems, are responsible for adhering to the College information security requirements, including but not limited to the following:

7.1 Protect System and Network Access

- Know and follow the requirements in the College's Appropriate Use Policy.
- Treat HCC credentials (e.g., usernames and passwords) for access to College systems and/or the cloud services, as confidential. Such credentials are non-transferable and should never be shared, even with College personnel from Technology Services.
- Use strong passwords to access College systems and/or cloud services to properly secure all College systems.
- Do not write down passwords where they are easily accessible to others.
- Do not save any HCC credentials with the capacity to access College systems and/or cloud services in any type of web browser.
- Do not attempt to access College systems and/or cloud services for Heartland unless authorization has been provided (see System Access Requirements, above).
- Access College systems and Restricted College Information only on College provided or specifically College approved hardware.
- Do not use College systems and/or cloud services (e.g., Office365) in a way that negatively impacts the functioning or availability of those systems.
- Do not download or install computer programs or software onto College Systems without prior approval from IT Help Desk.
- Do not install client software that synchronizes HCC data stored on the cloud to public or private computers/devices. , other than HCC college-owned devices.
- If using public or private computers/devices to access the HCC data stored on the cloud via a web browser, the same device should have the web browser fully closed after each use and clear all history and website data (e.g., clear the cache).
- Be vigilant when sharing the College data stored on the cloud with external users (e.g., HCC Restricted College Information share files) and if warranted share this data read-only and do not share entire folders.

- Log out from a College systems and/or cloud services when finished working, or if away from the computer for more than a few minutes.
- Maintain up-to-date anti-virus software and system patches on all computers/devices. When prompted to update such software or patches do so as soon as possible.

7.2 Protect the Confidentiality of Information

- Do not share information collected for a specific purpose with those outside the College community without notification and consent.
- Do not access or use Restricted College Information other than for a Legitimate Business Function.
- Do not share Restricted College Information with those who do not have a Legitimate Business Function which requires knowledge of that information.
- Fax confidential data only after confirming that the receiving fax machine is located in a secure area accessed only by those with a legitimate need to see the information being transmitted.
- Do not leave paper documents containing Restricted College Information where they are accessible to those who do not have a legitimate need to know that information. Secure all such documents in a locked suite, office, desk, or file cabinet.

7.3 Protect the Integrity of Information

- Do not modify College information for purposes other than a Legitimate Business Function.
- Do not use College information for personal use or benefit.
- Protect the intellectual property of others.

7.4 Take Care with E-mail

- Do not use personal e-mail for work purposes.
- Do not use College e-mail for personal reasons.
- Do not download e-mail attachments from unknown senders.
- Do not e-mail CSI to non-College addresses unless the file is appropriately encrypted or pursuant to departmental procedures regarding transmission of such CSI.

7.5 Dispose of Information and Equipment Properly

- Employees may not divulge, copy, release, review, or destroy any CSI unless properly authorized as part of their official job duties.
- Employees may contact the IT Help Desk at 309-268-8350 or by e-mail at helpdesk@heartland.edu for assistance disposing of personal computers or Mobile Devices that were used for College business. Disposal of College computer equipment and Mobile Devices may contain Restricted College Information that must be removed; in addition, there is the risk of other exposures such as potential hazardous materials if disposed of improperly.
- Shred all written documents that contain Restricted College Information when they are no longer required.
- If employee is unsure whether he/she is authorized to access, share, or transmit and/or purge confidential information, or have other questions about protecting that information or disposing of it, contact IT Help Desk at 309-268-8350 or by e-mail at helpdesk@heartland.edu.

7.6 Additional Responsibilities for College System Administrators

In addition to the employee responsibilities stated above, College System Administrators have additional responsibilities regarding the use of CSI in their respective departments. College System 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 IT Help Desk at 309-268-8350.

7.7 Report Potential Information Security Breaches

Immediately report potential information security breaches, or evidence of potential illegal activity, to the IT Help Desk at 309-268-8350 or by email at helpdesk@heartland.edu, and to immediate supervisor.

7.8 Vendor Agreements

When negotiating contracts with third-party vendors, HCC 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 CSI, they will be required to provide proof of their compliance with all applicable laws.

7.9 Updating the Information Security Policy

The Information Security Policy will be reviewed at least one time per year by the Information Security Team and by the CIO. The policy may be reviewed and updated more often if circumstances arise that require significant changes to the policy.

7.10 Training and Communication

Associate Director, Human Resources is responsible for providing annual Information Security Practices training to all HCC employees. This training will inform employees of their responsibilities when working with CSI at HCC 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.

Associate Director, Human Resources is responsible for the Employee FERPA Training that is provided to all employees.

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:

Information System Risks:

- Unauthorized access of Protected Information by someone other than the owner of the covered data and information
- System security compromised as a result of system access by unauthorized persons
- Interception of data during transmission
- Loss of data integrity
- Errors introduced into the system
- Corruption of data or data systems
- Unauthorized access of covered data and information by employees
- Unauthorized requests for covered data and information
- Unauthorized access through hard copy files or reports, and
- Unauthorized transfer of covered data and information through third parties.

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 HCC 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.