7 DETECTION, PREVENTION, AND MITIGATION OF IDENTITY THEFT

(Owner: Chief Strategic Operations Officer; Last Reviewed: 7/20/20; Last Updated 08/08/19)

It is the policy of Central Christian College of Kansas to ensure the security and confidentiality of information used in our college operations and to comply with all applicable laws and regulations providing for such security. Security and confidentiality are matters of concern for all faculty, staff, and students within the college who have access to our computer data systems or physical facilities.

All records created by employees as a part of their work are the property of the College. All persons working in the college offices who have access to constituent information hold a position of trust relative to this information, and they must recognize the responsibility to preserve the security and confidentiality of this information. Therefore, any person with access to any constituent information:

- Will not make or permit improper or unauthorized use of any information.
- Will not seek personal benefit, or permit others to benefit personally, by any confidential information.
- Will not exhibit or divulge the contents of any record or report to any person except in the conduct of their work assignment and in accordance with college policies.
- Will not knowingly include, or cause to be included, in any record or report a false, inaccurate, or misleading entry.
- Will not remove any official record or report (or copy thereof) from the office where it is kept except in the authorized performance of his or her duties.
- Will dispose of records in accordance with record retention procedures.
- Will not aid, or act in conspiracy with, another to violate any part of this code.
- Will immediately report any violation of this code to his or her work supervisor.

As custodians of official College records, we all share the responsibility for ensuring the security and privacy of the records and data we maintain.

A violation of this code may lead to reprimand, suspension, dismissal or other disciplinary action, consistent with the general policies of the College related to personnel (including student employee) discipline.

Each employee is required to sign a statement of compliance at the time of hiring. Forms are available in the Business Office.

7.1 EMPLOYEE CONFIDENTIALITY AGREEMENT

The College adheres to the Family Educational Rights and Privacy Act (“FERPA”), a federal law enacted in 1974 that provides safeguards regarding the confidentiality of student records. All employees of the College are expected to be familiar with the basic provisions of FERPA and PII regulation to ensure that they do not violate federal law.

- Employees understand that all information gained from student and/or employee files (including computer generated documents) or heard in the course of my employment is strictly confidential. Employees will not share this information with anyone other than with those authorized to receive the information or as mandated by provisions in state or federal law.
Employees will not acquire or seek to acquire confidential information about students and/or employees, including information contained in student or personnel files, unless the information is needed and is essential to perform my job duties. Employees will not reveal information about students that they may learn or have learned while performing their jobs. Employees understand that even a minor disclosure of information, e.g., disclosing a student’s class schedule, may be a violation of FERPA and/or College policy and could result in disciplinary action, up to and including the loss of employment.

Employees understand that anyone having access to the college's data information systems is not allowed to leave campus with any information obtained from the college's data information systems by means of any storage device such as flash drives, cloud storage, cd/dvd, external hard drives, or any kind of paper form of the information unless required for approved telework.

Employees understand that they can only use the College's equipment to access the college's data information systems. This data can only be printed to a network printer or saved to the College’s network drive.

Employees agree that files with protected information or other documents in print or electronic format will not be left unattended in public areas for others to view, and that no files or copies of records in any format will leave the office/department without proper authorization.

Employees understand that computer passwords that may be provided will not be shared with anyone other than those authorized. Employees will ensure the electronic devices that they use, or for which they are responsible, are properly secured when not in use.

Employees agree to abide by the guidelines and procedures of the College in accepting credit card payments on behalf of college in the course of my employment. Guidelines are established by the President which will remain in compliance with those set by the Payment Card Industry (PCI).

7.2 RED FLAGS POLICY (IDENTITY THEFT PREVENTION PROGRAM)
Central Christian College of Kansas developed this Identity Theft Prevention Program (Program) pursuant to the Federal Trade Commission’s (FTC) Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This Program was developed with oversight and approval of the College’s Board of Trustees. After consideration of the size and complexity of the College’s operations and account systems, and the nature and scope of the College’s activities, the College determined that this Program was appropriate for the College.

Red Flags Rule - Definitions Used in this Program:

- “Identity Theft” is a “fraud committed or attempted using the identifying information of another person without authority.”
- A “Red Flag” is a “pattern, practice, or specific activity that indicates the possible existence of Identity Theft.”
- A “Covered Account” includes all student accounts or loans that are administered by the College.
• “Program Administrator” is the individual designated with primary responsibility for oversight of the program. See number 6 below.
• “Identifying Information” is “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including: name, address, telephone number, social security number, date of birth, government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer’s Internet Protocol address, or routing code.

Under the Red Flags Rule, the College is required to establish an “Identity Theft Prevention Program” tailored to its size, complexity and the nature of its operation. Each program must contain reasonable policies and procedures to:

• Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program.
• Detect Red Flags that have been incorporated into the Program.
• Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft.
• Ensure the Program is updated periodically to reflect changes in risks to students or to the safety and soundness of the student from Identity Theft.

In order to identify relevant Red Flags, the College considers the types of accounts that it offers and maintains, methods it provides to open its accounts, and its previous experiences with Identity Theft. The College identifies the following Red Flags in each of the listed categories:

1. Notifications and Warnings from Credit Reporting Agencies Red Flags
   b. Notice or report from a credit agency of a credit freeze on an applicant.
   c. Notice or report from a credit agency of an active duty alert for an applicant.
   d. Receipt of a notice of address discrepancy in response to a credit report request.
   e. Indication from a credit report of activity that is inconsistent with an applicant’s usual pattern or activity.

2. Suspicious Documents – Red Flags
   a. Identification document or card that appears to be forged, altered or inauthentic.
   b. Identification document or card on which a person’s photograph or physical description is not consistent with the person presenting the document.
   c. Other document with information that is not consistent with existing student information.
   d. Application for service that appears to have been altered or forged.

3. Suspicious Personal Identifying Information – Red Flags
   a. Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates).
   b. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application).
   c. Identifying information present that is the same as information shown on other applications that were found to be fraudulent.
   d. Identifying information presented that is consistent with fraudulent activity such as an invalid phone number or fictitious billing address).
   e. Social security number presented that is the same as one given by another student.
f. An address or phone number presented that is the same as that of another person.
g. A person fails to provide complete personal identifying information on an application when reminded to do so.
h. A person’s identifying information is not consistent with the information that is on file for the student.

4. Suspicious Covered Account Activity or Unusual Use of Account – Red Flags
   a. Change of address for an account followed by a request to change the student’s name.
   b. Payments stop on an otherwise consistently up-to-date account.
   c. Account used in a way that is not consistent with prior use.
   d. Mail sent to the student is repeatedly returned as undeliverable.
   e. Notice to the College that a student is not receiving mail sent by the College. Notice to the College that an account has unauthorized activity.
   f. Breach in the College’s computer system security.
   g. Unauthorized access to or use of student account information.

5. Alerts from Others – Red Flags
   • Notice to the College from a student, Identity Theft victim, law enforcement or other person that the College has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

7.2.1.1 Detecting Red Flags
In order to detect any of the Red Flags identified above associated with the enrollment of a student, College personnel will take the following steps to obtain and verify the identity of the person opening the account:

• Require certain identifying information such as name, date of birth, academic records, home address or other identification.
• Verify the student’s identity at time of issuance of student identification card (review of driver’s license or other government-issued photo identification).

In order to detect any of the Red Flags identified above for an existing Covered Account, College personnel will take the following steps to monitor transactions on an account.

• Verify the identification of students if they request information (in person, via telephone, via facsimile, via email).
• Verify the validity of requests to change billing addresses by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes.
• Verify changes in banking information given for billing and payment purposes.

In order to detect any of the Red Flags identified above for an employment or volunteer position for which a credit or background report is sought, College personnel will take the following steps to assist in identifying address discrepancies:

• Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency.
• In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the College has reasonably confirmed is accurate.
In the event College personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

- Continue to monitor a Covered Account for evidence of Identity Theft.
- Contact the student or applicant (for which a credit report was run).
- Change any passwords or other security devices that permit access to Covered Accounts.
- Not open a new Covered Account.
- Provide the student with a new student identification number.
- Notify the Program Administrator for determination of the appropriate steps(s) to take.
- Notify law enforcement.
- File or assist in filing a Suspicious Activities Report (“SAR”).
- Determine that no response is warranted under the particular circumstances.

Protect Student Identifying Information – In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the College will take the following steps with respect to its internal operating procedures to protect student identifying information:

- Ensure that its Website is secure or provide clear notice that the Website is not secure.
- Ensure complete and secure destruction of paper documents and computer files containing student account information when a decision has been made to no longer maintain such information.
- Ensure that office computers with access to Covered Account information are password protected.
- Avoid use of social security numbers.
- Ensure computer virus protection is up-to-date.
- Require and keep only the kinds of student information that are necessary for College purposes.

Responsibility for developing, implementing and updating this Program lies with the Chief Information Security Officer. Division Directors will act as an ad hoc committee. The Chief Information Security Officer will be responsible for ensuring appropriate training of College staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

College staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. College staff shall be trained, as necessary, to effectively implement the Program. College employees are expected to notify the Program Administrator once they become aware of an incident of Identity Theft or of the College’s failure to comply with this Program. At least annually or as otherwise requested by the Program Administrator, College staff responsible for development, implementation, and administration of the Program shall report to the Program Administrator on compliance with this Program. The report should address such issues as effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts, service provider arrangements, significant incidents involving identity theft and management’s response, and recommendations for changes to the Program.

In the event the College engages a service provider to perform an activity in connection with one or more Covered Accounts, the College will take the following steps to ensure the service provider
performs its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft.

- Require, by contract, that service providers have such policies and procedures in place.
- Require, by contract, that service providers review the College’s Program and report any Red Flags to the Program Administrator or the College employee with primary oversight of the service provider relationship.

Non-disclosure of Specific Practices – For the effectiveness of this Identity Theft Prevention Program, knowledge about specific Red Flag identification, detection, mitigation and prevention practices may need to be limited to the Committee who developed this Program and to those employees with a need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered “confidential” and should not be share with other Green employees or the public. The Program Administrator shall inform the Committee and those employees with a need to know the information of those documents or specific practices which should be maintained in a confidential manner.

The Committee will periodically review and update this Program to reflect changes in risks to students and the soundness of the College from Identity Theft. In doing so, the Committee will consider the College’s experiences with Identity Theft situations, changes in the methods, changes in Identity Theft detection and prevention methods, and changes in the College’s business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Committee will update the Program.

7.3 CREDIT CARD PAYMENT GUIDELINES

- Credit Card Information (Cardholder Data) is obtained from customers only for business purposes and only with cardholder consent.
- The full credit card track number, including the 3 digit security code, is never solicited or kept.
- Credit cardholder data should never be kept in a ‘shadow’ database such as an Excel spreadsheet.
- Merchant receipts (receipt kept by college) should not have full card number – only the last 4 digits should be displayed. If credit card merchant service provider cannot eliminate the full card number on the merchant receipt, then the merchant receipt should be handled same as cash (i.e., locked in safe, never left unattended) and should be shredded when no longer needed.
- Cardholder data collected from phone-in sales should be destroyed by shredding immediately after the sale is processed and credit cards are settled.
- Cardholder data should never be E-mailed, faxed, or mailed (US or Intercampus) in an unsealed envelope.
- Credit card sales should be settled at least once daily.
- Access to cardholder data is on a need-to-know basis only. Supervisors are to determine who in your area has a need to access this information.
• Any suspected security breach (files that appear to have been tampered with, lost or stolen keys or passwords, etc.) should be reported to the Controller immediately.

• Passwords should be changed regularly.

• Misuse of credit card information is punishable to the full extent of the law.