INFORMATION SECURITY PLAN

CENTRAL CHRISTIAN COLLEGE OF KANSAS

Updated Summer 2018

1. PURPOSE AND OBJECTIVE

The purpose of this Information Security Plan ("ISP") is to describe how Central Christian College of Kansas ("the College," "we," or "our") complies with the Gramm-Leach-Bliley Act Safeguards Rule ("GLBA") and develops, implements, and maintains appropriate administrative, technical, and physical safeguards to protect the confidentiality of Personal Information that we access, collect, distribute, process, protect, store, use, transmit, dispose, or otherwise handle.

The objectives of this ISP are to: (1) ensure the security and confidentiality of Personal Information; (2) protect against any anticipated threats or hazards to the security or integrity of Personal Information; and (3) protect against unauthorized access to or use of Personal Information that could result in substantial harm or inconvenience to any individual.

We take seriously our responsibility to protect confidential information and to comply with applicable federal and state privacy and data security laws and regulations. To that end, we have implemented a number of policies, procedures, plans, and documents that make up our comprehensive written information security program ("CISP"). This document is one component of our CISP and should be read in conjunction with such other materials.

2. DEFINITION OF PERSONAL INFORMATION

"***Personal Information"*** includes nonpublic personally identifiable financial information and other personally identifiable information.

"***Nonpublic Personally Identifiable Financial Information***" means any information that is not publicly available and:

(i) An individual provides to obtain a financial product or service from THE COLLEGE;

(ii) About an individual resulting from a transaction with THE COLLEGE involving a financial product or service; or

(iii) THE COLLEGE otherwise obtains about an individual in connection with providing a financial product or service.

Examples of nonpublic personally identifiable financial information include (but are not limited to):

1. Information an individual provides to THE COLLEGE on an application to obtain a student loan, credit card, or other financial product or service;

2. Account balance information, payment history, loan or deposit balances, debts, overdraft history, and credit or debit card purchase information;

3. The fact that an individual has obtained federal student aid or a financial product or service from THE COLLEGE;

4. Any information an individual provides to THE COLLEGE or that THE COLLEGE otherwise obtains in connection with collecting on, or servicing, a credit account;

5. Any information THE COLLEGE collects through an Internet "cookie;";

6. Information from a consumer report; and

7. Any list, description, or other group that is derived using any nonpublic personally identifiable financial information (as described in 1-6 above) that is not publicly available.

"***Personally identifiable information"*** generally means information that can be used to distinguish or trace an individual's identity and any other information that is linked or linkable to an individual.

Examples of Personally Identifiable Information include (but are not limited to):

- First name and last name or first initial and last name
- Maiden name
- Alias
- Name of student's parents or other family members
- Mother's maiden name
- Address
- Telephone number
- Fax number
- Email address
- Social media address
- Social security number
- Driver's license number, state-issued identification card number
- Federal or state government issued identification card or tribal identification card
- Passport number
- Date of birth
- Place of birth
- Financial account number

- Bank account number
- Credit or debit card number
- Password, PIN, or other access code or security code that would permit access to the person's financial account
- Tax return information, including taxpayer identification number
- Medical (mental or physical) history information
- Medical (mental or physical) condition information
- Medical (mental or physical) treatment or diagnosis information
- Health account numbers
- Health account payment information
- Health insurance information, subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any medical information in an individual's health insurance application and claims history
- Medical records or medical record numbers
- Other insurance account number
- License plate number
- Device identifiers and serial numbers
- Fingerprints
- Digital signature
- Handwriting
- Biometric data – retina or iris scan, voice, facial geometry
- Photos, especially of face or other identifying characteristics
- Educational information, including performance evaluations
- Any unique identifying number, characteristic, or code, including electronic identification number or routing code

"Personal Information" <u>does not</u> include:

1. Publicly available information, which means information that THE COLLEGE has a reasonable basis to believe is lawfully made available to the general public from federal, state, or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state, or local law;

2. Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any Personal Information that is not publicly available; or

3. Information that does not identify an individual, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.

3. SCOPE

This ISP applies to all THE COLLEGE employees, whether full-time or part-time, including faculty, administrative staff, contract or temporary workers, consultants, interns, and student

employees. This ISP also applies to certain contracted third-party vendors. This ISP applies to any Personal Information, whether in paper, electronic, or other form, that is accessed, collected, distributed, processed, protected, stored, used, transmitted, disposed, or otherwise handled by or on behalf of THE COLLEGE or its affiliates. This ISP is not intended to supersede any existing THE COLLEGE policy that provides more specific requirements for safeguarding certain types of data, including the definition of directory information under the Family Educational Rights and Privacy Act (FERPA).

4. RISK ASSESSMENT

THE COLLEGE recognizes that there are both internal and external risks to the security, confidentiality, and integrity of Personal Information that could result in unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information. THE COLLEGE is currently using the Higher Education Security Council (HEISC) tool and the ICS-CERT Cybersecurity Evaluation Tool

THE COLLEGE has conducted a risk assessment of reasonably foreseeable internal and external risks to Personal Information in the following areas of operation:

(1) ***Internal Risks:*** Employee training and management, especially as it relates to access to and use of student records, including financial aid information;

(2) ***Operational Risks:*** Information systems, including network and software design, information processing, storage, transmission, and disposal; and

(3) ***External Risks:*** Security breaches, attacks, intrusions, and other system failures, especially as it relates to detecting, preventing, and responding to attacks or other system failures.

Based on the risks identified in the risk assessment, THE COLLEGE has assessed the sufficiency of existing safeguards and has designed and implemented the following information safeguards to minimize or control identified risks. THE COLLEGE will regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

THE COLLEGE recognizes that risks change and new risks are created periodically. THE COLLEGE will, at least annually, conduct a risk assessment and evaluate and adjust our information security program in light of the results of the testing and monitoring; any material changes to our operations or business arrangements; or any other circumstances that we know or have reason to know may have a material impact on our information security program.

5. CHIEF INFORMATION SECURITY OFFICER

THE COLLEGE has designated **DOUG VANDERHOOF** as the Chief Information Security Officer ("CISO") to coordinate our information security program. The CISO may designate other THE COLLEGE representatives to oversee and coordinate particular elements of the ISP.

Any questions or concerns regarding this ISP or THE COLLEGE information security should be addressed to the CISO at:

Doug Vanderhoof, Director, Information Technology Services

Central Christian College of Kansas – [1200 S. Main, McPherson, KS. 67460]

Email: [doug.vanderhoof@centralchristian.edu]

Office: [620-241-0723 ext. 146)]

Fax: [620-241-3529]

The CISO will be responsible for implementing, supervising, and maintaining the ISP. These responsibilities include:

- Conducting on-going training of THE COLLEGE employees regarding their responsibilities and duties under the ISP;

- Regularly conducting a risk assessment of reasonably foreseeable internal and external risks to Personal Information in the three areas of operation identified above and assessing the sufficiency of existing safeguards to control identified risks;

- Regularly testing and monitoring the effectiveness of the safeguards' key controls, systems, and procedures;

- Regularly evaluating and adjusting the information security program in light of the results of tests and monitoring; any material changes to operations or business arrangements; or any other circumstances that may have a material impact on the information security program; and

- Evaluate the ability of THE COLLEGE's third party service providers to implement and maintain appropriate safeguards and contractually require third party service providers to implement and maintain appropriate safeguards.

6. INTERNAL RISK SAFEGUARDS

- THE COLLEGE only collects Personal Information that is necessary to accomplish our legitimate business transactions or to comply with applicable laws and regulations.

- Access to Personal Information is restricted to only those employees or authorized third parties that require access in the regular course of their duties, based on their job description. Employees or third parties may only access Personal Information if they have a legitimate need to access such information.

- Personal Information shall only be used for authorized business purposes.

- THE COLLEGE will check employee references and conduct a background check before hiring employees who will have access to Personal Information where appropriate.

- A copy of this ISP will be distributed to each current employee and each new employee on the first date of employment. THE COLLEGE will require each employee to acknowledge in writing that the employee received a copy of this document and will abide by THE COLLEGE's confidentiality and security standards for handling Personal Information.

- All employees will receive initial and on-going training regarding this ISP and the steps they need to take to protect the security, confidentiality, and integrity of Personal Information. Employees will be required to certify their attendance at training sessions.

- The CISO will provide supplemental training, education, and alerts to update employees on new security issues and threats, as applicable.

- THE COLLEGE will regularly remind employees of the company policy, and the legal requirement, to keep Personal Information secure and confidential. For example, THE COLLEGE will post reminders about employees' responsibility in file rooms and other locations where Personal Information is stored.

- Employees are required to immediately report suspicious or unauthorized use of Personal Information to the CISO, including any lost or misplaced device such as a cellphone or laptop which may contain Personal Information, regardless of data encryption.

- Employees are encouraged to advise the CISO of any suspicious incident, activity, or operation which appears to pose a risk to the security of Personal Information. If an employee suspects the CISO is involved with such risk, the employee is encouraged to inform the CHIEF FINANCIAL/OPERATIONS OFFICER.

- Employees who violate this ISP will be subject to disciplinary action even if no Personal Information was compromised.

- Employees will be required to use "strong" passwords (consistent with accepted security standards) and according to NIST Special Pub 800-63B passwords are updated as required due to negotiation, neglect, phishing, or breach. Employee computers will also have password-activated screen savers to lock employee computers after a period of inactivity. Employees will receive training on how to securely protect their passwords. Employees who do not change their passwords on a regular basis will be denied access to Personal Information.

- Employees are not allowed to store or access Personal Information at home or on their personal computers.

- Employees are strongly discouraged from storing Personal Information on laptops or mobile devices (e.g., USBs, flash drives, smart phones, external hard drives). If it is necessary to transport Personal Information electronically, the transported data must be encrypted.

- Personal Information must not be stored on cloud-based storage solutions that are unsupported by THE COLLEGE.

- Employees must lock rooms or file cabinets where records containing Personal Information are kept.

- Employees are prohibited from keeping unsecured paper files containing Personal Information in their work area when they are not present.

- Employees must ensure that Personal Information is encrypted when it is transmitted electronically via public networks.

- Laptops, cell phones, and other devices must be stored in a secure place when not in use.

- Upon termination of an employment relationship with THE COLLEGE, the terminated individual's electronic and physical access to documents, systems, or networks containing Personal Information must be immediately terminated. Terminated employees must return to THE COLLEGE all records containing Personal Information, in any form, in their possession at the time of termination. All keys, keycards, access devices, badges, company IDs, business cards, and the like, shall be surrendered at the time of termination.

7. OPERATIONAL RISK SAFEGUARDS

- THE COLLEGE will maintain an inventory of all computers or other devices on which Personal Information is stored.

- THE COLLEGE will review company records and systems to determine which records and systems contain Personal Information.

- Storage areas containing records with Personal Information must be protected against destruction or damage from physical hazards, such as fire or flood.

- Records containing Personal Information should only be kept in rooms or file cabinets that are locked when unattended.

- All computers and devices must restrict user access to employees who have an authorized and unique log-in ID assigned by the CISO. User passwords must be stored in an encrypted format.

- All computers that have been inactive for fifteen (15) or more minutes will require re-log-in.

- After three (3) unsuccessful log-in attempts by a user ID, that user ID will be blocked from accessing any computer or file stored on any computer until access privileges are reestablished by the CISO.

- When Personal Information is stored on a server or computer, the server or computer must only be accessible with a "strong" password (consistent with accepted security standards) and kept in a physically-secured area.

- When practicable, all visitors must be restricted from the areas where Personal Information is accessible or stored.

- THE COLLEGE will maintain secure backup records and will keep archived data secure by storing it off-line and in a physically-secure area.

- THE COLLEGE will only transmit Personal Information securely. All Personal Information will be encrypted before it is sent or transported electronically. Any Personal Information stored on portable devices must be encrypted. Sensitive financial data will only be transmitted using SSL or other secure connection.

- Personal Information shall not be removed from THE COLLEGE premises in electronic or written form absent a legitimate business need and adherence to the security measures described herein.

- Where there is a legitimate need to provide records containing Personal Information outside THE COLLEGE, electronic records must be password-protected and/or encrypted and paper records must be marked "confidential" and securely sealed.

- Paper documents containing Personal Information shall be disposed of either by burning, pulverizing, or shredding so that the Personal Information cannot be read or reconstructed.

- Electronic media, hardware, and other non-paper media, such as computers, disks, CDs, magnetic tapes, hard drives, laptops, cellphones, USBs, etc., shall be destroyed or erased so that Personal Information cannot be read or reconstructed.

8. EXTERNAL RISK SAFEGUARDS

- THE COLLEGE will maintain up-to-date and appropriate programs and controls to prevent unauthorized access to Personal Information, including:

    - Installing and using anti-virus, anti-spyware, and anti-malware software that update automatically on any computer, device, network, or system that stores, processes, or transmits Personal Information;

    - Maintaining up-to-date firewalls and intrusion prevention on any computer, device, network, or system that stores, processes, or transmits Personal Information;

- Regularly ensuring that ports not actively used for business are closed; and

- Regularly obtaining and installing security patches to resolve software vulnerabilities.

- The CISO will promptly provide information and instructions to employees regarding any new security risks.

- THE COLLEGE will use appropriate oversight and audit procedures to detect the improper disclosure or theft of Personal Information, including:

    - Keeping logs of activity on the network and monitoring them for signs of unauthorized access to Personal Information;

    - Using an up-to-date intrusion detection system that will alert of attacks;

    - Implementing systems capable of monitoring both in-and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from the system to an unknown user; and

    - Inserting a dummy account into each customer list and monitoring the account to detect any unauthorized contacts or charges.

- THE COLLEGE will take steps to preserve the security, confidentiality, and integrity of Personal Information in the event of a security breach. See Section 10 for breach response instructions.

9. SERVICE PROVIDERS

THE COLLEGE will oversee service providers by:

- Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for Personal Information; and

- Requiring service providers to contract to implement and maintain appropriate safeguards.

THE COLLEGE will maintain a list of current third party service providers and a copy of the contracts with such service providers.

10. BREACH RESPONSE INSTRUCTIONS

Any possible or actual unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of Personal Information, or a violation or attempted violation of the information

safeguards described herein, must be reported immediately to the CISO. The CISO will document all reported or detected breaches and subsequent responsive action.

Defining a Breach

1. Event = "any observable occurrence in a system or network." Adverse event = event with "negative consequence . . . that destroys data"[1]

2. Security Incident = "Event that violates an organization's security policies and procedures."[2]

3. Privacy Incident = "Adverse event that happens as a result of violating" the college's "privacy policies and procedures" which pertains to "unauthorized use or disclosure of regulated data"[3]

4. Data Brach = A privacy incident that meets State and/or Federal breach legal definitions.

In the event of a breach of Personal Information, THE COLLEGE will:

- Take immediate action to secure any Personal Information that has or may have been compromised;

- Preserve and review files or programs that may indicate how the breach occurred; and

- If appropriate, retain professionals to assess the breach.

THE COLLEGE will follow federal and state laws and regulations with respect to breach notification.

In the event of a security breach, THE COLLEGE will review and implement appropriate safeguards to mitigate the reoccurrence of such a breach.

11. IDENTITY THEFT PREVENTION PROGRAM

THE COLLEGE has developed and implemented a written program to detect, prevent, and mitigate identity theft. The program includes policies and procedures to:

1. Identify the red flags of identity theft that may occur in day-to-day operations;

2. Detect red flags;

3. Prevent, mitigate, and respond to red flags; and

[1] NIST Computer Security Incident Handling Guide (Special Pub 800-61)
[2] Verizon's 2016 Data Breach Investigations Report
[3] Department of Homeland Security Privacy Incident Handling Guidance

4. Update the program.

12. ADDITIONAL SECURITY POLICIES

1. Family Education Right to Privacy Act of 1974 Policy
2. Red Flags Policy
3. Network Acceptable Use Policy
4. Computer System Policy
5. Password Policy