TRAVELERS

Travelers Casualty and Surety Company of America **CyberRisk Renewal Application**

Claims-Made: The information requested in this Application is for a Claims-Made policy. If issued, the policy will apply only to claims first made during the policy period, or any applicable extended reporting period.

Defense Within Limits: The limits of liability will be reduced, and may be completely exhausted, by amounts paid as defense costs, and any retention will be applied against defense costs. The Insurer will not be liable for the amount of any judgment, settlement, or defense costs incurred after exhaustion of the limit of liability.

IMPORTANT INSTRUCTIONS

Under this CyberRisk Coverage, affiliates, other than Subsidiaries as defined in this coverage, are not covered unless the Insurer has agreed specifically to schedule such entities by endorsement.

GENERAL INFORMATION

Name of Applicant: Carl Sandburg College

Street Address: 2400 Tom L Wilson

City: Galesburg State: IL Zip: 61401

Applicant website: www.sandburg.edu

Expiring Policy Number: Year Established: 1966 NAICS Code: 611210

Total assets as of most recent fiscal year-end: $ 113,054,327.00

Annual revenues or expenditures as of most recent fiscal year-end: $ 28,730,920.00

Entity type (select all that apply):

□ Private □ Nonprofit □ Financial Institution □ Publicly Traded □ Franchisor or Franchisee □ Homeowner or Condo Association ☒ Public Entity

REQUESTED INSURANCE TERMS

1. Does the Applicant desire any changes to the expiring policy limits or retentions? □ Yes □ No

If Yes, indicate the desired changes in the table below.

Requested Terms:

Insuring Agreement	Limit Requested	Retention Requested
Privacy And Security	$	$
Media	$	$
Regulatory Proceedings	$	$
Privacy Breach Notification	$	$
Computer And Legal Experts	$	$
Betterment	$	$
Cyber Extortion	$	$
Data Restoration	$	$
Public Relations	$	$
Computer Fraud	$	$
Funds Transfer Fraud	$	$
Social Engineering Fraud	$	$
Telecom Fraud	$	$
Business Interruption	$	$
Dependent Business Interruption	$	$
Reputation Harm	$	$

© 2020 The Travelers Indemnity Company. All rights reserved.

2. Solely with respect to increased limits, is the Applicant, any Subsidiary, or any person proposed for this insurance aware of any circumstance that could give rise to a claim against them under this CyberRisk coverage? □ Yes □ No

3. Requested Terms:
Aggregate Limit Requested: $ ……………………

UNDERWRITING INFORMATION

DATA INVENTORY

4. Indicate whether the Applicant, or a third party on the Applicant's behalf, collects, receives, processes, transmits, or maintains the following types of data as part of its business activities:

a. Credit/Debit Card Data ☒ Yes □ No

If Yes:

i. Is the Applicant currently compliant with Payment Card Industry Data Security Standards (PCI-DSS)? □ Yes ☒ No

ii. How many credit card transactions are processed or accepted for payment in a typical year? ……………………

iii. What is the Applicant's reporting level? □ 1 □ 2 □ 3 □ 4

iv. Was the Applicant's last PCI assessment conducted within the past 12 months? □ Yes ☒ No

b. Medical information, other than that of the Applicant's own employees ☒ Yes □ No

c. Non-employee Social Security Numbers ☒ Yes □ No

d. Employee/HR Information ☒ Yes □ No

5. What is the approximate number of unique individuals for whom the Applicant, or a third party on the Applicant's behalf, collects, stores, or processes any amount of personal information as outlined in Question 4?

☒ fewer than 100,000 □ 100,000 – 250,000 □ 250,001 – 500,000 □ 500,001 – 1,000,000
□ 1,000,001 – 2,500,000 □ 2,500,001 – 5,000,000 □ > 5,000,000

6. Indicate whether the data indicated in Question 4 is encrypted:

a. While at rest in the Applicant's databases or on the Applicant's network □ Yes ☒ No □ N/A

b. While in transit in electronic form □ Yes ☒ No □ N/A

c. While on mobile devices □ Yes ☒ No □ N/A

d. While on employee owned devices □ Yes ☒ No □ N/A

e. While in the care, custody, and control of a third party service provider ☒ Yes □ No □ N/A

7. Is the Applicant a Healthcare Provider, Business Associate, or Covered Entity under HIPAA? □ Yes ☒ No

If Yes, is the Applicant HIPAA compliant? □ Yes □ No

8. Is the Applicant subject to the General Data Protection Regulation (GDPR)? □ Yes ☒ No

If Yes, is the Applicant currently compliant with GDPR? □ Yes ☒ No

If the Applicant is subject to GDPR, and is not currently compliant, attach a description of steps being taking toward compliance.

PRIVACY CONTROLS

9. Indicate whether the Applicant currently has the following in place:

a. A Chief Privacy Officer or other individual assigned responsibility for monitoring changes in statutes and regulations related to handling and use of sensitive information ☒ Yes □ No

b. A publicly available privacy policy which has been reviewed by an attorney ☒ Yes □ No

c. Sensitive data classification and inventory procedures ☒ Yes □ No

d. Data retention, destruction, and record keeping procedures ☒ Yes □ No

e. Annual privacy and information security training for employees ☒ Yes □ No

f. Restricted access to sensitive data and systems based on job function ☒ Yes □ No

NETWORK SECURITY CONTROLS

10. Indicate whether the Applicant currently has the following in place:

a. A Chief Information Security Officer or other individual assigned responsibility for privacy and security practices ☒ Yes □ No

b. Up-to-date, active firewall technology ☒ Yes □ No

© 2020 The Travelers Indemnity Company. All rights reserved.

c. Up-to-date, active anti-virus software on all computers, networks, and mobile devices ☒ Yes ☐ No

d. A process in place to regularly download, test, and install patches ☒ Yes ☐ No

If Yes, is this process automated? ☒ Yes ☐ No

If Yes, are critical patches installed within 30 days of release? ☒ Yes ☐ No

e. Intrusion Detection System (IDS) ☒ Yes ☐ No

f. Intrusion Prevention System (IPS) ☒ Yes ☐ No

g. Data Loss Prevention System (DLP) ☒ Yes ☐ No

h. Multi-factor authentication for administrative or privileged access ☒ Yes ☐ No ☐ N/A

i. Multi-factor authentication for remote access to the Applicant's network and other systems and programs that contain private or sensitive data in bulk ☒ Yes ☐ No ☐ N/A

j. Multi-factor authentication for remote access to email ☒ Yes ☐ No ☐ N/A

k. Remote access to the Applicant's network limited to VPN ☒ Yes ☐ No ☐ N/A

l. Backup and recovery procedures in place for all important business and customer data ☒ Yes ☐ No

If Yes, are such procedures automated? ☒ Yes ☐ No

If Yes, are such procedures tested on an annual basis? ☒ Yes ☐ No

m. Annual penetration testing ☒ Yes ☐ No

If Yes, is such testing conducted by a third party service provider? ☒ Yes ☐ No

n. Annual network security assessments ☒ Yes ☐ No

If Yes, are such assessments conducted by a third party service provider? ☒ Yes ☐ No

o. Systematic storage and monitoring of network and security logs ☒ Yes ☐ No

p. Enforced password complexity requirements ☒ Yes ☐ No

q. Procedures in place to terminate user access rights as part of the employee exit process ☒ Yes ☐ No

PAYMENT CARD CONTROLS

Complete only if the Applicant, or a third party on the Applicant's behalf, collects, processes, stores, or accepts payment card information.

11. Indicate whether the Applicant's current payment card environment:

a. Processes all payment cards using End-to-End or Point-to-Point encryption ☒ Yes ☐ No

b. Encrypts or tokenizes card data when stored ☒ Yes ☐ No

c. Processes card present transactions using EMV capable devices ☒ Yes ☐ No ☐ N/A

CONTENT LIABILITY CONTROLS

☐ **Media Liability Coverage is not requested.**

12. Does the Applicant have a comprehensive written program in place for managing intellectual property rights? ☒ Yes ☐ No

13. Indicate whether the Applicant has formal policies or procedures for:

a. Avoiding the dissemination of content that infringes upon intellectual property rights ☒ Yes ☐ No

b. Editing or removing controversial, offensive, or infringing content from material distributed or published by or on behalf of the Applicant ☒ Yes ☐ No

c. Responding to allegations that content created, displayed, or published by the Applicant is libelous, infringing, or in violation of a third party's privacy rights ☒ Yes ☐ No

BUSINESS CONTINUITY / DISASTER RECOVERY / INCIDENT RESPONSE

14. Indicate whether the Applicant has the following:

a. A disaster recovery plan, business continuity plan, or equivalent to respond to a computer system disruption ☒ Yes ☐ No

b. An incident response plan to respond to a network intrusion ☒ Yes ☐ No

15. Are all plans indicated above tested regularly with any critical deficiencies remediated? ☒ Yes ☐ No ☐ N/A

16. Based upon testing results, how long does it take to restore the Applicant's critical business operations following a network or systems interruption?

☐ Unknown ☐ 0 – 12 hours ☒ 12 – 24 hours ☐ More than 24 hours

VENDOR CONTROLS

17. For vendors with access to the Applicant's computer system or confidential information, indicate whether the Applicant has the following in place:

© 2020 The Travelers Indemnity Company. All rights reserved.

a. Written policies which specify appropriate vendor information security controls ☒ Yes □ No

b. Periodic review of, and updates to, vendor access rights ☒ Yes □ No

c. Prompt revocation of vendor access rights when access is no longer needed ☒ Yes □ No

d. Logging and monitoring of vendor access to the Applicant's system ☒ Yes □ No

e. A requirement that vendors carry their own Professional Liability or Cyber Liability insurance ☒ Yes □ No

f. Hold harmless / indemnity clauses that benefit the Applicant in contracts with vendors ☒ Yes □ No

18. Indicate which of the following services are outsourced:

Data back up	☒ Yes □ No □ N/A	Payment processing	☒ Yes □ No □ N/A
Provider:		Provider:	
Data center hosting	□ Yes ☒ No □ N/A	Physical security	□ Yes ☒ No □ N/A
Provider:		Provider:	
IT infrastructure	□ Yes ☒ No □ N/A	Software development	□ Yes ☒ No □ N/A
Provider:		Provider:	
IT security	□ Yes □ No □ N/A	Customer marketing	□ Yes ☒ No □ N/A
Provider:		Provider:	
Web hosting	☒ Yes □ No □ N/A	Data processing	□ Yes ☒ No □ N/A
Provider:		Provider:	

If Data center hosting or IT infrastructure is answered Yes above:

a. What is the likely impact to the organization if these services become unavailable?

b. Does the Applicant have an alternative solution in the event of a failure or outage to one of these service providers?

If Payment processing is answered Yes above, does the Applicant have an alternative means of processing card data in the event of an outsourced provider failure or outage? □ Yes ☒ No

Provide details:

REQUIRED ATTACHMENTS

As part of this Application, provide copies of the documents listed below. Such documents are made a part of this Application; the Insurer may elect to obtain requested information from public sources, including the Internet.

- CyberRisk Employed Lawyers Supplement to be completed if Employed Lawyers coverage is sought.

ORGANIZATIONS NOT ELIGIBLE FOR COVERAGE

Coverage will not be considered for companies involved in whole or in part with paramilitary operations, pornography, adult entertainment, escort services, prostitution, or the manufacturing, distribution, or sale of marijuana.

NOTICE REGARDING COMPENSATION

For information about how Travelers compensates independent agents, brokers, or other insurance producers, please visit this website: http://www.travelers.com/w3c/legal/Producer_Compensation_Disclosure.html

If you prefer, you can call the following toll-free number: 1-866-904-8348. Or you can write to us at Travelers, Agency Compensation, One Tower Square, Hartford, CT 06183.

FRAUD STATEMENTS – ATTENTION APPLICANTS IN THE FOLLOWING JURISDICTIONS

ALABAMA, ARKANSAS, DISTRICT OF COLUMBIA, MARYLAND, NEW MEXICO, AND RHODE ISLAND: Any person who knowingly (or willfully in MD) presents a false or fraudulent claim for payment of a loss or benefit or who knowingly (or willfully in MD) presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

COLORADO: It is unlawful to knowingly provide false, incomplete, or misleading facts or information to an insurance company to defraud or attempt to defraud the company. Penalties may include imprisonment, fines, denial of insurance, and civil damages. Any insurance company or agent of an insurance company who knowingly provides false, incomplete, or misleading facts or information to a policyholder or claimant to defraud or attempt to defraud the policyholder or claimant regarding a settlement or award payable from insurance proceeds will be reported to the Colorado Division of Insurance within the Department of Regulatory Agencies.

© 2020 The Travelers Indemnity Company. All rights reserved.

FLORIDA: Any person who knowingly and with intent to injure, defraud, or deceive any insurer files a statement of claim or an application containing any false, incomplete, or misleading information is guilty of a felony of the third degree.

KENTUCKY, NEW JERSEY, NEW YORK, OHIO, AND PENNSYLVANIA: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information or conceals for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime and subjects such person to criminal and civil penalties. (In New York, the civil penalty is not to exceed five thousand dollars ($5,000) and the stated value of the claim for each such violation.)

LOUISIANA, MAINE, TENNESSEE, VIRGINIA, AND WASHINGTON: It is a crime to knowingly provide false, incomplete, or misleading information to an insurance company to defraud the company. Penalties include imprisonment, fines, and denial of insurance benefits.

OREGON: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or who knowingly presents false information in an application for insurance may be guilty of a crime and may be subject to fines and confinement in prison.

PUERTO RICO: Any person who knowingly and intending to defraud presents false information in an insurance application, or presents, helps, or causes the presentation of a fraudulent claim for the payment of a loss or any other benefit, or presents more than one claim for the same damage or loss, will incur a felony and, upon conviction, will be sanctioned for each violation with the penalty of a fine of not less than $5,000 and not over $10,000, or a fixed term of imprisonment for three years, or both penalties. Should aggravating circumstances be present, the penalty established may be increased to a maximum of five years; if extenuating circumstances are present, it may be reduced to a minimum of two years.

SIGNATURES

The undersigned Authorized Representative represents that to the best of his or her knowledge and belief, and after reasonable inquiry, the statements provided in response to this Application are true and complete, and, except in NC, may be relied upon by Travelers as the basis for providing insurance. The Applicant will notify Travelers of any material changes to the information provided.

□ Electronic Signature and Acceptance – Authorized Representative*

*If electronically submitting this document, electronically sign this form by checking the Electronic Signature and Acceptance box above. By doing so, the Applicant agrees that use of a key pad, mouse, or other device to check the Electronic Signature and Acceptance box constitutes acceptance and agreement as if signed in writing and has the same force and effect as a signature affixed by hand.

Authorized Representative Signature: **X** Seamus Reilly	Authorized Representative Name, Title, and email address: SEAMUS REILLY, PRESIDENT sReilly@sandburg.edu	Date *(month/dd/yyyy)*: 5/20/2024
Producer Name (required in FL & IA): **X**	State Producer License No (required in FL):	Date *(month/dd/yyyy)*:
Agency:	Agency contact and email address:	Agency Phone Number:

ADDITIONAL INFORMATION

© 2020 The Travelers Indemnity Company. All rights reserved.

TRAVELERS

Travelers Property Casualty Company of America **Multi-Factor Authentication Supplement**

Claims-Made: The information requested in this Application is for a Claims-Made policy. If issued, the policy will apply only to claims first made during the policy period, or any applicable extended reporting period.

Defense Within Limits: The limits of liability will be reduced, and may be completely exhausted, by amounts paid as defense costs, and any retention will be applied against defense costs. The Insurer will not be liable for the amount of any judgment, settlement, or defense costs incurred after exhaustion of the limit of liability.

GENERAL INFORMATION

Name of Applicant:
Carl Sandburg College

Street Address:
2400 Tom L. Wilson

City: Galesburg State: IL Zip: 6401

Applicant Website(s):
www.sandburg.edu

Multi-Factor Authentication

Multi-factor authentication refers to the use of two or more means of identification and access control—sometimes referred to as "something you know, something you have, or something you are." A username and password, for example, is something you know. Requiring a code sent via text message (SMS) establishes "something you have," i.e., a mobile phone belonging to you. Biometric authentication, through a fingerprint or retina scan, establishes "something you are." Multi-factor authentication is successfully enabled when at least two of these categories of identification are required in order to successfully verify a user's identity when accessing systems.

Multi-Factor Authentication for Remote Network Access

Requiring multi-factor authentication for remote network access is an important security control that can help reduce the potential for a network compromise caused by lost or stolen passwords. Without this control an intruder can gain access to an insured's network in a similar manner to an authorized user.

Multi-Factor Authentication for Administrative Access

Requiring multi-factor authentication for both remote and internal access to administrative accounts helps to prevent intruders that have compromised an internal system from elevating privileges and obtaining broader access to a compromised network. The existence of this control can prevent an intruder from gaining the level of access necessary to successfully deploy ransomware across the network.

Multi-Factor Authentication for Remote Access to Email

Requiring multi-factor authentication for remote access to email can help reduce the potential for a compromise to corporate email accounts caused by lost or stolen passwords. Without this control an intruder can easily gain access to a user's corporate email account. Threat actors often use this access to perpetrate various cyber crime schemes against the impacted organization and its clients and customers.

MULTI-FACTOR AUTHENTICATION

For any "No" answers, provide an explanation in the Additional Information section provided at the end of this Application.

1. Multi-Factor authentication is required for all employees when accessing email through a website or cloud based service. ☒ Yes ☐ No ☐ Email is not web based
2. Multi-Factor authentication is required for all remote access to the network provided to employees, contractors, and 3rd party service providers. ☒ Yes ☐ No

© 2023 The Travelers Indemnity Company. All rights reserved.

3. In addition to remote access, multi-factor authentication is required for the following, including such access provided to 3rd party service providers:

   a. All internal & remote admin access to directory services (active directory, LDAP, etc.). ☒ Yes □ No

   b. All internal & remote admin access to network backup environments. ☒ Yes □ No

   c. All internal & remote admin access to network infrastructure (firewalls, routers, switches, etc.). ☒ Yes □ No

   d. All internal & remote admin access to the organization's endpoints/servers. ☒ Yes □ No

4. The signer of this form has done so with the assistance of the person in charge of IT security. ☑ Yes □ No

NOTICE REGARDING COMPENSATION

For information about how Travelers compensates independent agents, brokers, or other insurance producers, please visit this website: http://www.travelers.com/w3c/legal/Producer_Compensation_Disclosure.html

If you prefer, you can call the following toll-free number: 1-866-904-8348. Or you can write to us at Travelers, Agency Compensation, One Tower Square, Hartford, CT 06183.

FRAUD STATEMENTS – ATTENTION APPLICANTS IN THE FOLLOWING JURISDICTIONS

ALABAMA, ARKANSAS, DISTRICT OF COLUMBIA, MARYLAND, NEW MEXICO, AND RHODE ISLAND: Any person who knowingly (or willfully in MD) presents a false or fraudulent claim for payment of a loss or benefit or who knowingly (or willfully in MD) presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

CALIFORNIA: For your protection California law requires the following to appear on this form. Any person who knowingly presents false or fraudulent information to obtain or amend insurance coverage or to make a claim for the payment of a loss is guilty of a crime and may be subject to fines and confinement in state prison.

COLORADO: It is unlawful to knowingly provide false, incomplete, or misleading facts or information to an insurance company to defraud or attempt to defraud the company. Penalties may include imprisonment, fines, denial of insurance, and civil damages. Any insurance company or agent of an insurance company who knowingly provides false, incomplete, or misleading facts or information to a policyholder or claimant to defraud or attempt to defraud the policyholder or claimant regarding a settlement or award payable from insurance proceeds will be reported to the Colorado Division of Insurance within the Department of Regulatory Agencies.

FLORIDA: Any person who knowingly and with intent to injure, defraud, or deceive any insurer files a statement of claim or an application containing any false, incomplete, or misleading information is guilty of a felony of the third degree.

KENTUCKY, NEW JERSEY, NEW YORK, OHIO, AND PENNSYLVANIA: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information or conceals for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime and subjects such person to criminal and civil penalties. (In New York, the civil penalty is not to exceed five thousand dollars ($5,000) and the stated value of the claim for each such violation.)

LOUISIANA, MAINE, TENNESSEE, VIRGINIA, AND WASHINGTON: It is a crime to knowingly provide false, incomplete, or misleading information to an insurance company to defraud the company. Penalties include imprisonment, fines, and denial of insurance benefits.

OREGON: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or who knowingly presents false information in an application for insurance may be guilty of a crime and may be subject to fines and confinement in prison.

PUERTO RICO: Any person who knowingly and intending to defraud presents false information in an insurance application, or presents, helps, or causes the presentation of a fraudulent claim for the payment of a loss or any other benefit, or presents more than one claim for the same damage or loss, will incur a felony and, upon conviction, will be sanctioned for each violation with the penalty of a fine of not less than $5,000 and not over $10,000, or a fixed term of imprisonment for three years, or both penalties. Should aggravating circumstances be present, the penalty established may be increased to a maximum of five years; if extenuating circumstances are present, it may be reduced to a minimum of two years.

© 2023 The Travelers Indemnity Company. All rights reserved.

SIGNATURES

The undersigned Executive Officer represents that to the best of his or her knowledge and belief, and after reasonable inquiry, the statements provided in response to this Application are true and complete, and, except in North Carolina may be relied upon by Travelers as the basis for providing insurance. The Applicant will notify Travelers of any material changes to the information provided.

□ Electronic Signature and Acceptance – Executive Officer

*If electronically submitting this document, electronically sign this form by checking the Electronic Signature and Acceptance box above. By doing so, the Applicant agrees that use of a key pad, mouse, or other device to check the Electronic Signature and Acceptance box constitutes acceptance and agreement as if signed in writing and has the same force and effect as a signature affixed by hand.

**Executive Officer is defined as the applicant's chief executive officer, chief financial officer, chief information security officer, risk manager, in-house general counsel, or the functional equivalent.*

Executive Officer Signature: X Seamus Reilly	Executive Officer Name and Title: SEAMUS REILLY, President	Date *(month/dd/yyyy)*: 5/20/2024
Producer Name (required in FL & IA): X N/A	State Producer License No (required in FL):	Date *(month/dd/yyyy)*:
Agency: N/A	Agency contact and email address:	Agency Phone Number:

ADDITIONAL INFORMATION

© 2023 The Travelers Indemnity Company. All rights reserved.