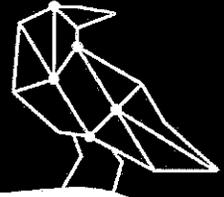# Application for
Smart Cyber Insurance®

1. Company Name

   ## Spartanburg School District 3

2. Company Address

   3535 Clifton Glendale Road, Spartanburg, SC 29307

3a. Primary Website[1]

   ## www.spartanburg3.org

3b. Additional Websites

   www.dmtconline.org

4. Nature of Business (Industry)

   ## Public Education

5. Projected Gross Annual Revenue (next 12 months)

   ## $45,000,000

6. Estimated amount of unique personally identifiable records[2] maintained by the Applicant (including records stored by third-party providers).

   ☑ **0–250,000**　　☐ **500,001–1,000,000**　　☐ **2,500,001–5,000,000**　　☐ **10,000,000+**
   ☐ **250,001–500,000**　　☐ **1,000,001–2,500,000**　　☐ **5,000,001–10,000,000**

7. Does the Applicant have formal processes for regularly backing up, archiving, restoring, and segregating sensitive data?　　◉ **Yes**　○ **No**

8. If the Applicant accepts payment cards in exchange for goods or services rendered, is the Applicant or their outsourced payment processor PCI-DSS compliant?　　◉ **Yes**　○ **No**　○ **N/A**

9. If the Applicant allows remote access to their network, do they use a properly configured VPN or Multi-Factor Authentication?　　◉ **Yes**　○ **No**　○ **N/A**

10. Does the Applicant use Multi-Factor Authentication to secure all domain or network administrator accounts?　　◉ **Yes**　○ **No**

11. If the Applicant's users can access email through a web app on a non-corporate device, does the Applicant enforce Multi-Factor Authentication?　　◉ **Yes**　○ **No**　○ **N/A**

12. Does the Applicant use an email security filtering tool?
    If Yes: Please list the vendor.　　◉ **Yes**　○ **No**

    ## Windows Defender and KnowBe4

CORVUS

13. If the Applicant stores over 1MM PII records, do they encrypt private or sensitive information stored on mobile devices[3]? ○ Yes ○ No ◉ N/A

14. If the Applicant's industry is retail, restaurant, or online retailer, do they deploy either end-to-end or point-to-point encryption technology on all of their point of sale terminals? ○ Yes ○ No ◉ N/A

15. If revenue is over $100MM and the Applicant uses multimedia material provided by others, does the Applicant always obtain the necessary rights, licenses, releases, and consents prior to publishing? ○ Yes ○ No ◉ N/A

16. Has the Applicant experienced in the past three years any cyber security incident, data privacy incident or any multimedia liability claim[4]? ○ Yes ◉ No
    If Yes: Is the actual or expected total financial impact to the Applicant and its insurer more than $25,000? ○ Yes ○ No ◉ N/A
    Please provide additional details.

17. Does the Applicant or any other person or organization proposed for this insurance have knowledge of any actual or alleged: security breach, privacy breach, privacy-related event or incident, breach of privacy, or multimedia incident[5] that may reasonably be expected to give rise to a claim or to costs being incurred? ○ Yes ◉ No
    If Yes: Please provide additional details.

18. Has the Applicant or any other organization proposed for this insurance sustained any unscheduled network outage or interruption lasting longer than six hours within the past twenty-four months? ○ Yes ◉ No
    If Yes: Please provide additional details.

CORVUS

19. Additional Notes

20. Desired Limit/Retention Options (check all desired pairs)

		Retentions							
		$2.5k	$5k	$10k	$15k	$25k	$50k	$100k	$250k
Limits (Each Claim/Aggregate)	$500k/$500k								
	$1MM/$1MM					✔			
	$2MM/$2MM								
	$3MM/$3MM								
	$4MM/$4MM								
	$5MM/$5MM								
	$10MM/$10MM								

James G. Mack Digitally signed by James G. Mack Date: 2023.03.02 16:36:47 -05'00'   James G. Mack   03.02.2023
Applicant Signature   Print Name   Date

gmack@spartanburg3.org   Asst. Supt. for Fin & Ops
Applicant Email Address[6] (optional)   Applicant Title (optional)

FOOTNOTES

[1] Corvus runs a scan on the Applicant's primary corporate website and any affiliated sites in order to create our Dynamic Loss Prevention report. We include the high-level results of the scan in our quote along with a preview of several personalized recommendations for the Applicant. After the Applicant binds a quote, Corvus generates a full report detailing the results of the scan, including all of our personalized recommendations for the Applicant.

[2] PII includes any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

[3] Laptops, tablets, phones, hard drives, USB drives, etc.

[4] A multimedia liability claim includes one alleging defamation, disparagement, invasion of privacy, commercial misappropriation of likeness, plagiarism, piracy, or copyright or trademark infringement.

[5] Defamation, disparagement, invasion of privacy, commercial misappropriation of likeness, plagiarism, piracy, or copyright or trademark infringement.

[6] You will be added to our software platform, the CrowBar, which provides helpful risk management advice, alerts and services.

CORVUS

NOTICE

Notice to All Applicants: 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, for the purpose of misleading, conceals information concerning any fact material thereto, may commit a fraudulent insurance act which is a crime and subjects such person to criminal and civil penalties in many states.

Notice to Colorado Applicants: It is unlawful to knowingly provide false, incomplete or misleading facts or information to an insurance company for the purpose of defrauding or attempting 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 for the purpose of defrauding or attempting to defraud the policyholder or claiming with regard to a settlement or award payable for insurance proceeds shall be reported to the Colorado Division of Insurance within the Department of Regulatory Agencies.

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

Notice to Florida Applicants: Any person who knowingly and with intent to injure, defraud or deceive any insurance company, files a statement of claim containing any false, incomplete, or misleading information is guilty of a felony of the third degree.

Notice to Oklahoma Applicants: Any person who knowingly, and with intent to injure, defraud or deceive any insurer,files a statement of claim containing any false, incomplete or misleading information is guilty of a felony.

Notice to Kansas Applicants: An act committed by any person who, knowingly and with intent to defraud, presents,causes to be presented or prepares with knowledge or belief that it will be presented to or by an insurer, purported insurer, broker or any agent thereof, any written statement as part of, or in support of, an application for the issuance of, or the rating of an insurance policy for personal or commercial insurance, or a claim for payment or other benefit pursuant to an insurance policy for commercial or personal insurance which such person knows to contain materially false information concerning any fact material thereto; or conceals, for the purpose of misleading, information concerning any fact material thereto.

Notice to Maine, Tennessee, Virginia and Washington Applicants: It is a crime to knowingly provide false,incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties may include imprisonment, fines and/or denial of insurance benefits.

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

Notice to New Hampshire Applicants: Any person who, with a purpose to injure, defraud or deceive an insurance company, files a statement of claim containing any false, incomplete or misleading information is subject to prosecution and punishment for insurance fraud as provided in RSA 638:20.

Notice to New York Applicants: 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 shall also be subject to a civil penalty not to exceed $5,000 and the stated value of the claim for each such violation.

Notice to Pennsylvania Applicants: 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 purposes 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.

CORVUS

&CORVUS

Ransomware Supplemental Application

EMAIL SECURITY

1. Company Name

Spartanburg School District Three

2. If your users can access email through a web app on a non-corporate device, do you enforce Multi-Factor Authentication? ☒ Yes ○ No

3a. Which email security filtering tool are you using?

Microsoft Defender and KnowBe4

3b. Are you using all available security features (for example: quarantine service, sandboxing and URL rewriting)? ☒ Yes ○ No

4. Do you conduct regular phishing training and testing?

○ Quarterly ☒ Semi-annually ○ Annually ○ Never

5. Do you have a secure web gateway or proxy solution to secure inbound internet traffic? ☒ Yes ○ No

DATA BACK-UP & RECOVERY

6. How frequently do you back up electronic data?

☒ Daily with multi-generations retained ○ Daily ○ Weekly ○ Less than weekly

7. Are all of your backups kept separate from your network ("offline") so that they are inaccessible from endpoints and servers that are joined to the corporate domain, or in a cloud service designed for this purpose? ☒ Yes ○ No

If no: please describe compensating controls that you have in place.

8. Is Multi-Factor Authentication required for access to backup files? ☒ Yes ○ No

9. Have you tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months? ☒ Yes ○ No

CORVUS

10. As part of your data back-up strategy, do you maintain at least 3 separate copies of your data stored in different geographic locations? (Production, Local Copies, and offsite storage). ☒ Yes ○ No

INTERNAL SECURITY & CONTROLS

11. Do you use Multi-Factor Authentication to secure all domain or network administrator accounts? ☒ Yes ○ No

12. Do you restrict employee access to sensitive information on a business-need to know basis? ☒ Yes ○ No

13. Do you use an Endpoint Detection and Response (EDR) or a Next-Generation Antivirus (NGAV) (i.e. CrowdStrike, SentinelOne, CybeReason, Carbon Black) software to secure all system endpoints? ☒ Yes ○ No

If yes: please list providers.

Cisco Amp

---

14. Do you allow remote access to your network? ☒ Yes ○ No

If yes: do you use

a) a properly configured and secure VPN? ☒ Yes ○ No

b) Multi-Factor Authentication to secure all remote access to your network? ☒ Yes ○ No

15. Do you have a Business Continuity Plan (BCP) or Disaster Recovery Plan (DRP) in place? ☒ Yes ○ No

If yes: is your BCP/DRP tested at least annually? ○ Yes ☒ No

16. Do you encrypt all sensitive and confidential information

a) stored on your organization's systems and networks? ☒ Yes ○ No

b) stored on your organization's backups? ☒ Yes ○ No

If no to either: are the following compensating controls in place:

I) Segregation of servers that store sensitive and confidential information? ☒ Yes ○ No

II) Access control with role-based assignments? ☒ Yes ○ No

CORVUS

17. Do you encrypt all sensitive and confidential information

   c) stored on mobile devices?   ☒ Yes   ○ No

   d) in transit from your network?   ☒ Yes   ○ No

Warranty

All insureds agree that the statements contained herein are their agreements and representations, which shall be deemed material to the risk, and that, if issued, the Policy will be in reliance upon the truth thereof. The misrepresentation or non-disclosure of any material matter by the Insured or its agent will render the Policy null and void and relieve the Company from all liability under the Policy.

Signature   _Sinus G. Mack_   _06/14/23 03.02023_
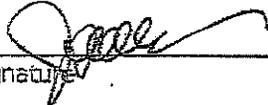
Signature   Print Name   Date

Policyholder Disclosure: Notice of Terrorism Insurance Exclusion and Coverage Option

You are hereby notified that under the Terrorism Risk Insurance Act, as amended, you now have a right to purchase insurance coverage for losses resulting from acts of terrorism, as defined in Section 102(1) of the Act. The term "act of terrorism" means any act that is certified by the Secretary of the Treasury – in consultation with the Secretary of Homeland Security, and the Attorney General of the United States – to be an act of terrorism; to be a violent act or an act that is dangerous to human life, property, or infrastructure; to have resulted in damage within the United States, or outside the United States in the case of an air carrier or vessel or the premises of a United States mission; and to have been committed by an individual or individuals acting on behalf of any foreign person or foreign interest, as part of an effort to coerce the civilian population of the United States or to influence the policy or affect the conduct of the United States Government by coercion.

YOU SHOULD KNOW THAT WHERE COVERAGE IS PROVIDED BY THIS POLICY FOR LOSSES RESULTING FROM CERTIFIED ACTS OF TERRORISM SUCH LOSSES MAY BE PARTIALLY REIMBURSED BY THE UNITED STATES GOVERNMENT UNDER A FORMULA ESTABLISHED BY FEDERAL LAW. HOWEVER, YOUR POLICY MAY CONTAIN OTHER EXCLUSIONS WHICH MIGHT AFFECT YOUR COVERAGE, SUCH AS AN EXCLUSION FOR NUCLEAR EVENTS. UNDER THIS FORMULA, THE UNITED STATES GOVERNMENT GENERALLY REIMBURSES 85% THROUGH 2015; 84% BEGINNING ON JANUARY 1, 2016; 83% BEGINNING ON JANUARY 1, 2017; 82% BEGINNING ON JANUARY 1, 2018; 81% BEGINNING ON JANUARY 1, 2019 AND 80% BEGINNING ON JANUARY 1, 2020 OF COVERED TERRORISM LOSSES EXCEEDING THE STATUTORILY ESTABLISHED DEDUCTIBLE PAID BY THE INSURANCE COMPANY PROVIDING THE COVERAGE. THE PREMIUM CHARGED FOR THIS COVERAGE IS PROVIDED BELOW AND DOES NOT INCLUDE ANY CHARGES FOR THE PORTION OF LOSS COVERED BY THE FEDERAL GOVERNMENT UNDER THE ACT.

YOU SHOULD ALSO KNOW THAT THE TERRORISM RISK INSURANCE ACT, AS AMENDED, CONTAINS A $100 BILLION CAP THAT LIMITS U.S. GOVERNMENT REIMBURSEMENT AS WELL AS INSURERS' LIABILITY FOR LOSSES RESULTING FROM CERTIFIED ACTS OF TERRORISM WHEN THE AMOUNT FOR SUCH LOSSES IN ANY ONE CALENDAR YEAR EXCEEDS $100 BILLION. IF THE AGGREGATE INSURED LOSSES FOR ALL INSURERS EXCEED $100 BILLION, YOUR COVERAGE MAY BE REDUCED.

You have the right to accept or reject any coverage that might be provided under provisions of the Act and under the terms, conditions and exclusions of the policy. If you decide to purchase a policy from us and wish to take advantage of any terrorism coverage that might be provided, you will have to pay an additional premium for terrorism coverage in the amount of:

Limit Each Trigger	Aggregate Limit	Retention Each Trigger	Base Premium*	Additional Premium for Certified Acts of Terrorism Coverage* (1% of Base)
$1,000,000	$1,000,000	$25,000	$13,882	$139

*does not include surplus lines taxes and/or fees

Even if you do decide to take advantage of any terrorism coverage that might be provided under terms of the Act, we will exclude coverage for losses not eligible for federal reinsurance under the Act, which include losses due to domestic acts of terrorism and losses due to acts of terrorism to property located outside the United States. Further, as respects all losses, even losses eligible for federal reinsurance under the Act, the actual coverage available under our policies for acts of terrorism will still be limited by all of the terms, conditions, exclusions and endorsements of the policy and by generally applicable rules of law. This means that even if you decide to pay the additional premium to buy terrorism coverage to the extent provided under the Act, all terms, conditions and exclusions in the policy, will apply, even if they prevent coverage for losses resulting from terrorism.

If you decide not to accept this offer of terrorism coverage to the extent provided by the Act and not otherwise excluded by the policy, you must sign below to waive such coverage and return the original of this document to us.

Waiver of Coverage

I/we hereby waive all rights to any coverage for terrorism that may have been available under the Terrorism Risk Insurance Act and authorize Accredited Specialty Insurance Company to fully exclude terrorism coverage under the policy issued or to be issued to me/us.

Proposed Named Insured

SPARTANBURG SCH. DISTRICT 3

Proposed Named Insured Address

3535 CLIFTON-GLENDALE RD.
SPARTANBURG, SC 29307

Applicant's Signature

(signature)

Date

06.14.23

Print Name

JAMES G. Macc

Title

Assistant Supt, Finance & Operations