CYBER INSURANCE APPLICATION

Before any question is answered please carefully read, then sign, the declaration at the end of the application. Underwriters will rely on the statements made in this application, and any insurance coverage issued based upon this application will be void if this application contains falsehoods, misrepresentations, or omissions.

Business to be Insured

1. Business Information for the company applying for coverage:

   Company Name: Greenwood School District 50

   Physical Address: 1855 Calhoun Road, Greenwood SC 29649

   Website: www.gwd50.org

   Total number of employees: 1,339

   Confirm insured's total revenues (if a school or public entity, then budget):

Revenues			
	Most Recent Fiscal Year ending 6/30 / 2023	Projected Current Fiscal Year ending 6/30 / 2024	Projected Next Fiscal Year ending 06/30 / 2025
Total Gross Revenues:	$ 84,265,000 (General Fund)	$ 90,340,000(General Fund)	$ 95,000,000 General Fund

2. Provide a brief description of insured's business activities/professional services:

K12 Public School District

3. Please list any company that is not a subsidiary of the named insured that insured wishes to have covered under this policy. Please confirm ownerships structure, relationship to the named insured, and whether or not they run on the same computer network.

N/A

4. Indicate the types and amount of confidential client, customer or employment related information the insured stores or access through the insured's network or through a hosted network (i.e. the cloud):

Social Security Numbers	☑ <100K	☐ 100K-500K	☐ 500K-1M	☐ 1M-2M	☐ 2M-5M	☐ >5M	Estimated _____
Financial Data (including PCI)	☑ <100K	☐ 100K-500K	☐ 500K-1M	☐ 1M-2M	☐ 2M-5M	☐ >5M	Estimated _____
Protected Health Information	☑ <100K	☐ 100K-500K	☐ 500K-1M	☐ 1M-2M	☐ 2M-5M	☐ >5M	Estimated _____
Other PII	☑ <100K	☐ 100K-500K	☐ 500K-1M	☐ 1M-2M	☐ 2M-5M	☐ >5M	Estimated _____

Insured's Media Content

5. Does the insured actively screen website content for possible disparagement, intellectual property infringement and invasion of privacy before publishing? ☑ Yes ☐ No

6. Does the insured company have established procedures for editing or removing potentially libelous material, controversial material and content that infringes the Intellectual Property rights of others (copyright, trademark, trade name, trade secrets etc.)? ☑ Yes ☐ No

eCrime Controls

7. When a vendor or supplier requests changes to its account details (including routing numbers, account numbers, or contract information), does the insured:

   a. Confirm all changes in by a call to a predetermined number? ☑ Yes ☐ No
   b. Send written notice to a person at the vendor/supplier other than who made the request? ☑ Yes ☐ No
   c. Require review of all change requests by a supervisor or approver? ☑ Yes ☐ No
   d. Other controls: _____

Prior Claims Experience or Incidents That May Give Rise to a Claim

8. During the past three (3) years, has the insured suffered a failure of a computer system, wrongful disclosure of private information, a wrongful transfer of money or has anyone filed a claim for invasion of or interference with any right of privacy, wrongful disclosure of personal information, or violation of any privacy related statute or regulation? ☐ Yes ☑ No

   If "Yes", detail separately and include any pending or prior incident, event or litigation providing full details of all relevant facts:

   _____

9. Is the undersigned individual aware of any circumstances that is likely to give rise to a claim under the coverage the insured is applying for? ☐ Yes ☑ No

   If so, please explain below.

   _____

Additional Notes

Please use the below space to include any additional information pertaining to the section above.

Budgets & Personnel

10. a. Annual IT Budget $ 360000

b. Percentage of IT budget spent on cybersecurity < 5 %

11. a . Full time IT employees 12

b. Full-time IT cybersecurity employees 0

12. Cybersecurity point of contact (CISO or equivalent role):

Name	Title	Email	Telephone
Zachary Lloyd	Director of Computing Servi	lloydz@gwd50.org	8649415429

13. Is network security outsourced? ☐ Yes ☑ No

a. If "Yes", please list provider: _____

Notable Controls

These controls are required by the majority of the market to provide coverage without drawbacks.[1]

14. Does the insured allow access to their corporate email through a non-corporate device or web application (Google Chrome, Safari, etc.)? ☑ Yes ☐ No

a. If "Yes", does the applicant have MFA enabled? ☑ Yes ☐ No

15. Does the insured allow access to the corporate network from a remote location? ☑ Yes ☐ No

a. If "Yes", is MFA enforced? ☑ Yes ☐ No

i. Provide MFA Provider: Google Authenticator

ii. Provide MFA type: One Time Passcode

Examples: One Time Passcode, Physical Key, Push-based Authentication, etc.

iii. Is MFA configured to ensure a compromise of a single device will only compromise that device ☑ Yes ☐ No

iv. Is MFA enforced when 3rd party service providers access the corporate network from a remote location? ☑ Yes ☐ No

16. Does the insured have MFA enforced on cloud-based applications? ☑ Yes ☐ No ☐ N/A

[1] Factors such as class of business, revenue size, and limits purchased may impact this list.

17. Does the insured use MFA to protect all local and remote access to privileged user accounts? ☑ Yes ☐ No

a. If MFA is enforced, please answer:

i. Provide MFA Provider: Google Authenticator

ii. Provide MFA type: One Time Passcode

Examples: Mobile OTP, Physical Key, Push-based Authentication, etc.

b. Including 3rd Parties, does the insured have MFA on the below:

i. All Internal & Remote Admin Access to Directory Services (active directory, LDAP,etc) ☑ Yes ☐ No

ii. All Internal & Remote Access to Network Backup Environments ☑ Yes ☐ No

iii. All Internal & Remote Access to Network Infrastructure ☑ Yes ☐ No

iv. All Internal & Remote Access to the Organization's endpoints/servers ☑ Yes ☐ No

18. Does the insured require MFA on Mission-Critical Systems? ☑ Yes ☐ No

19. Does the insured have off-line backups or backups in the cloud? ☑ Yes ☐ No

20. Does the insured offer security awareness & phishing training? ☑ Yes ☐ No

a. If "Yes", how often: Annually

b. Are phishing simulations included in training? ☑ Yes ☐ No

i. Is phishing covered as part of security awareness training? ☑ Yes ☐ No

ii. Are communications sent to employees when real-world phishing attempts occur? ☑ Yes ☐ No

iii. If formalized training is not provided, how are employees educated on security risks and organizational policies?

Please explain: _____

iv. Does the insured require additional training for employees who fail phishing email simulations? ☐ Yes ☑ No

21. Does the insured have any of the below:

Security Solution	Implemented	Vendor(s)
Endpoint Protection Platform (EPP)	Yes	Microsoft Defender for Endpoint Plan 2
Endpoint Detection and Response (EDR)	Yes	Microsoft Defender for Endpoint Plan 2
Managed Detection and Response (MDR)	Yes	Tyler Detect/Tyler MDR
Next Generation Anti-Virus (NGAV)	Yes	Microsoft Defender for Endpoint Plan 2

22. Please answer a few control questions regarding specific solutions above:

a. How is your EDR solution monitored? Microsoft Defender portal and email alerts

b. How is your NGAV solution monitored? Microsoft Defender portal and email alerts

c. If the Insured has an EDR, what percentage of endpoints is covered 100 %

If not "100%", which systems has it been deployed on, and which has it not?

Please explain: _____

d. Can users access the Insured's network with their own device (Bring Your Own Device)? ☐ Yes ☑ No

If "Yes", is EDR installed on those devices? ☐ Yes ☐ No

Notable Controls Explanation

Please use the below space to include any additional information pertaining to the section above:

Email Security

23. What security controls do you have in place for incoming email? (choose all that apply)

a. ☑ Screening for malicious attachments

b. ☑ Screening for malicious links

c. ☑ Quarantine service

d. ☑ Detonation and evaluation of attachments in a sandbox

e. ☑ Tagging external emails

f. ☑ DomainKeys Identified Mail (DKIM)

g. ☑ Sender Policy Framework (SPF) strictly enforced

h. ☑ Domain Based Message Authentication, Reporting and Conformance (DMARC)

24. Are employees trained to place extra scrutiny on attachments and links that come from external emails? ☑ Yes ☐ No

25. Does the insured utilize Web Filtering to block access to known malicious websites? ☑ Yes ☐ No

26. Does the insured have a secure email gateway? ☑ Yes ☐ No

a. If "Yes", what tool is used? Google Workspace

b. If "No", what controls are in place to filter/block spam emails, malicious senders, and malicious attachments or links in email?

Please explain: _____

27. Does the insured disable macros in their office productivity software by default? ☑ Yes ☐ No

    a. If "Yes", are users allowed to enable macros? ☐ Yes ☑ No

Email Security Explanation

Please use the below space to include any additional information pertaining to the section above:

Security Solutions

28. Does the insured have a Privileged Access Management (PAM) tool? ☐ Yes ☑ No

    a. If "Yes", are all privileged accounts managed with a PAM tool? ☐ Yes ☐ No

    b. Does the PAM Tool require checkout and password rotation for privileged credentials? ☐ Yes ☐ No

29. Does the insured use a Security Information & Event Management (SIEM) Tool? ☑ Yes ☐ No

    a. If "Yes", what is the name of the tool?: Tyler Detect/Tyler MDR

    b. If "Yes", what percent of mission critical assets feed into the SIEM?

    ☐ <25 ☐ 25- 50 ☐ 50-75 ☑ >75

30. Does the insured have a Security Operations Center (SOC)? ☑ Yes ☐ No

    a. If "Yes,"

        i. Operating Hours: ☐ Working Hours Only ☑ 24/7 ☐ Other: _____

            1. If "Working Hours Only" or "Other", are there on-call personnel during non-business hours?
               Please explain: _____

            2. If "Other," what hours is monitoring occurring? _____

        ii. How is SOC managed? Tyler Detect/Tyler MDR serves as our SOC

        iii. Does the SOC have authority and ability to remediate security events? ☑ Yes ☐ No

31. Are host-based and network firewalls configured to disallow inbound connections by default? ☑ Yes ☐ No

32. Does the insured use Remote Desktop Protocol (RDP), Virtual Network Computing (VNC), AnyDesk, TeamViewer, or other remote desktop software? ☐ Yes ☑ No

    a. If "Yes", and RDP is exposed externally, is MFA enforced? ☐ Yes ☐ No

33. Does the insured ensure employees utilize least privilege at all times and do not operate as local administrators? ☑ Yes ☐ No

    a. If "No,"

        i. What percentage of employees have local admin rights? < 0.01 %

        ii. Why do they require local admin rights? Only the IT staff have local administrator rights

        iii. Is there an exception process to review and approve local administrator rights? ☑ Yes ☐ No

34. Does the insured provide your employees with password management software? ☐ Yes ☑ No

35. Does the insured segment the corporate network based on the classification level of information stored on said systems? ☑ Yes ☐ No

    a. If "No",

        i. Is the network segmented by some other criteria? ☐ Yes ☐ No

        Please explain: _____

        ii. Does the Insured have a data classification policy in place? ☐ Yes ☐ No

        iii. Is data currently classified under sensitive, proprietary, confidential, etc. tiers, and what controls are in place to limit access? ☐ Yes ☐ No

        Please explain: _____

36. Does the insured implement PowerShell best practices as outlined in the Environment Recommendations by Microsoft? ☑ Yes ☐ No

    a. If "No", how does the organization monitor for and block potentially malicious PowerShell usage?

        Please explain:

37. Does the insured have a formal vendor management process to perform due diligence and ongoing monitoring for vendors with access to the organization's systems or data? ☑ Yes ☑ No

    a. If "No,"

        i. Is the information security team involved in the due diligence process for any new vendor that may have access to the organizations systems or data? ☐ Yes ☐ No

        Please explain: The PDF checkbox for question 37 selects both yes and no simultaneously. The answer is yes

        ii. Is there a process to perform ongoing monitoring of vendors? ☐ Yes ☐ No

        Please explain: _____

38. Does the insured accept payment cards for goods or services rendered? ☑ Yes ☐ No

    a. If "Yes", does the insured ensure point-to-point encryption of payment card data? ☑ Yes ☐ No

    b. If "Yes", data is stored: ☐ Unencrypted ☑ Tokenized or encrypted

Security Solutions Explanation

Please use the below space to include any additional information pertaining to the section above:

Legacy Systems

39. Does the insured have an asset discovery tool that continuously maps devices on their internal network? ☑ Yes ☐ No

40. Does the insured have an up-to-date asset database? ☑ Yes ☐ No

41. Does the insured have end-of-life software on their network? ☐ Yes ☑ No

    a. If "Yes",

        i. Is the software segregated from the rest of the network? ☐ Yes ☐ No

        ii. Does the insured purchase additional support for the software, if available? ☐ Yes ☐ No

        iii. Which EOL platforms are in use?

        Please explain: _____

        iv. How many servers/workstations/devices are operating on each EOL platform?

        Please explain: _____

        v. Do these machines store, process, or transmit sensitive information or support critical business function? ☐ Yes ☐ No

        Please explain:_____

        vi. What compensating controls are in use to protect these systems?

        Please explain: _____

        vii. What is the timeframe for when the company will migrate off of these platforms?

        Please explain: _____

42. Does the insured have a process to decommission unused systems? ☑ Yes ☐ No

Legacy Systems Explanation

Please use the below space to include any additional information pertaining to the section above:

Service Accounts

43. How many machine service accounts with Domain Administrator Privileges does the insured have? 2

If greater than 0, please answer the following questions:

a. Does the insured configure service accounts using the principle of least privilege? ☑ Yes ☐ No

b. Does the insured have specific monitoring rules in place for service accounts to alert their Security Operations Center (SOC) of abnormal behavior? ☑ Yes ☐ No

c. Has the insured configured service accounts to deny interactive logins? ☑ Yes ☐ No

d. Does the insured require service account passwords to be ≥25 characters or be randomly generated? ☑ Yes ☐ No

e. Does the insured rotate passwords for service accounts regularly? ☑ Yes ☐ No

f. Does the insured manage passwords for service accounts with a PAM solution or password vault? ☑ Yes ☐ No

Service Accounts Explanation

Please use the below space to explain:
1) what each account does in terms of functionality and software products it supports and 2) what hosts it authenticates to (ie solely domain controllers, servers (including DC's), but not workstations or workstations and servers (including DC's).

Both accounts are used in account provisioning and are only allowed to authenticate to one domain controller.

Vulnerabilities and Scanning

44. Does the insured use a hardened baseline configuration across all (or mostly all) of their devices? ☑ Yes ☐ No

45. What percentage of the insured's network is covered by scheduled vulnerability scans? 100 %

46. Does the insured's patching program extend to other platforms like third-party applications, web browsers, and mobile applications? ☑ Yes ☐ No

47. How often has the insured conducted penetration testing on their network?
☑ Quarterly or more frequent ☐ Bi-annually ☐ Annually ☐ Less frequent or none

Vulnerabilities and Scanning Explanation

Please use the below space to include any additional information pertaining to the section above:

Backups & Business Continuity

48. What best describes the insured's back-up solution? ☑ Local/on prem ☐ Offline ☑ Offsite ☑ Cloud
    a. If "Offsite", please describe where back-ups are stored: Local backups are stored at remote site
    b. If "Cloud", list the vendor name: Wasabi cloud storage

49. Please check all controls surrounding the insured's backups:
    a. How frequently are backups run? ☐ Continuously ☑ Daily ☐ Weekly ☐ Less frequent
    b. Encrypted ☑ Yes ☐ No
    c. MFA Enforced ☑ Yes ☐ No
    d. Separate Credentials Used ☑ Yes ☐ No
    e. Scanned for Malware ☑ Yes ☐ No
    f. Tested the successful restoration of critical data ☑ Yes ☐ No
       If yes, how often: Quarterly
    g. How long would it the insured to restore essential systems from backups in the event of a widespread ransomware attack? ☐ 0-24 hours ☑ 1-3 days ☐ 4-6 days ☐ 1 week or longer
    h. Immutable ☑ Yes ☐ No
       i. If "Yes", what is the retention period? 2 weeks
    i. Does the insured have redundant backup copies stored in 2+ locations, with one offline (offline includes cloud based backups)? ☑ Yes ☐ No

50. Does the insured have a business continuity and disaster recovery plan, that includes responding to cybersecurity threats? ☑ Yes ☐ No

    a. If "Yes,"

        i. Has the incident response team engaged in any exercises to run through the plan start to finish? ☐ Yes ☑ No

        ii. How frequently is it tested? _____

51. Does the insured have an annually tested Incident Response plan that addresses network intrusions and malware incidents? ☑ Yes ☐ No

    a. If "Yes", when was the last test? _____

52. Has the insured conducted a cybersecurity incident tabletop exercise in the last 2 years? ☐ Yes ☑ No

    a. If "Yes," did the tabletop include the threat from ransomware? ☐ Yes ☐ No

Backups & Business Continuity Explanation

Please use the below space to include any additional information pertaining to the section above:

Fraud Warning Notice

WARNING 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 CONCEALS, FOR THE PURPOSE OF MISLEADING, INFORMATON CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT INSURANCE ACT WHICH IS A CRIME AND MAY SUBJECT SUCH PERSON TO CRIMINAL AND CIVIL PENALTIES. SPECIFIC STATE FRAUD NOTICES MAY APPLY, PLEASE READ BEFORE SIGNING.

Declaration

I hereby declare that I am authorized to complete this application on behalf of the applicant and that after due inquiry, to the best of my knowledge and belief, the statements and particulars in this application are true and complete and no material facts have been misstated, suppressed, or omitted. I undertake to inform underwriters of any alteration or addition to these statements or particulars which occur before or during any contract of insurance based on the applications affected. I also acknowledge that this application (together with any other information supplied to underwriters) shall be the basis of such contract.

I understand that underwriters will rely on the statements that I make on this application. In this context, any insurance coverage that may be issued based upon this application will be void if the form contains falsehoods, misrepresentations or omissions.

Name: _____ Signature: _____

Position:* _____ Date: _____

*The signatory should be a director or senior officer of, or a partner, in the Applicant

State Specific Fraud Notices

NOTICE TO ALABAMA, ARKANSAS, ARIZONA, NEW MEXICO, RHODE ISLAND, AND WEST VIRGINIA APPLICANTS: 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 IS GUILTY OF A CRIME AND MAY BE SUBJECT TO FINES OR CONFINEMENT IN PRISON.

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 CLAIMANT WITH REGARD TO A SETTLEMENT OR AWARD PAYABLE FROM INSURANCE PROCEEDS SHALL BE REPORTED TO THE COLORADO DIVISION OF INSURANCE WITHIN THE DEPARTMENT OF REGULATORY AGENCIES.

NOTICE TO DISTRICT OF COLUMBIA APPLICANTS: WARNING: IT IS A CRIME TO PROVIDE FALSE OR MISLEADING INFORMATION TO AN INSURER FOR THE PURPOSE OF DEFRAUDING THE INSURER OR ANY OTHER PERSON. PENALTIES INCLUDE IMPRISONMENT AND/OR FINES. IN ADDITION, AN INSURER MAY DENY INSURANCE BENEFITS IF FALSE INFORMATION MATERIALLY RELATED TO A CLAIM WAS PROVIDED BY THE APPLICANT.

NOTICE TO FLORIDA APPLICANTS: 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 IN THE THIRD DEGREE.

NOTICE TO LOUISIANA AND MARYLAND APPLICANTS: ANY PERSON WHO KNOWINGLY AND WILLFULLY PRESENTS A FALSE OR FRAUDULENT CLAIM FOR PAYMENT OF A LOSS OR BENEFIT OR WHO KNOWINGLY AND 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 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 OR A DENIAL OF INSURANCE BENEFITS.

NOTICE TO OKLAHOMA APPLICANTS: WARNING: ANY PERSON WHO KNOWINGLY, AND WITH INTENT TO INJURE, DEFRAUD OR DECEIVE ANY INSURER, MAKES ANY CLAIM FOR THE PROCEEDS OF AN INSURANCE POLICY CONTAINING ANY FALSE, INCOMPLETE OR MISLEADING INFORMATION IS GUILTY OF A FELONY.

NOTICE TO NEW YORK AND KENTUCKY 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. NEW YORK APPLICANTS SHALL ALSO BE SUBJECT TO A CIVIL PENALTY NOT TO EXCEED FIVE THOUSAND DOLLARS AND THE STATED VALUE OF THE CLAIM FOR EACH SUCH VIOLATION.