GREAT AMERICAN INSURANCE GROUP

Great American Risk E-Business Cyber Loss and Liability Insurance Policy Over 25M

NOTICE: THIS APPLICATION IS FOR CLAIMS-MADE AND REPORTED COVERAGE, WHICH APPLIES ONLY TO CLAIMS FIRST MADE AND REPORTED IN WRITING DURING THE POLICY PERIOD OR ANY EXTENDED REPORTING PERIOD. THE LIMIT OF LIABILITY TO PAY DAMAGES OR SETTLEMENTS WILL BE REDUCED AND MAY BE EXHAUSTED BY DEFENSE EXPENSES AND DEFENSE EXPENSES WILL BE APPLIED AGAINST THE DEDUCTIBLE AMOUNT. THE COVERAGE AFFORDED UNDER THIS POLICY DIFFERS IN SOME RESPECTS FROM THAT AFFORDED UNDER OTHER POLICIES. READ THE ENTIRE APPLICATION CAREFULLY BEFORE SIGNING.

1. Company's Name _____
   DBA _____
   Name of CISO/IT Contact _____
   CISO/IT Contact Email Address _____
   CISO/IT Contact Phone Number _____
   Name of Third Party Provider *(insert Not Applicable if a Third Party Provider in not used)* _____
   Contact and Email of Third Party Provider _____
2. Type of Business _____
3. Street Address _____
   City _____ State _____ Zip _____
4. Primary Web Address _____
5. Year Business Started _____ Number of Employees _____

Please use the addendum portion of this application to provide any additional information necessary.

Additional Entity	Nature of Operations	Relationship to the Company with the Percentage of Common Ownership

Complete each question for the remainder of this application with ALL entities above in mind.

6. Nature of Operations _____
7. Financial Background:

Provide the Following

Gross Revenues	Prior Fiscal Year Gross Revenues	Current Fiscal Year Gross Revenues	Projected Fiscal Year Gross Revenues
US Domestic			
Foreign			
Total			

Data Security and Governance

	Yes	No
8. Estimated volume of **Protected Information** the company processes or stores _____		
How long does the company store the above **Protected Information**? _____		
Confirmation above Protected Information are not kept longer than legally required.	☐	☐

9. Which controls are in place to protect confidential, sensitive, or otherwise regulated data? *(Check all that apply)*
   ☐ Network segmentation ☐ Encryption policies *(in transit and/or at rest)* ☐ Privilege access management
   ☐ Data loss prevention software (DLP) ☐ Physical access controls

Data Security and Governance *Continued*

	Yes	No
10. Does the company maintain documented compliance programs for the applicable laws/rules/regulations below *(Check all that apply)* ☐ HIPPA ☐ GLBA ☐ BIPA ☐ GDPR ☐ CCPA ☐ PIPEDA ☐ PCI (DDS) ☐ Other _____		
11. Does the company have a privacy policy in place published on its website?	☐	☐
If yes, is it reviewed/updated at least annually by legal counsel?	☐	☐
12. Which security framework does the company align with? *(Check all that apply)* ☐ NIST ☐ ISO ☐ 27001 ☐ SOC ☐ CIS ☐ Other _____		
13. When did the company last assess alignment with the above framework(s)? _____		
14. Indicate which of the following controls the company has implemented and consistently enforces with respect to electronic funds transfer. *(Check all that apply)* ☐ Callback procedures to verify funds transfer requests or changes to banking information ☐ Dual sign-off prior to funds transfers exceeding $10,000 ☐ No Wire Transfer exceeds $10,000 ☐ Other *(Please describe)* _____		
15. How often do all staff receive employee security awareness training, including phishing? ☐ Never ☐ Quarterly ☐ Semi-Anually ☐ Anually		
16. Endpoint *(PC's, Laptops, Smartphones, Tablets, Etc.)* security controls include the following:		
Password passcode protected	☐	☐
Encryption	☐	☐
Traditional or next generation firewalls enabled/turned on	☐	☐
Traditional or next generation anti-virus products on all endpoints	☐	☐
Endpoint Detection and Response (EDR) 24/7/365 on all devices	☐	☐
If yes to EDR, who is the company's provider? _____		
Managed Detection and Response (MDR)	☐	☐
If yes to MDR, who is the company's provider? _____		
Security Information and Event	☐	☐
If yes to SIEM Management (SIEM), who is the company's provider? _____		
17. General patches are pushed within 30 days and critical patches within 14 days.	☐	☐
18. Zero-day vulnerabilities are monitored and responded to within 5 days.	☐	☐
19. Are there any end-of-life or end-of-support software in use?	☐	☐
If yes, are they segregated from the network?	☐	☐
If yes, give details on the systems, why used, with they be retired? _____		
20. Are Sender Policy Framework (SPF), Domain-based Message Authentication Reporting and Compliance (DMARC) or Domain Keys Identified Mail (DKIM) in place?	☐	☐
21. Is an email filtering tool in place to detect and/or block SPAM, malicious links and attachments?	☐	☐
22. Are emails from outside organizations tagged or otherwise marked for identifications?	☐	☐
23. Is multi factor authentication (MFA) required to access Email?	☐	☐
24. Is multi factor authentication (MFA) required for personal devices?	☐	☐
25. Is multifactor authentication (MFA) required to remotely connect to the network, all critical internet facing systems and privilege accounts?	☐	☐
26. Are firewalls configured according to the principles of least privilege?	☐	☐
27. Are firewalls rules and alerts regularly reviewed?	☐	☐

Data Security and Governance *Continued*

	Yes	No
28. When did the company last have a comprehensive network security assessment completed? *(i.e. inclusive of vulnerability scanning and penetration testing)* ☐ Last 6 months ☐ Last 18 months ☐ Last 36 months ☐ Never		
Was the network security assessment completed internally?	☐	☐
Was the network security assessment completed by a third party?	☐	☐
Name of third party _____		
29. Does the company's website use trackers, web beacons and/or pixels?	☐	☐
If yes, is the data being collected in compliance with applicable data privacy laws - specific to consent of user?	☐	☐
If yes, is the data being collected limited to the minimum information necessary to accomplish its purpose and not used or disclosed beyond what is legally permissible?	☐	☐

30. How frequently does the company backup all mission critical systems and data?
☐ Daily/Nightly ☐ Weekly ☐ Less frequently than weekly ☐ Never

Which of the following back-up solutions does the company employ? *(Check all that apply)*
☐ Local ☐ Network Drives ☐ Tapes/disks ☐ Offsite ☐ Cloud

Indicate which controls are in place to protect backups *(Check all that apply)*
☐ Encryption ☐ Disconnected from the network *(Air gapped)* ☐ Virus/Malware Scanning
☐ Credentials are stored separately ☐ Multi-Factor Authentication ☐ Immutable
☐ Other _____

31. Does the company implement any of the following response plans? *(Check all that apply)*
☐ Business Continuity Plan (BCP) ☐ Incident Response Plan (IRP) ☐ Disaster Recovery Plan (DRP)

32. How quickly can the company restore from backups? ☐ Same day ☐ 24-48 hours ☐ Longer

33. Are back-up restoration plans tested?	☐	☐

34. How frequently does the company test its ability to restore from back ups?
☐ Quarterly ☐ Semi-Annually ☐ Anually ☐ Never

35. What is the company's estimated recovery time objective (RTO) (in hours) _____

36. A formal program for evaluating the security posture of its vendors is in place and such program aligns with the company's	☐	☐

37. The company attempts to mitigate its exposure to media liability by using the following controls *(Check all that apply)*
☐ Obtaining all necessary rights to use third party content
☐ Social media policy
☐ Take-down procedures
☐ Legal review of all materials
☐ Privacy policy in place is published on the company's website and is reviewed/updated at least annually

Insurance Information

	Yes	No
38. Has the company experienced any of the following situations within the last three years?		
Privacy Incident and/or **claims**?	☐	☐
Network Incident and/or **claims**?	☐	☐
System Failure Incident and/or **claims**?	☐	☐
Cyber Crime Incident and/or **claims**?	☐	☐
Media Incident and/or **claims**?	☐	☐

If yes to any of the above, please provide detail in a separate attachment a description of the incident including relevant dates, the number and type of records involved, the total dollar amount of expenses in connection with the incident, a summary of the company's response to the incident, and subsequent changes made to prevent the likelihood of future events.

39. Does the company presently purchase Cyber Risk Insurance?	☐	☐

Insurance Information *Continued*

	Yes	No
40. Is the company aware of any fact, circumstance, or situation involving the company that it has a reason to believe will cause a **Privacy Incident**, **Network Security Incident**, **System Failure Incident**, **Cyber Crime Incident**, **Media Incident** or **Claim**? *(NOTE: Current Great American policyholders need not respond to this Question)*	☐	☐

It is understood and agreed that if the company responded yes to the question above, there is no coverage for any **Privacy Incident**, **Network Security Incident**, **System Failure Incident**, **Cyber Crime Incident**, **Media Incident** or **Claim** based upon, arising out of, or in any way involving any such fact or circumstance.

Application Addendum

Please use this section to supplement the information provided above regarding the company's Information Security program:

Fraud Warnings

Alabama, Arkansas, Louisiana, New Mexico, Rhode Island, and West Virginia: 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 and/or confinement in prison. In Alabama, a person may also be subject to restitution.

Colorado, Maine, Tennessee, Virginia, Washington: 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 a denial of insurance benefits. In Colorado, penalties may also include civil damages. In Colorado, 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 policy- holder 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.

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 payment of a loss is guilty of a crime and may be subject to fines and confinement in state prison.

District of Columbia: 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.

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: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance 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.

Maryland: 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.

New Jersey: Any person who includes any false or misleading information on an application for an insurance policy is subject to criminal and civil penalties.

New York: 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 five thousand dollars and the stated value of the claim for each such violation.

Ohio: Any person who, with intent to defraud or knowing that he is facilitating a fraud against an insurer, submits an application or files a claim containing a false or deceptive statement is guilty of insurance fraud.

Oklahoma: 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.

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.

Applicable in other states: Your policy may be void in any case of fraud, intentional concealment or misrepresentation of material fact by you in securing this insurance.

Representations and Signatures

The undersigned declares that to the best of his or her knowledge the statements set forth herein are true and correct and that reasonable efforts have been made to obtain sufficient information from each and every person and entity proposed for this insurance to facilitate the proper and accurate completion of this application. The undersigned further agrees that if any significant adverse change in the condition of the applicant is discovered between the date of this application and the effective date of the Policy, which would render this application inaccurate or incomplete, notice of such change will be reported in writing to the Insurer immediately. The signing of this application does not bind the undersigned to purchase the insurance.

It is agreed by the Named Insured and the Insured that the particulars and statements contained in this application and any information provided herewith *(which shall be on file with the Insurer and be deemed attached hereto as if physically attached hereto)* are the basis of this Policy and are to be considered as incorporated in and constituting a part of this Policy. It is further agreed that the statements in this application or any information provided herewith are their representations, they are material, and any Policy issued is in reliance upon the truth of such representations.

Applicant Signature _____ **Title** _____ **Date** _____

Printed Name _____

Agent Name _____ **Agent Signature** _____

NOTE: This Application, including any material submitted herewith will be treated in strictest confidence.

Great American Insurance Group Cyber Risk Division

Cincinnati, OH
301 E. 4th Street
Cincinnati, OH 45202

Visit our website for more information.