GREAT AMERICAN INSURANCE GROUP

Great American Spirit Insurance Company Risk E-Business Cyber Loss And Liability Insurance Policy℠

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. Name _____

   DBA _____

   Name of Person Completing Application _____

   Email Address _____

2. Type of Business *(select one)*:

   ☐ Private Corporation ☐ Public Company ☐ LLC

   ☐ Partnership ☐ Non-Profit ☐ Investment Fund

3. Principal Address _____

   City _____ State _____ Zip _____

   Primary Web Address _____

4. Please provide name, nature of operations, and relationship to the Company of all additional entities to be covered. Or, enter "none".

Additional Entity	Nature of Operations	Relationship to Company

Please complete each question for the remainder of this application with ALL entities above in mind *(herein after "the Company".)*

Background and Financial Information

5. Nature of business _____

6. Year Business Started _____

7. Total Number of Employees *(please include all full, part, time seasonal, leased, etc.)* _____

8. Please provide the following financial information:

Total Assets as of Most Recent Fiscal Year End	Total Gross Revenues Last Fiscal Year	Anticipated Revenues This Fiscal Year	Anticipated Revenues Next Fiscal Year
$	$	$	$

9. Percentage of Annual Revenues Estimated to be attributable to E-Commerce/Online Sales _____%

Insurance Information

	Yes	No
10. Has the Company experienced any of the following situations within the last three years?		
Privacy Incident and/or claims?	☐	☐
Media Incident and/or claims?	☐	☐
Cyber Crime Incident?	☐	☐
Network 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.

	Yes	No
11. Do you presently purchase Cyber Risk Insurance?	☐	☐

If yes, please complete the following table.

Limits	Deductible	Continuity Date

	Yes	No
12. Do you presently purchase Technology Errors and Omissions Insurance?	☐	☐

If yes, please provide the following:

Insurer	Limit	Deductible	Have you had any claims?	
	$	$	☐	☐

	Yes	No
13. Are you aware of any fact, circumstance, or situation involving the Company that you have reason to believe will cause a Privacy Incident, Network Security Incident, Media Incident, Cyber Crime Incident, or Claim? *(NOTE: Current Great American policyholders need not respond to this question)*	☐	☐

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

Social Engineering

14. Indicate which of the following controls you have implemented with respect to electronic funds transfers:

☐ Callback procedures to verify funds transfer requests or changes to banking information

☐ Dual authorization for funds transfers greater than $2,500

☐ Other *(please describe)*_____

Personal Device Usage

15. What percent of your employees handle Company business from their personal devices *(select one)*?

☐ We prohibit it ☐ I don't know ☐ Less than 25%

☐ 25 – 75% ☐ More than 75%

Personally Identifiable Information (PII) Security

16. a. Please estimate the annual volume of each type of information you process or store, taking into account both electronic and paper files as well as employee and customer information:

- ☐ SSN, individual taxpayer ID, driver's license, passport or federal ID numbers _____
- ☐ Payment card data *(credit or debit cards)* _____
- ☐ Protected health information _____
- ☐ Other confidential or protected information _____

b. How long do you store the above records? _____

	Yes	No
c. Do you have a record retention/destruction policy in place?	☐	☐

d. Which controls are in place to protect PII in the Company's care, custody and control?

- ☐ Physical controls on access to computer systems and sensitive documents.
- ☐ Network segmentation of sensitive data
- ☐ Encryption policies
- ☐ Privilege management
- ☐ Annual employee security awareness training

End Point Security

17. Please indicate below the endpoint *(PC's, laptops, Smartphones, tablets, etc.)* security controls your Company is using:

- ☐ Password/passcode protected
- ☐ Encryption
- ☐ Firewalls enabled/turned on
- ☐ Traditional antivirus products on all endpoints
- ☐ Next generation antivirus on all endpoints

18. Who is primarily responsible for patching end points?

☐ A managed services provider ☐ The Company's IT department ☐ The user/employee

Email Security

	I Don't Know	Yes	No
19. Do you use Sender Policy Framework (SPF)?	☐	☐	☐
20. How often is phishing training conducted to all staff: ☐ Never ☐ I don't know ☐ Semiannually ☐ Annually			
21. Do you use an email filtering tool to detect and/or block SPAM, malicious links, and attachments?	☐	☐	☐
22. Do you require multifactor authentication (MFA) to access email?	☐	☐	☐

Network Security

	Yes	No
23. Is your network WiFi enabled?	☐	☐

If yes, please indicate level of WPA protocol: ☐ WPA ☐ WPA2 ☐ WPA3 ☐ I don't know

24. Who monitors the Company's networks for intrusions or other unusual activity *(select one)*?

- ☐ Nobody/we do not monitor
- ☐ Somebody in the Company's IT department
- ☐ A third party/managed security provider
- ☐ Somebody in the Company's IT department AND a third party/managed security provider

Network Security *Continued*

	I Don't Know	Yes	No
25. Are your firewalls configured according to the principles of least privileges?		☐	☐
26. Do you regularly review firewall rules and alerts?	☐	☐	☐
27. Is multi-factor authentication required to remotely connect to the network?	☐	☐	☐

28. When did the Company last have a comprehensive *(i.e. inclusive of vulnerability scanning and penetration testing)* network security assessment conducted by a third party *(select one)*?

☐ Last 6 months ☐ Last 18 months ☐ Last 36 months ☐ Never

	Yes	No
29. Does the Company maintain a formal program for evaluating the security posture of its vendors?	☐	☐

Back-Up Security

	Yes	No
30. Do you back up all mission critical systems and data?	☐	☐

If yes, please provide the following:

How Frequently do you back up? ☐ Daily/nightly ☐ Weekly ☐ Less frequently then weekly

Which of the following back-up solutions do you employ?

☐ Local ☐ Network drives ☐ Tapes/disks ☐ Off-site ☐ Cloud

Which of the above are encrypted?

☐ Local ☐ Network drives ☐ Tapes/disks ☐ Off-site ☐ Cloud

How quickly can you restore from back-ups? ☐ Same day ☐ 24-48 hours ☐ Longer

How frequently do you test your ability to restore from back ups?

☐ Never ☐ Quarterly ☐ Semi-annually ☐ Annually

Web Hosting

	Yes	No
31. Do you outsource your web hosting?	☐	☐

Compliance

32. Are you compliant with the Payment Card Industry Data Security Standard (PCI-DSS) *(select one)*?

☐ Yes ☐ No

☐ I don't know ☐ We do not process ANY payment card transactions

	I Don't Know	Yes	No
33. Does the Company maintain documented compliance programs for applicable laws/ rules/regulations such as HIPAA, GLBA, GDPR, etc?	☐	☐	☐

Media Content

34. The Company's attempts to mitigate its exposure to media liability by using the following controls *(select all that apply)*:

☐ Obtaining all necessary rights to use third party content

☐ Social media policy

☐ Take-down procedures

☐ Legal review of all materials

Fraud Warnings

Alabama, Arkansas, District of Columbia, Louisiana, Maryland, New Mexico, Rhode Island, West Virginia: Any person who knowingly *(or willfully)** presents a false or fraudulent claim for payment of a loss or benefit or 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.
**Applies in MD Only.*

Colorado: 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.

Florida and Oklahoma: 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)**.
**Applies in FL Only.*

Kansas: 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, electronic, electronic impulse, facsimile, magnetic, oral, or telephonic communication or 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 commits fraud.

Kentucky, New York, Ohio, 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 *(not to exceed five thousand dollars and the stated value of the claim for each such violation)**. **Applies in NY Only.*

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 denial of insurance benefits. **Applies in ME Only.*

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.

Oregon: Any person who knowingly and with intent to defraud or solicit another to defraud the insurer by submitting an application containing a false statement as to any material fact may be violating state law.

Puerto Rico: Any person who knowingly and with the intention of defrauding 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, shall incur a felony and, upon conviction, shall be sanctioned for each violation by a fine of not less than five thousand dollars ($5,000) and not more than ten thousand dollars ($10,000), or a fixed term of imprisonment for three (3) years, or both penalties. Should aggravating circumstances [be] present, the penalty thus established may be increased to a maximum of five (5) years, if extenuating circumstances are present, it may be reduced to a minimum of two (2) years.

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 Company and the Insured Persons 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

Windsor, CT
5 Waterside Crossing
3rd Floor
Windsor, CT 06095

Chicago, IL
1450 American Lane
8th Floor
Schaumburg, IL 60173

New York, NY
One Penn Plaza
Suite 2100
New York, NY 10119