ABA Insurance Services

EVEREST NATIONAL INSURANCE COMPANY

CYBER COVER APPLICATION

FDIC No. _____

THE LIABILITY POLICY WHICH MAY BE ISSUED BASED UPON THIS APPLICATION PROVIDES CLAIMS MADE COVERAGE WRITTEN ON A NO DUTY TO DEFEND BASIS. DEFENSE COSTS ARE INCLUDED WITHIN THE LIMIT OF LIABILITY. AMOUNTS INCURRED AS DEFENSE COSTS WILL REDUCE THE LIMIT OF LIABILITY AVAILABLE TO PAY JUDGMENTS OR SETTLEMENTS. PLEASE READ YOUR POLICY CAREFULLY.

Applicant _____

_____

(List all entities applying for coverage including all Subsidiaries)

Address _____ City _____ State _____ Zip Code _____

P.O. Box _____ City _____ State _____ Zip Code _____

Telephone _____ Fax _____ Website _____

Representative authorized to receive notices on behalf of all persons and entities:

Name _____ Title _____ E-mail _____

GENERAL INFORMATION

1. Provide the websites addresses proposed for coverage:

_____

_____

_____

2a. List any Third Party Service Providers used for the following services, if applicable:

- Managed Security Services
- Application Service Provider
- Disaster Recovery
- Information security risk assessments
- Data destruction
- Internet Service Provider
- Website hosting
- Vulnerability assessment and penetration testing
- Data archiving and restoration
- Credit card processing

_____

_____

_____

_____

2b. If applicable, do all vendor contracts:

i. indemnify/hold the Applicant harmless for vendor misconduct, errors, omissions or negligence? ❑ Yes ❑ No

ii. outline the vendor's responsibility for safeguarding customer and confidential information and stipulate what security measures are provided by the vendor? ❑ Yes ❑ No

3. **SECURITY AND PRIVACY MEASURES:**

a. Does the bank have a Chief Information Security Officer? ❑ Yes ❑ No

b. Are the systems backed up on a daily basis? ❑ Yes ❑ No

c. Are system backup and recovery procedures documented and tested for all critical systems? ❑ Yes ❑ No

d. Are firewall and router technology utilized? ❑ Yes ❑ No

e. Are intrusion detection or prevention systems employed? ❑ Yes ❑ No

f. Is antivirus software used? ❑ Yes ❑ No

g. Are computer applications, software and operating systems kept current with the latest updates and patches? ❑ Yes ❑ No

h. Are internet browsers and plug-ins kept updated and patched? ❑ Yes ❑ No

i. Are passwords utilized to authenticate users for Company networks (including wireless networks)? ❑ Yes ❑ No

j. If yes, what is the required number of characters for passwords? _____

k. Is all confidential information which is transmitted to/from, or stored within your networks (including wireless networks) encrypted? ❑ Yes ❑ No

l. Are wireless transmissions protected using WPA/WPA2, IPSEC, or SSL? ❑ Yes ❑ No

m. Are computer systems, applications and servers that collect confidential information segregated from the rest of the network? ❑ Yes ❑ No

n. Are all System Administrative accounts limited to only absolutely essential personnel? ❑ Yes ❑ No

o. Has an independent network security assessment or audit been conducted within the past 12 months? ❑ Yes ❑ No

p. If yes, have all vulnerabilities identified in the audit been remediated? ❑ Yes ❑ No

q. Does the bank maintain:

i. a written information security policy? ❑ Yes ❑ No
ii. a written privacy policy? ❑ Yes ❑ No
iii. a written data breach response plan? ❑ Yes ❑ No
iv. a network security incident response plan? ❑ Yes ❑ No
v. a written disaster recovery/business continuity policy? ❑ Yes ❑ No
vi. a written records retention and destruction policy? ❑ Yes ❑ No
vii. a security policy designed to prohibit and track unauthorized access to your network, computer systems and data centers? ❑ Yes ❑ No

r. Is a formal process in place to ensure that network privileges and physical access to the building are revoked in a timely manner following an employee's termination or resignation? ❑ Yes ❑ No

s. Is the bank currently compliant with the following regulations?

i. Gramm-Leach Bliley Act of 1999 ❑ Yes ❑ No
ii. Identity Theft Red Flags under the Fair and Accurate Credit Transactions Act of 2003 ❑ Yes ❑ No
iii. Payment Card Industry (PCI) Data Security Safeguard ❑ Yes ❑ No

t. Are all systems and devices used for Company purposes configured according to industry accepted system hardening standards? ❑ Yes ❑ No

4. FUNDS TRANSFERS:

a. Does the bank have written agreements in place with all customers who request wire transfers via:

i. voice (phone) ❑ Yes ❑ No
ii. telefacsimile device (fax) ❑ Yes ❑ No
iii. email ❑ Yes ❑ No
iv. online ❑ Yes ❑ No

b. If yes, does the agreement specify the names of persons authorized to initiate such transfers? ❑ Yes ❑ No

c. Has the Bank established an instruction verification mechanism to be used with these authorized individuals? ❑ Yes ❑ No

d. If "No" to any of the questions above, please provide an explanation:

_____

_____

e. Please complete the table below regarding call-back or other authentication procedures

Does the bank require an authentication procedure for the following transfers?	**PERSONAL ACCOUNTS** If yes, indicate the dollar amount above which a call-back is required?	**CORPORATE ACCOUNTS** If yes, indicate the dollar amount above which a call-back is required?
Voice (phone) initiated transfers	❑ Yes $ ❑ No ❑ N/A	❑ Yes $ ❑ No ❑ N/A
Telefacsimile device (fax) initiated transfers	❑ Yes $ ❑ No ❑ N/A	❑ Yes $ ❑ No ❑ N/A
E-mail initiated transfers	❑ Yes $ ❑ No ❑ N/A	❑ Yes $ ❑ No ❑ N/A

f. If "No" or "N/A" to any of the questions above, please provide an explanation:

_____

_____

g. Does the bank allow customers to initiate wire transfers online? ❑ Yes ❑ No

h. If yes, which authentication controls are in place to monitor funds transfer requests initiated online?

Description	**Answer**
User ID and password	❑ Yes ❑ No
Device authentication using a cookie	❑ Yes ❑ No
Risk profiling using an algorithm that assigns a risk score to each login and transaction based on factors such as location, IP address and size, type and frequency of orders	❑ Yes ❑ No
Challenge questions	❑ Yes ❑ No
Dollar amount of the order that triggers challenge questions	❑ Yes ❑ No
Blacklisting of IP addresses associated with known instances of fraud	❑ Yes ❑ No
Out-of-bank authentication or tokens	❑ Yes ❑ No
Additional Control - Please describe:	

i. Does the bank allow international wire transfers? ❑ Yes ❑ No

j. If yes, are there any additional controls or reviews prior to the execution of the transfer? ❑ Yes ❑ No

k. If yes, please describe the additional controls or methods used to verify the authenticity of such requests:

_____

_____

l. If repetitive customer initiated funds transfers are established, do procedures for changes or deviations require supervisor approval and appropriate confirmation? ❑ Yes ❑ No

m. Are wire transfer verifications sent to customers daily? ❑ Yes ❑ No

n. If no, how often are verifications sent?

_____

o. Does the bank require senior officer approval for wire transfer requests over a specified dollar amount? ❑ Yes ❑ No

p. If "Yes", indicate dollar amount: $_____

5. CYBER PUBLISHING:

a. Do you maintain policies or procedures to screen all forms of content (website and social media) for potential infringement of third party intellectual property rights? ❑ Yes ❑ No

b. Are policies or procedures maintained to screen all forms of content (website and social media) for elements that may lead to personal injury claims including but not limited to libel, slander and defamation? ❑ Yes ❑ No

c. Are written policies or procedures in place to audit the use of software licenses? ❑ Yes ❑ No

6. Which insurance carrier currently provides Property and General Liability coverage? _____

a. What are the policy expiration dates? _____

LOSSES, PENDING LITIGATION AND CLAIMS HISTORY

New Applicants Only

1. During the past 3 years, has the Applicant:
   a. been made aware of any unauthorized access to information of the Applicant or its customers through the Applicant's computer system, Website, Internet Service Provider or Website host; or ❑ Yes ❑ No
   b. sustained a systems intrusion, tampering, hacking or similar incident that resulted in:
      1) damage to or destruction of data or computer programs;
      2) damages to a third party; or
      3) other loss to the institution? ❑ Yes ❑ No
2. Does the undersigned or any director or officer have knowledge of any fact, circumstance or situation involving the Applicant, its Subsidiaries or any past or present director, officer or employee, which could reasonably be expected to give rise to a future claim? ❑ Yes ❑ No
3. Has any insurance carrier declined, refused to renew or cancelled insurance similar to the coverage herein applied for? (**Not applicable in Missouri**) ❑ Yes ❑ No

If any of the answers in this section are Yes, provide details by attachment.

RENEWAL APPLICANTS: IT IS UNDERSTOOD AND AGREED THAT IF THE UNDERSIGNED OR ANY INSURED HAS KNOWLEDGE OF ANY FACT, CIRCUMSTANCE OR SITUATION WHICH COULD REASONABLY BE EXPECTED TO GIVE RISE TO A FUTURE CLAIM, THEN ANY INCREASED LIMIT OF LIABILITY OR COVERAGE ENHANCEMENT SHALL NOT APPLY TO ANY CLAIM ARISING FROM OR IN ANY WAY INVOLVING SUCH FACTS, CIRCUMSTANCES OR SITUATIONS. IN ADDITION, ANY INCREASED LIMIT OF LIABILITY OR COVERAGE ENHANCEMENT SHALL NOT APPLY TO ANY CLAIM, FACTS, CIRCUMSTANCES OR SITUATIONS FOR WHICH THE INSURER HAS ALREADY RECEIVED NOTICE.

NEW APPLICANTS: IT IS UNDERSTOOD AND AGREED THAT ANY CLAIM ARISING FROM ANY PRIOR OR PENDING LITIGATION OR WRITTEN OR ORAL DEMAND SHALL BE EXCLUDED FROM COVERAGE. IT IS FURTHER UNDERSTOOD AND AGREED THAT IF KNOWLEDGE OF ANY FACT, CIRCUMSTANCE OR SITUATION WHICH COULD REASONABLY BE EXPECTED TO GIVE RISE TO A CLAIM EXISTS, ANY CLAIM OR ACTION SUBSEQUENTLY ARISING THEREFROM SHALL BE EXCLUDED FROM COVERAGE.

REPRESENTATION STATEMENT

The undersigned declare that, to the best of their knowledge and belief, the statements in this application, any prior applications, any additional material submitted, and any publicly available information published or filed by or with a recognized source, agency or institution regarding business information for the Applicant for the 3 years preceding the Policy's inception, and any amendments thereto [hereinafter called "Application"] are true, accurate and complete, and that reasonable efforts have been made to obtain sufficient information from each and every individual or entity proposed for this insurance. It is further agreed by the Applicant that the statements in this Application are their representations, they are material and that the Policy is issued in reliance upon the truth of such representations.

The signing of this Application does not bind the undersigned to purchase the insurance and accepting this Application does not bind the Insurer to complete the insurance or to issue any particular Policy. If a Policy is issued, it is understood and agreed that the Insurer relied upon this Application in issuing each such Policy and any Endorsements thereto. The undersigned further

agrees that if the statements in this Application change before the effective date of any proposed Policy, which would render this Application inaccurate or incomplete, notice of such change will be reported in writing to the Insurer immediately.

FRAUD WARNINGS

ARKANSAS, LOUISIANA, MARYLAND, NEW JERSEY, NEW MEXICO and **VIRGINIA:** 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. In Arkansas, Louisiana and Maryland, that person may be subject to fines, imprisonment or both. In New Mexico, that person may be subject to civil fines and criminal penalties. In Virginia, penalties may include imprisonment, fines and denial of insurance benefits.

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.

DISTRICT OF COLUMBIA, KENTUCKY, PENNSYLVANIA and **OREGON:** 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 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. In District of Columbia, penalties include imprisonment and/or fines. In addition, the Insurer may deny insurance benefits if the applicant provides false information materially related to a claim. In Pennsylvania and Oregon, the person may also be subject to criminal and civil penalties.

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

MAINE, **TENNESSEE** and **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 denial of insurance benefits.

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

OREGON: Any person who knowingly and with intent to defraud any insurance company or another 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, may be committing a fraudulent insurance act, which may be a crime and may subject the person to criminal and civil penalties.

Chief Executive Officer, President or Chairman of the Board:

Print Name:	Signature:
Title:	Date:

Information Technology Officer or comparable title:

Print Name:	Signature:
Title:	Date:

A POLICY CANNOT BE ISSUED UNLESS THE APPLICATION IS SIGNED/DATED BY TWO INDIVIDUALS.

Agent Name _____ License Number _____

Agent Signature _____

Submit Application to:
ABA Insurance Services Inc.
3401 Tuttle Road, Suite 300 • Shaker Heights, OH 44122
Telephone: (800) 274-5222 • Fax: (800) 456-6590 • www.abais.com

ABA Insurance Services Inc., dba Cabins Insurance Services in CA; ABA Insurance Services of Kentucky Inc. in KY; and ABA Insurance Agency Inc. in MI

