National Casualty Company

Home Office:
Scottsdale, Arizona
Administrative Office:
8877 North Gainey Center Drive • Scottsdale, Arizona 85258
1-800-423-7675 • Fax (480) 483-6752

APPLICATION FOR ENTERPRISE CYBER INSURANCE POLICY

THIS POLICY APPLIES ONLY TO CLAIMS FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD OR DISCOVERY PERIOD. THE LIMIT OF LIABILITY AVAILABLE TO PAY JUDGMENTS OR SETTLEMENTS SHALL BE REDUCED BY PAYMENT OF DEFENSE COSTS. DEFENSE COSTS ARE SUBJECT TO THE APPLICABLE RETENTION. PLEASE READ AND REVIEW THE POLICY CAREFULLY. Fully answer all questions and submit all requested information. Terms appearing in bold in this **Application** are defined in the Policy and have the same meaning in this **Application** as in the Policy. The **Company** will hold this **Application,** including all materials submitted herewith, in confidence.

SECTION I. **GENERAL INFORMATION**

1. Name of applicant: _____
   Mailing Address: _____
   City: _____ State: _____ ZIP: _____
   Risk Manager or functional equivalent: _____
   Phone: _____ E-mail: _____

SECTION II. **REVENUE INFORMATION** (see publicly filed annual report ☐)

	Most Recent Twelve (12) Months	**Prior Year**
US Revenue	$	$
Non-US Revenue	$	$
Total	$	$

SECTION III. **DATA CLASSIFICATION**

1. Please indicate the approximate number of records containing personally identifiable information the applicant handles, processes, stores, destroys or maintains:

Type	**Number of Individually Identifiable Records**
Government Issued IDs including: SSN, Driver's License Number	
Medical/Health Information	
Financial Account Information	

2. Please indicate if data is encrypted in the following environments:

Type	**At-Rest**	**Mobile Devices**	**Storage Media**	**External Communications**
Government Issued IDs including: SSN, State Issued ID Cards, Driver's License Numbers, Passport Numbers	☐	☐	☐	☐
Medical/Health Information	☐	☐	☐	☐
Financial Account Information	☐	☐	☐	☐

SECTION IV. **NETWORK SECURITY CONTROLS**

1. Please describe which services are outsourced (if any):

IT Security	☐ Yes ☐ No	Data Hosting	☐ Yes ☐ No
IT Infrastructure	☐ Yes ☐ No	Data Back-up	☐ Yes ☐ No
Data Disposal	☐ Yes ☐ No	Data Storage	☐ Yes ☐ No

2. Does the applicant employ a Chief Security Officer, Chief Information Security Officer or equivalent position dedicated to Information Security? ☐ Yes ☐ No
3. Does the applicant segment their network to separate systems containing sensitive non-public information from those containing non-sensitive information? ☐ Yes ☐ No
4. Does the applicant utilize firewalls or a DMZ to segment web servers from networks containing sensitive non-public information? ☐ Yes ☐ No
5. Does the applicant enforce a software update process including installation of critical software patches within two to five business days? ☐ Yes ☐ No
6. Does the applicant perform internal audits on security controls on at least an annual basis? ☐ Yes ☐ No
7. Does the applicant utilize a VPN or similar secure connection technology for remote user access? ☐ Yes ☐ No
8. Does the applicant utilize an Intrusion Detection System (IDS) or Intrusion Detection and Prevention System (IDPS)? ☐ Yes ☐ No
9. Has the applicant conducted a network vulnerability assessment within the past twelve (12) months? ☐ Yes ☐ No
   If no, when was the last assessment? _____
10. Does the applicant conduct an annual network penetration test? ☐ Yes ☐ No

SECTION V. **GOVERNANCE, RISK AND COMPLIANCE**

1. Does the applicant have a security policy which describes protection of physical and IT assets, acceptable use of those assets and enforcement for non-compliance? ☐ Yes ☐ No
2. Are the applicant's security policies reviewed and updated (if necessary) on an annual basis? ☐ Yes ☐ No
3. Are all employees and contractors with access to the applicant's network required to review and accept the terms of all security policies on at least an annual basis? ☐ Yes ☐ No
4. Is the applicant's privacy policy reviewed and updated (if necessary) on an annual basis? ☐ Yes ☐ No
5. Does the applicant terminate all network access as a part of their regular exit process when an employee leaves the company? ☐ Yes ☐ No
   Please indicate timeframe: ☐ Within 24 hours ☐ 24-48 hours ☐ 3-5 days ☐ Greater than 5 days
6. Has the applicant named an Incident Response Team (IRT) to serve as the centralized point of coordination in the event of a data breach, network security incident or business continuity incident? ☐ Yes ☐ No
7. Does the applicant have a formal, documented and tested Incident Response Plan (IRP)? ☐ Yes ☐ No
8. If yes to Question 7., is that plan tested on an annual basis? ☐ Yes ☐ No
9. Does the applicant conduct mandatory training for all employees on the following:
   ☐ Password management ☐ Acceptable Network Use ☐ Phishing and Social Engineering Risk
   ☐ Mobile Device Security ☐ Physical Security
10. Does the applicant require all vendors which process, store or maintain confidential Third Party Data on their behalf to demonstrate adequate network security controls? ☐ Yes ☐ No

11. Does the applicant have documented procedures to ensure compliance with all applicable federal and state privacy laws pertaining to the applicant's industry, including HIPAA, HITECH, GLBA or the CA Online Privacy Prevention Act of 2003? ☐ Yes ☐ No

12. Are vendors with access to the applicant's network contractually obligated to indemnify the applicant for harm arising from a breach of the vendor's security? ☐ Yes ☐ No

13. Does the applicant store, process, maintain or destroy Third Party Corporate Confidential Information which is subject to a Non-Disclosure Agreement or any other contractual obligation to protect the confidentiality of such data? ☐ Yes ☐ No

14. In the past three years, has the applicant been subject to any formal civil, regulatory or administrative proceeding or litigation related to data privacy? ☐ Yes ☐ No

SECTION VI. **PAYMENT CARD CONTROLS** (answer only if applicant processes over 100,000 unique payment card transactions annually.)

1. Is the applicant PCI compliant? ☐ Yes ☐ No
   Please indicate level of compliance: _____
2. Please indicate the date of the applicant's latest PCI Report on Compliance (ROC): _____
3. Approximately how many unique payment card transactions does the applicant process annually? _____
4. Does the applicant segment the POS network from the remainder of the enterprise's network? ☐ Yes ☐ No
5. Are POS access credentials changed on a regular basis? ☐ Yes ☐ No
6. Are POS terminals restricted to internal POS related activities only, with no access to the Internet? ☐ Yes ☐ No
7. Is remote user access to the POS system permitted? ☐ Yes ☐ No
8. If yes to Question 7., is access permitted through a VPN connection only? ☐ Yes ☐ No

SECTION VII. **MEDIA CONTROLS**

1. Does the applicant review materials for the following prior to dissemination, distribution or publication:
   ☐ Copyright Infringement ☐ Libel or Slander ☐ Trademark Infringement ☐ Violations of Rights of Publicity
2. Does the applicant have an active take down policy for materials which could be considered libelous, slanderous or infringing upon the intellectual property rights of a third party? ☐ Yes ☐ No
3. Does the applicant comply with the safe harbor provisions of the Digital Millennium Copyright Act (DMCA) or equivalent? ☐ Yes ☐ No
4. Does the applicant's website(s) allow posting of third party content? ☐ Yes ☐ No
5. If yes to Question 4., when is the content reviewed?
   ☐ Prior to publication ☐ Within twenty-four (24) hours of publication ☐ Never
6. Does the applicant require third party content providers to warrant that their work does not violate another party's intellectual property? ☐ Yes ☐ No
7. Does the applicant require third party content providers to indemnify the applicant when an intellectual property Claim is made against the applicant based on content provided? ☐ Yes ☐ No
8. Within the last three years, has the applicant ever received a complaint or cease and desist order alleging trademark or copyright infringement, invasion or privacy, violation of rights of publicity or defamation with regard to any content displayed or published in the applicant's media or on behalf of the applicant? ☐ Yes ☐ No

SECTION VIII. **BUSINESS CONTINUITY**

1. Does the applicant have an active Business Continuity Plan (BCP) which specifically addresses a network outage (either partial or a total cessation)? ☐ Yes ☐ No
2. Is the applicant's BCP plan tested annually? ☐ Yes ☐ No
3. Approximately how much revenue does the applicant generate hourly? $_____
4. Within the last three years, has the applicant experienced any unplanned outages which affected part of or the entire network? ☐ Yes ☐ No
   If yes, what was the duration of the outage (in hours)? _____
5. Does the applicant regularly back-up all sensitive and/or mission critical data to a secure off-site location? ☐ Yes ☐ No

SECTION IX. **PRIOR LOSS EXPERIENCE**

1. Is the applicant aware of any circumstances that may give rise to a claim or notice under this policy? ☐ Yes ☐ No
   If yes, please describe: _____
2. During the last three years, has the applicant ever been the subject of a regulatory or administrative proceeding related to data privacy? ☐ Yes ☐ No
3. In the past three years, has the applicant sustained a breach of their network security resulting in the loss, theft, tampering or destruction of sensitive data? ☐ Yes ☐ No
   If yes, please describe: _____

AS TO QUESTIONS 1., 2. AND 3. ABOVE, IT IS UNDERSTOOD AND AGREED THAT IF THE UNDERSIGNED OR ANY INSURED PROPOSED FOR THIS INSURANCE HAS KNOWLEDGE OF ANY SUCH CLAIM, LITIGATION, FACT, CIRCUMSTANCE OR ACT, THEN ANY SUCH CLAIM OR LITIGATION AND ANY CLAIM THAT MIGHT ARISE FROM ANY SUCH CLAIM, LITIGATION, FACT, CIRCUMSTANCE OR ACT IS EXCLUDED FROM COVERAGE UNDER THE PROPOSED INSURANCE.

The persons signing this **Application** declare that to the best of their knowledge the statements set forth herein and the information in the materials submitted herewith are true and correct and that reasonable efforts have been made to obtain sufficient information from all proposed **Insureds** to facilitate the proper and accurate completion of this **Application** for the proposed policy. Signing this **Application** does not bind the undersigned to purchase the insurance, but this **Application** shall be the basis of the contract should a policy be issued.

It is agreed by all concerned that the particulars and statements contained in this **Application** are true and shall be deemed material to the decision of the **Company** to issue the insurance. The undersigned agree that if after the date of this **Application** and prior to the effective date of any policy based on this **Application,** any occurrence, event or other circumstance should render any of the information contained in this **Application** inaccurate or incomplete, then the undersigned shall notify the **Company** of such occurrence, event or circumstance and shall provide the **Company** with information that would compete, update or correct such information. In such event, the **Company** in its sole discretion may modify or withdraw any outstanding quotation. The **Company** shall maintain on file this **Application,** including material submitted therewith, which shall be considered to be physically attached to and part of the Policy, if issued. The information requested in this **Application** is for underwriting purposed only and does not constitute notice to the **Company** under any policy of a **Claim** or potential claim. All such notices must be submitted to the **Company** pursuant to the terms of the Policy, if and when issued.

FRAUD WARNING: 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 applicable in AL, CO, DC, FL, KS, LA, ME, MD, MN, NE, NY, OH, OK, OR, RI, TN, VA, VT or WA.)

NOTICE TO ALABAMA 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 restitution fines or confinement in prison, or any combination thereof.

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 policy holder 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.

WARNING TO DISTRICT OF COLUMBIA APPLICANTS: 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 in-surer files a statement of claim or an application containing any false, incomplete, or misleading information is guilty of a felony of the third degree.

NOTICE TO KANSAS APPLICANTS: 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, commits a fraudulent insurance act, which is a crime and subjects such person to criminal and civil penalties.

NOTICE TO 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 MAINE 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 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 MINNESOTA APPLICANTS: A person who files a claim with intent to defraud or helps commit a fraud against an insurer is guilty of a crime.

NOTICE TO OHIO APPLICANTS: 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.

NOTICE TO OKLAHOMA APPLICANTS: 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 RHODE ISLAND 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.

FRAUD WARNING (APPLICABLE IN VERMONT, NEBRASKA AND OREGON): Any person who intentionally presents a materially false statement in an application for insurance may be guilty of a criminal offense and subject to penalties under state law.

FRAUD WARNING (APPLICABLE IN TENNESSEE, VIRGINIA 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 include imprisonment, fines, and denial of insurance benefits.

NEW YORK FRAUD WARNING: 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.

APPLICANT NAME AND TITLE: _____

APPLICANT'S SIGNATURE: _____ DATE: _____

PRODUCER'S SIGNATURE: _____ DATE: _____

AGENT NAME: _____ AGENT LICENSE NUMBER: _____

(Applicable to Florida Agents Only)

IOWA LICENSED AGENT: _____

(Applicable in Iowa Only)

A POLICY CANNOT BE ISSUED UNLESS THIS APPLICATION IS PROPERLY SIGNED AND DATED.

For purposes of creating a binding contract of insurance by this application or in determining the rights and obligations under such contract in any court of law, the parties acknowledge that a signature reproduced by either digital signature, electronic signature, facsimile or photocopy shall be the same force and effect as an original signature and that the original and any such copies shall be deemed one and the same document.