CYBERCHOICE SECURE℠

New Business Application

WITH RESPECT TO THE LIABILITY COVERAGES, THE POLICY IS CLAIMS MADE. COVERAGE UNDER THE POLICY APPLIES ONLY TO CLAIMS FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD OR THE OPTIONAL EXTENDED REPORTING PERIOD (IF PURCHASED) AND REPORTED IN ACCORDANCE WITH SECTION 8 (NOTICE) OF THE POLICY. CLAIM EXPENSES ARE WITHIN AND REDUCE THE LIMIT OF LIABILITY AND ARE SUBJECT TO THE APPLICABLE RETENTIONS.

WITH RESPECT TO THE FIRST PARTY COVERAGES AND PRIVACY BREACH RESPONSE COVERAGES, THE POLICY IS INCIDENTS DISCOVERED. COVERAGE UNDER THE POLICY APPLIES ONLY TO INCIDENTS FIRST DISCOVERED BY THE INSURED DURING THE POLICY PERIOD AND REPORTED IN ACCORDANCE WITH SECTION 8 (NOTICE) OF THE POLICY.

1. GENERAL INFORMATION		
Applicant's name:		Website:
Applicant's address:	Street:	State:
	City:	Zip:
Requested Coverage and Limit of Insurance:		
Cyber Liability Coverage		Choose an item
Cyber First Party Coverage		Choose an item

2. EXPOSURE INFORMATION	
What were the applicant's total annual revenues in the most recent completed financial year?	$
What was the % of revenue generated from e-commerce?	Choose an item
What's the type and volume of sensitive third-party (not including employees) data stored or processed by the applicant?	
Basic personal information (e.g.,: name, email, address, phone number, password):	Volume:
Personally identifiable information (e.g.,: SSN, driver's license, ID card, passport, tax payer ID):	Volume:
Financial account information (e.g.,: bank account or other financial account information):	Volume:
Protected health information (e.g.,: health status information):	Volume:
Payment card information (e.g.,: credit or debit card number, expiration date, CVV):	
- PCI Merchant or Service Provider Level:	Choose an item
- Number of annual payment card transactions:	Volume:
- Number of stored payment card numbers (for recurring payments or otherwise):	Volume:

THE HARTFORD

3. GENERAL SECURITY INFORMATION	
What best describes the applicant's cyber security organization?	Choose an item
What best describes the applicant's cyber security policy?	Choose an item
What's the extent of the applicant's employee cyber security awareness program?	Choose an item
Which cyber security standards or frameworks has the applicant adopted?	Choose an item
How often does the applicant assess its network infrastructure and applications for common vulnerabilities?	Choose an item
Which standard or framework does the applicant use for common vulnerability assessments?	Choose an item
What's the extent of the applicant's internal cyber security assessments?	Choose an item
What's the extent of the applicant's use of external security assessments?	Choose an item
How quickly are critical vulnerabilities remediated?	Choose an item
What's required to access the applicant's network and applications?	Choose an item
How is access to network and application security settings controlled?	Choose an item
How is access controlled across the applicant's network?	Choose an item
How quickly is network access terminated upon employees leaving the company?	Choose an item
How do users access the network remotely?	Choose an item
Which security protocol is used for the applicant's wireless networks?	Choose an item
What's the extent of the applicant's firewall utilization?	Choose an item
How are the applicant's router and firewall configurations managed?	Choose an item
What's the extent of the applicant's utilization of Intrusion Prevention Systems (IPS) or Intrusion Detection Systems (IDS)?	Choose an item
What's the extent of the applicant's anti-malware protection?	Choose an item
How are the applicant's web-applications protected?	Choose an item
How are the applicant's server and application configurations managed?	Choose an item
How does the applicant restrict unauthorized applications, plug-ins, add-ons and scripts?	Choose an item
Does the applicant use anti-spam, email and web content filters?	Choose an item
What's the extent of the applicant's use of retired or unsupported systems?	Choose an item
Does the applicant maintain a complete inventory of all applications and devices?	Choose an item
What best describes the applicant's patch management procedure?	Choose an item
What's the extent of the applicant's security events monitoring and logging?	Choose an item
What's the level of physical access control used at the applicant's facilities?	Choose an item
What best describes the applicant's physical monitoring of its facilities?	Choose an item
What's the extent of the applicant's cyber security incident response preparedness?	Choose an item

4. DATA PROTECTION INFORMATION (complete ONLY if any third-party data volume is stated in Section 2)	
What's the applicant's level of compliance with the Gramm-Leach-Bliley Act "Safeguards Rule" or the HIPAA and HITECH "Security Rule" and "Privacy Rule"?	Choose an item
What best describes the applicant's privacy compliance organization?	Choose an item
How does the applicant store sensitive third-party information?	Choose an item
What's the maximum to total sensitive third-party records stored in one single application, database or repository?	Choose an item
How is access to sensitive third-party information granted and controlled?	Choose an item
What's the extent of the applicant's use of Data Loss Prevention (DLP)?	Choose an item
What's the extent of protection of sensitive third-party information: a. Stored in the applicant's data repositories? b. In motion across the applicant's network or in transit across open public networks? c. Stored on portable devices? d. Accessed through user portals operated by or on behalf of the applicant? e. Stored with a cloud service provider?	Choose an item Choose an item Choose an item Choose an item Choose an item
What best describes the applicant's vendor management program?	Choose an item
Which percentage of the applicant's vendor contracts contain: a. Indemnification or hold harmless provisions in favor of the applicant? b. Insurance provisions requiring the vendor to carry cyber insurance with limits of at least $1,000,000?	Choose an item Choose an item

5. PAYMENT CARD DATA PROTECTION INFORMATION (complete ONLY if any PCI data volume is stated in Section 2)	
What's the applicant's level of compliance with PCI-DSS?	Choose an item
When was the applicant's most recent PCI-DSS assessment?	Choose an item
What was the scope of the applicant's most recent PCI-DSS assessment?	Choose an item
How is cardholder data transmitted across the applicant's network or open, public networks?	Choose an item
For merchants accepting payments through point of sale devices (only complete if applicable):	
What best describes the applicant's Point of Sale (POS) payment solution?	Choose an item
Which percentage of the applicant's POS devices are EMV compliant and currently require chip card payment?	Choose an item
How are the applicant's Point of Sale system configurations managed?	Choose an item
For merchants accepting payments through e-commerce websites (only complete if applicable):	
What best describes the applicant's e-commerce payment solution?	Choose an item
For merchants or service providers storing cardholder data (only complete if storing cardholder data):	
How is Primary Account Number (PAN) data protected in the applicant's network?	Choose an item
Is any authentication data (for example CAV2, CVC2, CVV2 or CID) stored post authorization?	Choose an item
How is the applicant's cardholder data environment (CDE) protected?	Choose an item
How is access to the cardholder data environment granted and controlled?	Choose an item
How are the applicant's encryption keys stored?	Choose an item

6. NETWORK RESILIENCE INFORMATION	
In the event of an interruption to the applicant's core network and applications:	
a. How quickly would the applicant's business operations be impacted?	Choose an item
b. Which percentage of business operations would be impacted?	Choose an item
c. What's the applicant's network redundancy?	Choose an item
d. What's the estimated number of hours to restore the applicant's business operations?	Choose an item
How often is the applicant's fail-over procedure tested?	Choose an item
How often are the applicant's critical systems and data files backed up?	Choose an item
How often are the applicant's data recovery procedures tested?	Choose an item
How does the applicant prevent interruptions caused by network equipment failure?	Choose an item
What's the extent of the applicant's disaster recovery preparedness?	Choose an item
How is the applicant's network protected against Denial of Service (DOS) attacks?	Choose an item
What's the applicant's estimated dependency on third-party network and application services?	Choose an item
Which network and application services are used by the applicant?	
a. Infrastructure and data hosting services?	Choose an item
b. Content delivery network services?	Choose an item
c. Domain name system services?	Choose an item
d. Web hosting services?	Choose an item

7. CLAIM AND INCIDENT INFORMATION		
Has the insured experienced any claims, potential claims, cyber attacks, cyber extortion demands, privacy breaches or system failures (as defined in the Policy) in the past 36 months? *If yes, please describe in the box below.*	☐ Yes	☐ No

The Insured hereby represents after inquiry, that information contained in this application is true, accurate and complete, and that no material facts have been suppressed or misstated. The Insured acknowledges a continuing obligation to report to the Insurer as soon as practicable any material changes in all such information, after signing the application and prior to issuance of the Policy, and acknowledges that the Insurer will have the right to withdraw or modify any outstanding quotations and/or authorization or agreement to bind the insurance based upon such changes. Further, the Insured understands and acknowledges that information requested in the application is for underwriting purposes only and does not constitute notice to the Insurer under the Policy of a claim or potential claim.

FRAUD NOTICE: IN CERTAIN STATES, ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN APPLICATION FOR INSURANCE CONTAINING ANY FALSE INFORMATION, OR CONCEALS FOR THE PURPOSE OF MISLEADING INFORMATION CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT INSURANCE ACT, WHICH IS A CRIME.

Insured: _____ Title: _____

Insured Signature: _____ Date: _____

Agent/Broker Name: _____