CYBERCHOICE SECURE

SUPPLEMENTAL RANSOMWARE APPLICATION

1. RANSOMWARE PROTECTION INFORMATION	
What type of email filtering does the applicant use to prevent phishing?	Choose an item.
How does the applicant manage emails with suspected malicious code?	Choose an item.
Which protocols are used to authenticate the sender and content of emails?	Choose an item.
What type of Web filtering is used by the applicant?	Choose an item.
How do users access the applicant's network remotely?	Choose an item.
How is remote access to the applicant's network controlled?	Choose an item.
How is Remote Desktop Protocol protected in the applicant's network?	Choose an item.
Which Office 365 security add-ons are utilized by the applicant?	Choose an item.
How often is anti-phishing training conducted for the applicant's employees?	Choose an item.
How is access controlled across the applicant's network?	Choose an item.
How is privileged access to the applicant's data and applications controlled?	Choose an item.
What EDR solution is used by the applicant?	Choose an item.
What's the extent of unsupported systems and applications in the applicant's network?	Choose an item.
How does the applicant maintain open port hygiene?	Choose an item.
How is Managed Service Provider (MSP) access to the applicant's network controlled?	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.

2. RANSOMWARE RECOVERY INFORMATION	
In the event of an infection of 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 the network could be recovered from a back-up?	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.
What best describes the applicant's back-up procedure?	Choose an item.
How often are the applicant's critical systems and data files backed up?	Choose an item.

THE HARTFORD

What best describes the applicant's back-up storage?	Choose an item.
How often is the applicant's network fail-over and recovery procedure tested?	Choose an item.
What's the extent of the applicant's disaster recovery preparedness?	Choose an item.

3. ADDITIONAL RANSOMWARE PROTECTION INFORMATION

Please add any comments about additional ransomware protection or recovery measures, including any clarification of responses provided above:

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 renewal 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: _____