****

**RANSOMWARE SUPPLEMENTAL APPLICATION**

**E-MAIL SECURITY**

1. Do you pre-screen e-mails for potentially malicious attachments and Links? Yes \_\_\_ No\_\_\_
2. Do you have an e-mail “quarantine service” accessed by all users? Yes \_\_\_ No\_\_\_
3. Do you have the capability to determine if an attachment is malicious prior

to the delivery to the end-user? Yes \_\_\_ No\_\_\_

1. Do you have a “Sender Policy Framework” related to incoming e-mails? Yes \_\_\_ No\_\_\_
2. Is Phishing Training conducted for all staff? Yes \_\_\_ No\_\_\_

If so, how often? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Do you use Multi-Factor Authentication (MFA) when accessing e-mail remote? Yes \_\_\_ No\_\_\_
2. If your organization uses *Office 365* do you utilize the Threat Protection add on? Yes \_\_\_ No\_\_\_

**INTERNAL SECURITY**

1. Do you use an “End Point Protection” Product across your organization?

Including Detection and Response? Yes \_\_\_ No\_\_\_

1. Do you use Multi-Factor Authentication (MFA) to protect all users? Yes \_\_\_ No\_\_\_
2. What percentage of your organization is covered by scheduled vulnerability

Scans? Yes \_\_\_ No\_\_\_

1. In what time frame do you install critical patches across your organization? \_\_\_\_\_\_\_\_\_\_\_\_\_
2. Do your users have local administrative “rights” on their computers? Yes \_\_\_ No\_\_\_
3. Is a Password Management Software (such as “Dashlane”) provided? Yes \_\_\_ No\_\_\_
4. Are your security operations “in-house” or “outsourced”? ­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_

**BACK-UP AND RECOVERY POLICIES**

1. Are all back up systems encrypted? Yes \_\_\_ No\_\_\_
2. Are your back up files kept offline, or in a Cloud Service? \_\_\_\_\_\_\_\_\_\_\_\_
3. Have you tested restoration and recovery of key server configurations

and data from backups in the last six (6) months Yes \_\_\_ No\_\_\_

1. Are you able to test the integrity of backups prior to restoration to be

Confident it is free from malware? Yes \_\_\_ No\_\_\_

If your organization takes any additional steps to detect and prevent ransomware attacks (*e.g., Segmentation of your network, software tools, external security services, etc.*) please list below:

**I understand and acknowledge that the statements and answers are true, accurate and complete and that the information submitted in this supplement becomes a part of the DUAL Cybersecurity Insurance application and is subject to the same representations, fraud warnings and conditions.**

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_