CORVUS

Ransomware Supplemental Application

EMAIL SECURITY

1. Company Name

2. If your users can access email through a web app on a non-corporate device, do you enforce Multi-Factor Authentication? ◯ Yes ◯ No

3a. Which email security filtering tool are you using?

3b. Are you using all available security features (for example: quarantine service, sandboxing and URL rewriting)? ◯ Yes ◯ No

4. Do you conduct regular phishing training and testing?

◯ Quarterly ◯ Semi-annually ◯ Annually ◯ Never

5. Do you have a secure web gateway or proxy solution to secure inbound internet traffic? ◯ Yes ◯ No

DATA BACK-UP & RECOVERY

6. How frequently do you back up electronic data?

◯ Daily with multi-generations retained ◯ Daily ◯ Weekly ◯ Less than weekly

7. Are all of your backups kept separate from your network ("offline") so that they are inaccessible from endpoints and servers that are joined to the corporate domain, or in a cloud service designed for this purpose? ◯ Yes ◯ No

If no: please describe compensating controls that you have in place.

8. Is Multi-Factor Authentication required for access to backup files? ◯ Yes ◯ No

9. Have you tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months? ◯ Yes ◯ No

CORVUS

10. As part of your data back-up strategy, do you maintain at least 3 separate copies of your data stored in different geographic locations? (Production, Local Copies, and offsite storage). ◯ Yes ◯ No

INTERNAL SECURITY & CONTROLS

11. Do you use Multi-Factor Authentication to secure all domain or network administrator accounts? ◯ Yes ◯ No

12. Do you restrict employee access to sensitive information on a business-need to know basis? ◯ Yes ◯ No

13. Do you use an Endpoint Detection and Response (EDR) or a Next-Generation Antivirus (NGAV) (i.e. CrowdStrike, SentinelOne, CybeReason, Carbon Black) software to secure all system endpoints? ◯ Yes ◯ No

If yes: please list providers.

14. Do you allow remote access to your network? ◯ Yes ◯ No

If yes: do you use

a) a properly configured and secure VPN? ◯ Yes ◯ No

b) Multi-Factor Authentication to secure all remote access to your network? ◯ Yes ◯ No

15. Do you have a Business Continuity Plan (BCP) or Disaster Recovery Plan (DRP) in place? ◯ Yes ◯ No

If yes: is your BCP/DRP tested at least annually? ◯ Yes ◯ No

16. Do you encrypt all sensitive and confidential information

a) stored on your organization's systems and networks? ◯ Yes ◯ No

b) stored on your organization's backups? ◯ Yes ◯ No

If no to either: are the following compensating controls in place:

I) Segregation of servers that store sensitive and confidential information? ◯ Yes ◯ No

II) Access control with role-based assignments? ◯ Yes ◯ No

CORVUS

17. Do you encrypt all sensitive and confidential information

c) stored on mobile devices? ◯ Yes ◯ No

d) in transit from your network? ◯ Yes ◯ No

Warranty

All Insureds agree that the statements contained herein are their agreements and representations, which shall be deemed material to the risk, and that, if issued, the Policy will be in reliance upon the truth thereof. The misrepresentation or non-disclosure of any material matter by the Insured or its agent will render the Policy null and void and relieve the Company from all liability under the Policy.

Signature	Print Name	Date