Ransomware Supplemental Application

Please provide responses below concerning the Information Technology (IT) environment of your organization and any subsidiaries for which the insurance is being sought.

Responses to this application should be accurate as of the date that the application is signed and dated below. If your organization plans to make changes to its IT environment prior to inception of the policy, or during the policy period, please describe those plans in the "Other Cybersecurity Controls & Preventative Measures" section, below.

Budgets & Personnel

1. a. Annual IT budget $ _____ b. Percentage of IT budget spent on cybersecurity _____%
2. a. Full-time IT employees _____ b. Full-time IT cybersecurity employees _____
3. Cybersecurity point of contact (CISO or equivalent role):

Name	Title	Email	Telephone

Email Security

4. What security controls do you have in place for incoming email? Choose all that apply.

a. ☐ Screening for malicious attachments
b. ☐ Screening for malicious links
c. ☐ Quarantine service
d. ☐ Detonation and evaluation of attachments in a sandbox
e. ☐ Tagging external emails
f. ☐ DomainKeys Identified Mail (DKIM)
g. ☐ Sender Policy Framework (SPF) strictly enforced
h. ☐ Domain Based Message Authentication, Reporting and Conformance (DMARC)

5. How frequently do you conduct the following training for all employees?

Type of training	Never/not regularly	Annually	≥2x per year
a. Interactive phishing training	☐	☐	☐
b. Phishing email simulations	☐	☐	☐

6. Do you require additional training for employees who fail phishing email simulations? ☐ No ☐ Yes

7. a. What Microsoft 365 license (or equivalent license) do you use for all, or substantially all, of your users? ☐ E1 ☐ E3 ☐ E5 ☐ Other ☐ None

   b. If you use Microsoft 365, do you use the Microsoft 365 Defender (formerly known as Advanced Threat Protection) add-on or an equivalent cybersecurity product with advanced threat hunting? (Leave blank if you do not use Microsoft 365.) ☐ No ☐ Yes

8. a. Do you disable macros in your office productivity software by default? (E.g., Microsoft Office, Google Workspace) ☐ No ☐ Yes

   b. If "Yes" to a., are users allowed to enable macros? ☐ No ☐ Yes

9. Have you disabled legacy email protocols that use basic authentication (a username and password only), such as IMAP, POP3, and SMTP? ☐ No ☐ Yes

Identity & Access Management

10. Do you enforce multi-factor authentication (MFA) for all user accounts (other than Domain Administrator accounts) when accessing your network remotely? Please note any exceptions in the "Other Cybersecurity Controls & Preventative Measures" section, below.

☐ No ☐ Yes ☐ Remote access not permitted

MFA includes but is not limited to the following: a call, SMS, push notification, time-based one-time password, OATH token, hardware token, device pinning, authenticator apps, biometrics, or a FIDO2 key (e.g., YubiKey, RSA SecurID).

"User accounts" include employees and (where applicable) students, volunteers, interns, third-party contractors, and any other persons with a user account on your network; "user accounts" does not include service accounts, which are addressed in a separate section below.

11. a. Do you permit users remote access to web-based email (e.g., Outlook Web Access (OWA))? ☐ No ☐ Yes

    b. If "Yes" to a., do you enforce MFA for access to web-based email? ☐ No ☐ Yes

12. Do you provide your employees with password management software? ☐ No ☐ Yes

13. Do you enforce MFA for all Domain Administrator accounts? Please note any exceptions in the "Other Cybersecurity Controls & Preventative Measures" section, below. "Domain Administrator accounts" does not include service accounts, which are addressed in a separate section below. ☐ No ☐ Yes

14. Do you permit ordinary users local administrator rights to their devices (e.g., laptops)? ☐ No ☐ Yes

15. a. Do you use a Privileged Access Management (PAM) tool? ☐ No ☐ Yes

    b. If "Yes" to a., are all privileged accounts managed with a PAM tool? ☐ No ☐ Yes

Unsupported & End of Life Software

16. Do you use an asset discovery tool that continuously maps devices on your internal network? ☐ No ☐ Yes

17. Do you have an up-to-date asset database? ☐ No ☐ Yes

18. Do you have an up-to-date configuration management database (CMDB)? ☐ No ☐ Yes

19. a. Do you have any end-of-life or end-of-support software on your network? ☐ No ☐ Don't know ☐ Yes

    b. If "Yes" to a., is the software segregated from the rest of the network?

    ☐ No ☐ Some is, some isn't ☐ Yes

    c. If "Yes" to a., do you purchase additional support for the software, where available? ☐ No ☐ Yes

Service Accounts

20. How many service accounts with domain administrator privileges are in your IT environment? "Service accounts" are non-human privileged accounts used to execute applications, access local and network resources, and run automated services, virtual machine instances, and other processes.

☐ >10 ☐ 6-10 ☐ 1-5 ☐ 0

Please answer the remaining questions in this section only with respect to service accounts with domain administrator privileges. If you do not have any service accounts with domain administrator privileges, please skip the remaining questions in this section.

21. Do you configure service accounts using the principle of least privilege? (I.e., have you removed domain administrator privileges from those service accounts that don't require such privileges to function?) ☐ No ☐ Yes

22. Do you have specific monitoring rules in place for service accounts to alert your Security Operations Center (SOC) of any abnormal behavior? ☐ No ☐ Yes

23. Have you configured service accounts to deny interactive logins? ☐ No ☐ Yes

24. Do you require service account passwords to be ≥25 characters or to be randomly generated? ☐ No ☐ Yes

25. Do you rotate passwords for service accounts on a regular basis? ☐ No ☐ Yes

26. Do you manage passwords for service accounts with a PAM solution or password vault? ☐ No ☐ Yes

Security Products & Solutions

27. What security solutions do you use to prevent or detect malicious activity on your network?

Security solution	Vendor
a. Endpoint Protection Platform (EPP)	
b. Endpoint Detection and Response (EDR)	
c. Managed Detection and Response (MDR)	
d. Network Detection and Response (NDR)	
e. Security Information and Event Management (SIEM)	
f. Application Isolation and Containment	

28. a. Do you have a Security Operations Center (SOC)? ☐ No ☐ Yes, working hours only ☐ Yes, 24/7

b. If "Yes" to a., is your SOC internal or managed by a third party? ☐ Internal ☐ Third party ☐ Both

c. If "Yes" to a., does your SOC have the authority and ability to remediate security events (for example, by isolating and containing endpoints remotely)? ☐ No ☐ Yes

29. Do you use a protective DNS service (e.g., Quad9, OpenDNS or the public sector PDNS)? ☐ No ☐ Yes

30. Are host-based and network firewalls configured to disallow inbound connections by default? ☐ No ☐ Yes

31. a. Do you use Remote Desktop Protocol (RDP), Virtual Network Computing (VNC), AnyDesk, TeamViewer, or other remote desktop software?

☐ Yes ☐ Yes, but internally only and not exposed to the internet ☐ No

b. If "Yes" to a., does access require MFA? ☐ No ☐ Yes

32. Do you deny all Server Message Block (SMB) (i.e., Windows file sharing) inbound communications to servers (except where there is an identified business need)? ☐ No ☐ Yes

Vulnerabilities & Scanning

33. Do you use a hardened baseline configuration across all (or substantially all) of your devices? ☐ No ☐ Yes

34. What percentage of the enterprise is covered by scheduled vulnerability scans? ____%

35. In the past two years, how often have you conducted vulnerability scanning of the devices on your network?

☐ Never/not regularly ☐ Annually ☐ 2-3 times per year ☐ Quarterly or more often

36. In the past two years, what is the average time that your organization has taken to remediate Critical Common Vulnerabilities and Exposures (Critical CVEs) (CVSS version 3.1 Base Score 9.0-10.0) on your network?

☐ Unknown ☐ >2 weeks ☐ <2 weeks ☐ <1 week ☐ <48 hours

37. How often do you (or a third party on your behalf) conduct penetration testing on your network?

☐ Never/not regularly ☐ Annually ☐ 2-3 times per year ☐ Quarterly or more often

Backups & Resilience

38. Do you rely on a backup solution that is located on your corporate network? ☐ No ☐ Yes

39. a. Do you rely on a cloud-based service as your backup location? ☐ No ☐ Yes

    b. If "Yes" to a., is your cloud-based backup service a "syncing service"? (E.g., DropBox, OneDrive, SharePoint, Google Drive) ☐ No ☐ Yes

    c. If "Yes" to a., have you determined how long it would take to restore all of your data from the cloud?

    ☐ No ☐ Yes, >1 week ☐ Yes, >48 hours but <1 week ☐ Yes, <48 hours

40. Do you maintain any offline backups? ☐ No ☐ Yes, partial backups ☐ Yes, full backups

41. a. Are all of your backups encrypted? ☐ No ☐ Some backups are encrypted, some aren't ☐ Yes

    b. For your encrypted backups, do you maintain an offline backup of your decryption key(s)? ☐ No ☐ Yes (Skip this question if you do not have any encrypted backups.)

42. Are any of your backup solutions "immutable"? (Immutable backups cannot be altered or deleted.) ☐ No ☐ Yes

43. How frequently do you perform a test restoration from backups?

☐ Never/not regularly ☐ Annually ☐ 2-3 times per year ☐ Quarterly or more often

44. Do you have the ability to test the integrity of backups prior to restoration to be confident that your backups are free from malware? ☐ No ☐ Yes

Business Continuity & Planning

45. a. Do you have a business continuity or disaster recovery plan, that includes responding to cybersecurity threats, that was created or updated within the past two years? ☐ No ☐ Yes

    b. If "Yes" to a., have you engaged in any exercises to run through the plan (from start to finish) with your incident response team? ☐ No ☐ Yes

46. a. Have you conducted, within the past two years, a cybersecurity incident tabletop exercise? ☐ No ☐ Yes

    b. If "Yes" to a., did that tabletop exercise include the threat from ransomware? ☐ No ☐ Yes

Other Cybersecurity Controls & Preventative Measures

Please use the space below to clarify any answers above that may be incomplete or require additional detail. Please also describe any additional steps your organization takes to detect, prevent, and recover from ransomware attacks (e.g., segmentation of your network, additional software security controls, external security services, etc.).

THE UNDERSIGNED IS AUTHORIZED BY THE APPLICANT TO SIGN THIS APPLICATION ON THE APPLICANT'S BEHALF AND DECLARES THAT THE STATEMENTS CONTAINED IN THE INFORMATION AND MATERIALS PROVIDED TO THE INSURER IN CONJUNCTION WITH THIS APPLICATION AND THE UNDEWRITING OF THIS INSURANCE ARE TRUE, ACCURATE AND NOT MISLEADING. SIGNING OF THIS APPLICATION DOES NOT BIND THE APPLICANT OR THE INSURER TO COMPLETE THE INSURANCE, BUT IT IS AGREED THAT THE STATEMENTS CONTAINED IN THIS APPLICATION AND ANY OTHER INFORMATION AND MATERIALS SUBMITTED TO THE INSURER IN CONNECTION WITH THE UNDERWRITING OF THIS INSURANCE ARE THE BASIS OF THE CONTRACT SHOULD A POLICY BE ISSUED, AND HAVE BEEN RELIED UPON BY THE INSURER IN ISSUING ANY POLICY.

THIS APPLICATION AND ALL INFORMATION AND MATERIALS SUBMITTED WITH IT SHALL BE RETAINED ON FILE WITH THE INSURER AND SHALL BE DEEMED ATTACHED TO AND BECOME PART OF THE POLICY IF ISSUED. THE INSURER IS AUTHORIZED TO MAKE ANY INVESTIGATION AND INQUIRY AS IT DEEMS NECESSARY REGARDING THE INFORMATION AND MATERIALS PROVIDED TO THE INSURER IN CONNECTION WITH THE UNDERWRITING AND ISSUANCE OF THE POLICY.

THE APPLICANT AGREES THAT IF THE INFORMATION PROVIDED IN THIS APPLICATION OR IN CONNECTION WITH THE UNDERWRITING OF THE POLICY CHANGES BETWEEN THE DATE OF THIS APPLICATION AND THE EFFECTIVE DATE OF THE INSURANCE, THE APPLICANT WILL, IN ORDER FOR THE INFORMATION TO BE ACCURATE ON THE EFFECTIVE DATE OF THE INSURANCE, IMMEDIATELY NOTIFY THE INSURER OF SUCH CHANGES, AND THE INSURER MAY WITHDRAW OR MODIFY ANY OUTSTANDING QUOTATIONS OR AUTHORIZATIONS OR AGREEMENTS TO BIND THE INSURANCE.

I HAVE READ THE FOREGOING APPLICATION FOR INSURANCE AND REPRESENT THAT THE RESPONSES PROVIDED ON BEHALF OF THE APPLICANT ARE TRUE AND CORRECT.

Digital signature required below [click the red tab to create a digital ID or import an existing digital ID]:

Signed: _____

Print Name: _____

Title: _____

Company: _____

Date: _____