Cyber Insurance Application

1. Company Name

2. Company Address

3a. Primary Website[1]

3b. Additional Websites

4. Nature of Business (Industry)

5a. Current Gross Annual Revenue (previous 12 months) 5b. Projected Gross Annual Revenue (next 12 months)

6. Are there any subsidiaries for which the Named Insured wishes to cover under the policy? If Yes: Please list the names below and provide a relevant organization chart.

◯ Yes ◯ No

7. Estimated amount of records containing unique personally identifiable information, that are stored, processed or transmitted by the Applicant (including records stored by third-party providers).

◯ 0 - 250,000
◯ 250,001 - 500,000
◯ 500,001 - 1,000,000
◯ 1,000,001 - 2,500,000
◯ 2,500,001 - 5,000,000
◯ 5,000,001 - 10,000,000
◯ If greather than 10M, provide an estimate below:

8. Does the Applicant collect, capture, purchase, receive through trade, or otherwise obtain biometric data (biometric data is data related to body measurements and calculations related to human characteristics and includes, but is not limited to, fingerprints, iris or retina scans, voiceprints, sleep/health/exercise data, DNA or biological markers)?

◯ Yes ◯ No

9. Do you have ***email filtering*** in place?

◯ Yes ◯ No

9b. Do you use an advanced email security solution that includes features such as URL and attachment sandboxing. (Secure Email Gateway)

◯ Yes ◯ No

If "Yes", please list the name of your solution.

10. Do you have a backup solution ◯ Yes ◯ No

If "Yes", how frequently do you back up systems and data?

◯ Continuous ◯ Daily ◯ Weekly ◯ Monthly

10b. Which of the following are in place for your backup solution(s)? (Please select ALL that apply)

- ☐ Backup servers are segmented from the rest of the network
- ☐ Copy of backups are kept *offline* or *air-gapped*
- ☐ Cloud based backups
- ☐ Backup servers are not joined to a Windows domain
- ☐ Backup solution with *immutable backups*
- ☐ Backup servers and user accounts use unique credentials
- ☐ MFA required for access to backups
- ☐ Multiple copies of backups stored in 2 or more geographical locations

11. Which of the of the following apply to your *Multi-Factor Authentication (MFA)* implementation? (Please select ALL that apply)

a. MFA enforced to secure all *remote access* to your network. ◯ Yes ◯ No ◯ N/A

b. MFA enforced to secure internal use of privileged accounts (administrator accounts, service accounts, etc.) ◯ Yes ◯ No

c. MFA enforced for email access via webmail portal (i.e. Gmail), mailbox applications (i.e. Outlook Application) and non-corporate devices for all employees ◯ Yes ◯ No

d. MFA enforced to secure access to all critical applications ◯ Yes ◯ No

12. How are privileged accounts secured and managed? (Please select ALL that apply)

- ☐ Administrative users use different accounts for administrative use and non-administrative use (e.g. day to day activities such as web browsing and email)
- ☐ A password management vault is used to manage privileged accounts
- ☐ Standard users do not have administrative rights to their workstations
- ☐ Local administrator accounts are unique and complex on all systems

13. What Endpoint Security Technology do you have in place? (Please select ALL that apply and list the product and vendor)

- ☐ *Next Gen Antivirus*
- ☐ *Endpoint Detection & Response (EDR)*
- ☐ *Managed Detection & Response (MDR)*
- ☐ *Extended Detection & Response (XDR)*

14. What security controls are in place to protect against unauthorized access to sensitive and confidential data?

- [ ] Least privilege access using role-based assignments
- [ ] Network segmentation of servers containing sensitive data
- [ ] Logging and monitoring
- [ ] MFA required for all user access to systems/applications with sensitive data
- [ ] Encryption at Rest (File level)
- [ ] Encryption of Data in-transit

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

If yes, has it been tested in the last 12 months? ◯ Yes ◯ No

16. Do you have an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) in place? ◯ Yes ◯ No

17. Do you conduct penetration testing of your network at least annually? ◯ Yes ◯ No

18. Do you conduct employee security training or phishing training, for all employees, at least annually? ◯ Yes ◯ No

19. Prior to executing an electronic payment, do you verify the validity of the funds transfer request or payment change request, with the requestor, via a separate means of communication prior to transferring funds or making payment changes?[3] ◯ Yes ◯ No

20. If the Applicant uses multimedia material provided by others, does the Applicant always obtain the necessary rights, licenses, releases, and consents prior to publishing? ◯ Yes ◯ No ◯ **N/A**

21. If the Applicant accepts payment cards in exchange for goods or services rendered, is the Applicant or their outsourced payment processor PCI compliant? ◯ Yes ◯ No ◯ N/A

22. In the past three years, have you experienced any cyber security incident, data privacy incident or any multimedia liability claim? If Yes, please provide additional details via addendum. ◯ Yes ◯ No

23. Do you or any other person or organization proposed for this insurance have knowledge of any actual or alleged: security breach, privacy breach, privacy-related event or incident, breach of privacy, or multimedia incident that may reasonably be expected to give rise to a claim or to costs being incurred? If Yes, please provide additional details via addendum. ◯ Yes ◯ No

24. In the past 3 years, have you or any other organization proposed for this insurance sustained any unscheduled network outage or interruption lasting longer than 6 hours? If Yes, please provide additional details via addendum. ◯ Yes ◯ No

Glossary

Air Gapped Backups
A method to create an 'offline backup'. A barrier between primary digital assets and malicious actors / catastrophes. There are two methods to create an air gapped backup: physical or logical air gap.

Business Continuity Plan (BCP)
Document with predetermined set of instructions or procedures that describes the actions, process and tools for ensuring an organization can continue critical operations during a significant disruption.

Disaster Recovery Plan (DRP)
Document with processes, policies and procedures related to preparing for recovery or continuation of an organization's critical business functions, technology infrastructure, systems and applications following a disruption.

Email Filtering
Email security tool used to 'filter out' spam and other malicious content from an organization's inbound and outbound email messages. Email filtering provides average protection against obvious spam emails, but does not protect against more targeted and sophisticated email attacks.

Endpoint Detection & Response (EDR)
Security software that collects endpoint data and performs real-time continuous monitoring with rule-based automated response and analysis capabilities. An EDR has the capability to detect suspicious behavior, automatically block malicious activity, and provide remediation steps to restore affected system.

Extended Detection & Response (XDR)
XDR extends EDR capabilities to protect more than endpoints. The security solution aims to simplify an organization's entire security stack (endpoints, cloud resources, email, network, etc.) by providing integrated visibility and threat management within a single solution.

Immutable Backups
A type of backup copy that is unchangeable and prevents any deletion or modifications.

Intrusion Detection System (IDS) or Intrusion Prevention System (IPS)
An Intrusion Detection System (IDS) is a network tool used to monitor traffic for suspicious activity and alerts administrators when potential threats or suspicious activity is detected within a network. An Intrusion Prevention System (IPS) takes this a step further by detecting and also actively blocking malicious activity in real-time to prevent or reduce the impact of detected threats.

Logical Air Gap
Network and user access controls used to create an 'isolated backup' that is separate and inaccessible from the primary production environment.

Managed Detection & Response (MDR)
A third-party organization that provides 24/7 outsourced cybersecurity services like threat hunting, network monitoring, and remediation of detected threats.

Multi-factor Authentication (MFA)
Multi-factor authentication (MFA) is an authentication method that requires a user to provide two or more verification methods in order to gain access to a resource or system. MFA requires a combination of: something you know (a password or PIN), something you have (a code or token generated by a cell phone app or other hardware), and/or something you are (a fingerprint or face scan). Modern MFA does not include static authentication methods such as; certificates or pre-shared keys (PSK).

Next Generation Antivirus (NGAV)
Next-Gen AV (NGAV) can protect a system with more advanced malware enhanced capabilities to detect suspicious behaviors within the system with the limitations of exclusively focusing on the system it's installed on.

Offline backups
A copy of an organization's data which is offline (disconnected) and cannot be accessed from the primary environment.

Out-of-Band Authentication (OOBA)
Secondary verification method with the requester of a funds transfer through a communication channel separate from the original request. An example of this would be calling a known and trusted phone number to confirm a change in payment instructions sent via email from a vendor.

Personally Identifiable Information
Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. This includes, but is not limited to; social security number, medical service or healthcare data, driver's license or state identification number, account, credit card, or debit card number.

Penetration Testing
Penetration testing is a simulated 'pressure test' of an organization's systems and is typically performed by an authorized third-party. The goal of this exercise is to uncover vulnerabilities and misconfigurations within an environment before real attackers can exploit them, which helps to strengthen cyber defenses proactively.

Physical Air Gap
Backup copies on a storage media that are disconnected from the network and physically stored offsite.

Privileged Access Management (PAM) Solution
Software that focuses on secure management of privileged access. Privileged credentials are stored in a centralized, secure vault. PAM Solutions also include the ability to monitor and log privileged access and automate provisioning / deprovisioning of privileged accounts (i.e. account check-in and check-out).

Privileged Accounts
An account with elevated administrative privileges. Examples include domain admin accounts, local admin accounts, cloud admin accounts and service accounts.

Remote Access
Ability for a user to access a device, corporate web based service or network from any location through a network connection.

Secure Email Gateway (SEG)
Advanced email security solution used to monitor inbound and outbound emails to protect against spam, phishing, or malicious emails containing viruses and malware. The core functionality of SEG includes URL rewriting, URL and Attachment Sandboxing, impersonation protection for key individuals (CIO/CFO), and clawback ability to remove an email from an inbox if it is determined to be malicious after it has been delivered.

Standard Antivirus
Antivirus (AV) technology is most commonly used for personal computers, where it can be a useful tool for scanning systems and identifying malware. It blocks the execution of files, and quarantines or deletes detected malicious files, but it only offers minimal protection.

Virtual private network (VPN)
Encrypted connection over the internet from a device to a network. The encrypted connection ensures that sensitive data is securely transmitted. Most commonly used to provide a secure remote connection to an organization's network.

Applicant Signature

Print Name

Date

Applicant Email[2]

Applicant Title

Notices

Notice to All Applicants: Any person who knowingly, and with intent to defraud any insurance company or other person, files an application for insurance or statement of claim containing any materially false information, or, for the purpose of misleading, conceals information concerning any fact material thereto, may commit a fraudulent insurance act which is a crime and subjects such person to criminal and civil penalties in many states.

Notice to Alabama, Arkansas, New Mexico, and Rhode Island: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or who knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

Notice to California Applicants: For your protection California law requires the following to appear on this form. Any person who knowingly presents false or fraudulent information to obtain or amend insurance coverage or to make a claim for the payment of a loss is guilty of a crime and may be subject to fines and confinement in state prison.

Notice to Colorado Applicants: It is unlawful to knowingly provide false, incomplete or misleading facts or information to an insurance company for the purpose of defrauding or attempting to defraud the company. Penalties may include imprisonment, fines, denial of insurance and civil damages. Any insurance company or agent of an insurance company who knowingly provides false, incomplete, or misleading facts or information to a policyholder or claimant for the purpose of defrauding or attempting to defraud the policyholder or claiming with regard to a settlement or award payable for insurance proceeds shall be reported to the Colorado Division of Insurance within the Department of Regulatory Agencies.

Notice to District of Columbia and Louisiana Applicants: Any person who knowingly presents a false or fraudulent claim for payment of loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

Notice to Florida Applicants: Any person who knowingly and with intent to injure, defraud or deceive any insurance company, files a statement of claim containing any false, incomplete, or misleading information is guilty of a felony of the third degree.

Notice to Oklahoma Applicants: Any person who knowingly, and with intent to injure, defraud or deceive any insurer,files a statement of claim containing any false, incomplete or misleading information is guilty of a felony.

Notice to Kansas Applicants: An act committed by any person who, knowingly and with intent to defraud, presents,causes to be presented or prepares with knowledge or belief that it will be presented to or by an insurer, purported insurer, broker or any agent thereof, any written statement as part of, or in support of, an application for the issuance of, or the rating of an insurance policy for personal or commercial insurance, or a claim for payment or other benefit pursuant to an insurance policy for commercial or personal insurance which such person knows to contain materially false information concerning any fact material thereto; or conceals, for the purpose of misleading, information concerning any fact material thereto.

Notice to Maine, Tennessee, Virginia and Washington Applicants: It is a crime to knowingly provide false,incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties may include imprisonment, fines and/or denial of insurance benefits.

Notice to Maryland Applicants: Any person who knowingly or willfully presents a false or fraudulent claim for payment of a loss or benefit or who knowingly or willfully presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

Notice to New Hampshire Applicants: Any person who, with a purpose to injure, defraud or deceive an insurance company, files a statement of claim containing any false, incomplete or misleading information is subject to prosecution and punishment for insurance fraud as provided in RSA 638:20.

Notice to New York Applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information, or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime, and shall also be subject to a civil penalty not to exceed $5,000 and the stated value of the claim for each such violation.

Notice to Pennsylvania Applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information or conceals for purposes of misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime and subjects such person to criminal and civil penalties.