



5. Are you engaged in any of the following business activities?

- Adult content, gambling or cannabis (containing THC) as a grower, wholesaler or medical/recreational retailer;
- Cryptocurrency, blockchain technology, payment processing or debt collection;
- Data processing/aggregation, storage or hosting services to third parties as a professional service (e.g., as a managed services provider (MSP) or data aggregator); or
- Managed care or accountable care.

No Yes

Records

6. How many individual records do you hold for each type of information? If a record could fall into more than one category, count it toward the most appropriate category.

- a. Payment Card Information (PCI) _____
- b. Protected Health Information (PHI) _____
- c. Biometric Information _____
- d. Personally Identifiable Information (PII) _____

Cybersecurity Controls

7. Do you require Multi-Factor Authentication (MFA) for remote access to your network (both cloud-hosted and on-premises, including via Virtual Private Networks (VPNs))?

No Yes Remote access not permitted

8. Do you require MFA for access to web-based email?

No Yes Access not permitted/no web-based email

9. What security controls do you have in place to protect Domain Administrator accounts?

a. Do you enforce MFA for privileged accounts in Azure Active Directory (AAD) (including the members of the AAD Domain Controller administrators group)?

No Yes We do not use AAD

b. Are Domain Administrators permitted to connect only to domain controllers (and not email or connect to the internet)?

No Yes

c. Are Domain Administrators configured with unique, random, and long (>25 characters) passwords?

No Yes



10. What security controls do you have in place for incoming email? Choose all that apply.
- Screening for malicious attachments Screening for malicious links Tagging external emails
11. How often do you conduct interactive social engineering (i.e., phishing) training?
- Never/not regularly Annually ≥2x per year
12. Do you regularly backup your business critical data?
- No At least monthly At least weekly or daily
13. Where do you backup your business critical data? Choose all that apply.
- Corporate network Cloud service Offline
14. If you rely on a cloud-based backup service, is it a “syncing service”? (E.g., DropBox, OneDrive, Google Drive)
- No Yes No cloud backups
15. How frequently do you perform a test restoration from backups?
- Never/not regularly Annually 2-3 times per year Quarterly or more often
16. 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)	

17. Do you have a Security Operations Center (SOC)?
- No Yes, working hours only Yes, 24/7
18. 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 on your network?
- No Some is, some isn't Yes
19. Are network firewalls configured to disallow inbound connections by default? No Yes
20. Do you use a hardened baseline configuration across all (or substantially all) of your devices? No Yes
21. Do you permit ordinary users local administrator rights to their devices (e.g., laptops)? No Yes
22. Do you have an incident response plan for network intrusions and malware incidents? No Yes



23. Do you, or an outsourced service provider on your behalf, actively manage and install critical patches across your internet-facing systems? No Yes
24. Do you use the Microsoft 365 Defender add-on or an equivalent cybersecurity product with advanced threat hunting to protect against phishing and business email compromise? No Yes
25. Do you disable macros in your office productivity software by default? (E.g., Microsoft Office, Google Workspace) No Yes
26. Do you use any remote desktop clients (e.g., Microsoft Remote Desktop, TeamViewer, Virtual Network Computing (VNC), AnyDesk) that are exposed directly to the internet? No Yes

PCI Controls

27. a. Do you accept payment cards for goods sold or services rendered? No Yes
- b. If “Yes” to a., do you ensure point-to-point encryption of payment card data? No Yes
- c. If “Yes” to a., do you maintain payment card data on your network?
 No Yes, unencrypted Yes, tokenized or encrypted

Media Controls

28. a. Do you have a formal review process in place to screen any published or broadcast material (including digital content), for intellectual property and privacy compliance prior to any publication, broadcast, distribution, or use? No Yes
- b. If “Yes” to a., are such reviews conducted by, or under the supervision of, an attorney? No Yes
29. Do you have notice and take-down procedures in place to address potentially libelous, infringing, or illegal content on your website(s) (e.g., DMCA or similar)? No Yes

Money Transfer Controls

30. Are employees who are responsible for disbursing or transmitting funds provided anti-fraud training, including detection of social engineering, phishing, business email compromise and other scams, on at least an annual basis? No Yes
31. When a vendor or supplier requests any change to its account details (including routing numbers and account numbers), do you confirm requested changes via an out-of-band authentication (a method other than the original means of request)? For example, if a request is made by email, a follow-up phone call is placed to confirm that the supplier or vendor made the request. No Yes



Operational Technology Controls

Complete this section *only if* (1) you are in the manufacturing, construction, transportation, warehousing, utilities, and wholesale trade industries; (2) you have Operational Technology (OT) in your environment; *and* (3) your OT is accessible (i.e., not air-gapped) from your IT network or the internet.

Check here if these questions do not apply to you based on the above criteria.

32. Is your OT environment segmented from your Information Technology (IT) environment(s)? No Yes
33. Is your OT environment segmented from the internet? No Yes
34. Do you enforce MFA for employee remote access to your OT environment? No Yes Not permitted
35. Do you enforce MFA for third-party remote access to your OT environment? No Yes Not permitted

Mergers & Acquisitions

36. Have you, within the past 12 months, completed or agreed to a merger, acquisition, or consolidation? No Yes

If “Yes,” please provide details:

Prior Claims & Circumstances

37. Do you or any other proposed insured (including any director, officer, or employee) have knowledge of or information regarding any fact, circumstance, situation, event, or transaction that may give rise to a claim, loss, or obligation to provide breach notification under the proposed insurance? No Yes
38. During the past five years, have you:
- a. Received any claims or complaints with respect to privacy, breach of information, breach of network security or unauthorized disclosure of information? No Yes
 - b. Been subject to any government action, investigation or subpoena regarding any alleged violation of a privacy law or regulation? No Yes
 - c. Notified customers or any other third party of a data breach incident? No Yes
 - d. Experienced an actual or attempted extortion demand (including ransomware) with respect to your computer systems? No Yes

If you answered “Yes” to question 37 or any parts of question 38, please provide details regarding all such facts, circumstances, situations, incidents, or events in the “Additional Disclosures & Clarifications” section, below.



Additional Disclosures & Clarifications

Please use the space below to clarify any answers above that may be incomplete or require additional detail.

Signature Section

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 UNDERWRITING 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. FOR NORTH CAROLINA APPLICANTS, SUCH APPLICATION MATERIALS ARE PART OF THE POLICY, IF ISSUED, ONLY IF ATTACHED AT ISSUANCE.

THIS APPLICATION AND ALL INFORMATION AND MATERIALS SUBMITTED WITH IT SHALL BE RETAINED ON FILE WITH THE INSURER. 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.

FRAUD WARNING DISCLOSURE

ANY PERSON WHO, WITH INTENT TO DEFRAUD OR KNOWING THAT (S)HE IS FACILITATING A FRAUD AGAINST THE INSURER, SUBMITS AN APPLICATION OR FILES A CLAIM CONTAINING A FALSE OR DECEPTIVE STATEMENT MAY BE GUILTY OF INSURANCE FRAUD.

NOTICE TO ALABAMA, ARKANSAS, LOUISIANA, NEW MEXICO AND RHODE ISLAND APPLICANTS: ANY PERSON WHO KNOWINGLY PRESENTS A FALSE OR FRAUDULENT CLAIM FOR PAYMENT OF A 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 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 CLAIMANT WITH REGARD TO A SETTLEMENT OR AWARD PAYABLE FROM INSURANCE PROCEEDS SHALL BE REPORTED TO THE COLORADO DIVISION OF INSURANCE WITHIN THE DEPARTMENT OF REGULATORY AGENCIES.

NOTICE TO DISTRICT OF COLUMBIA APPLICANTS: WARNING: IT IS A CRIME TO PROVIDE FALSE OR MISLEADING INFORMATION TO AN INSURER FOR THE PURPOSE OF DEFRAUDING THE INSURER OR ANY OTHER PERSON. PENALTIES INCLUDE IMPRISONMENT AND/OR FINES. IN ADDITION, AN INSURER MAY DENY INSURANCE BENEFITS IF FALSE INFORMATION MATERIALLY RELATED TO A CLAIM WAS PROVIDED BY THE APPLICANT.

NOTICE TO FLORIDA APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO INJURE, DEFRAUD, OR DECEIVE ANY INSURER FILES A STATEMENT OF CLAIM OR AN APPLICATION CONTAINING ANY FALSE, INCOMPLETE OR MISLEADING INFORMATION IS GUILTY OF A FELONY IN THE THIRD DEGREE.

NOTICE TO KANSAS APPLICANTS: 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 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 COMMITS A FRAUDULENT INSURANCE ACT.

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 OR A 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 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 OKLAHOMA APPLICANTS: WARNING: ANY PERSON WHO KNOWINGLY, AND WITH INTENT TO INJURE, DEFRAUD OR DECEIVE ANY INSURER, MAKES ANY CLAIM FOR THE PROCEEDS OF AN INSURANCE POLICY CONTAINING ANY FALSE, INCOMPLETE OR MISLEADING INFORMATION IS GUILTY OF A FELONY.

NOTICE TO KENTUCKY, NEW JERSEY, OHIO AND 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 CLAIMS 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 SUBJECTS SUCH PERSON TO CRIMINAL AND CIVIL PENALTIES.

NOTICE TO VERMONT APPLICANTS: ANY PERSON WHO KNOWINGLY PRESENTS A FALSE STATEMENT IN AN APPLICATION FOR INSURANCE MAY BE GUILTY OF A CRIMINAL OFFENSE AND SUBJECT TO PENALTIES UNDER STATE LAW.

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 CLAIMS 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. (IN NEW YORK, THE CIVIL PENALTY IS NOT TO EXCEED FIVE THOUSAND DOLLARS (\$5,000) AND THE STATED VALUE OF THE CLAIM FOR EACH SUCH VIOLATION.)

For digital signature, click the red tab to create a digital ID or import an existing digital ID:

Print Name: _____

Job Title: _____ Company: _____

Signed: _____ Date: _____

If this **Application** is completed in Florida, please provide the Insurance Agent’s name and license number. If this **Application** is completed in Iowa please provide the Insurance Agent’s name and signature only.

Agent’s Printed Name: _____

Agent’s Signature: _____ Florida Agent’s License Number: _____