Notice

By completing this **Application**, the **Applicant** is applying for a **Policy** which contains one or more Insuring Agreements, some of which provide liability for **Claims** first made against any **Insured** during the **Policy Period**, or any applicable Extended Reporting Period, and reported to us pursuant to the terms of this **Policy**. **Claim Expenses** shall reduce the applicable **Aggregate Limit of Insurance** and Sub-Limits of Insurance and are subject to the applicable **Retentions**. Please read the entire **Application** and **Policy** carefully before signing. Whenever used in this **Application**, the term "**Applicant**" shall mean the **Named Insured** and all **Subsidiaries**, unless otherwise stated. All other terms which appear in bold type herein are used in this **Application** with the same respective meanings as set forth in the Cyber Insurance Policy (AB-CYB-001.2 Ed.08/2023).

General Information

01. Please complete **Applicant** details.

Name of **Applicant**
Applicant's address
Applicant's primary industry
Please list **Applicant's** website or domain (**Enter all the apply:** This should include the main website, any primary domains used for corporate email, franchise or subsidiary websites)
Applicant's previous fiscal year-end gross revenue (or projected current year-end revenue if **Applicant** did not generate previous revenue) $
Applicant's number of employees

We are not able to bind policies for any company that operates in one of our restricted industries: Gambling, Adult Content or Cannabis. Please contact our underwriting team with questions at underwriting@at-bay.com

General Information *Continued*

02. What percentage of the **Applicant's** annual revenue is from:

Ecommerce %	Online Advertising %

Data Records

03. For how many individuals does the **Applicant** store or process sensitive information?

Number of individuals

04. Indicate which of the following types of sensitive information the **Applicant** stores or processes:

- ☐ Drivers license, passport, SSN, other state ID, or federal ID numbers
- ☐ Financial account information (e.g., bank accounts)
- ☐ Payment card information (e.g., credit or debit cards)
- ☐ Protected health information (PHI)
- ☐ Combinations of usernames or email addresses with passwords to online accounts

Optional Provide any clarifying information on the records stored and processed by the **Applicant.**

Encryption & Data Security

05. Does the **Applicant** encrypt data stored and processed on databases and servers?

- ☐ Yes
- ☐ No

06. Does the **Applicant** have written policies or governance frameworks in place that define requirements for storing, securing, and transferring sensitive personal and corporate information?

- ☐ Yes
- ☐ No

Optional Describe any additional steps the **Applicant** takes to protect sensitive information.

Compliance & Payment Processing

07. Has the **Applicant** confirmed compliance with HIPAA?

- ☐ Yes
- ☐ No
- ☐ N/A

08. Has the **Applicant** confirmed compliance with the Payment Card Information Data Security Standard (PCI-DSS)?

- ☐ Yes
- ☐ No
- ☐ N/A

Optional Provide any clarifying information on the **Applicant's** compliance with HIPAA or PCI-DSS.

Compliance & Payment Processing *Continued*

09. What is the **Applicant's** current PCI Compliance Level?

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ N/A

10. Does the **Applicant** fully outsource payment card processing?

- ☐ Yes
- ☐ No
- ☐ N/A

Optional Describe any additional steps the **Applicant** takes to secure payment processing.

Financial Fraud

11. Does the **Applicant** have controls in place which require all fund and wire transfers over $25,000 to be authorized and verified by at least two employees prior to execution?

- ☐ Yes
- ☐ No

12. Does the **Applicant** conduct computer network security training for all employees (such as training on phishing prevention)?

- ☐ Yes
- ☐ No

Backups & Recovery

13. Does the **Applicant** have procedures and tools in place to back up and restore sensitive data and critical systems?

- ☐ Yes
- ☐ No

14. Does the **Applicant** keep offline backups that are disconnected from its network or store backups with a cloud service provider?

- ☐ Yes
- ☐ No

15. Which of the following describes how the backup copies are stored? Select all that apply. *Optional*

- ☐ Backups are offline/air-gapped
- ☐ Backups are stored without network separation
- ☐ Cloud sync (e.g. Google Drive, Microsoft OneDrive, Microsoft SharePoint)
- ☐ Dedicated cloud-based backup service (e.g. Acronis, Veeam, CrashPlan)
- ☐ Unknown

Please provide the names of the backup vendors:

16. Are all critical backup copies configured as immutable (cannot be modified or deleted within their retention window)? *Optional*

- ☐ Yes
- ☐ No
- ☐ Unknown

17. Does the **Applicant** have a formal Business Continuity / Disaster Recovery Plan that has been tested in the last year

- ☐ Yes
- ☐ No

Optional Describe any additional steps the Applicant takes to backup sensitive data and critical systems.

Security Controls

18. Which of the following security controls are used by the **Applicant**?

- ☐ Antivirus
- ☐ Data Loss Prevention (DLP)
- ☐ Intrusion Detection/Prevention System (IDS/IPS)
- ☐ Multi-factor Authentication
- ☐ Regular Penetration Tests

Optional Provide any additional details on the steps the **Applicant** takes to protect its networks.

19. Does the **Applicant** have multi-factor authentication enforced on all email access?

- ☐ Yes
- ☐ No

20. Does the **Applicant** have multi-factor authentication enforced on all remote access including VPN or other remote network access?

- ☐ Yes
- ☐ No

21. Does the **Applicant** utilize a Virtual Private Network (VPN) for remote connection to company resources? *Optional*

- ☐ Yes
- ☐ No
- ☐ Unknown

Security Controls *Continued*

22. How is the **Applicant's** VPN infrastructure hosted? *Optional*

- ☐ Exclusively Cloud-based (e.g. all VPNs are SaaS)
- ☐ Exclusively Non Cloud-based (e.g. all VPNs are hosted On-Prem)
- ☐ Hybrid (some VPN infrastructure hosted in the Cloud, some hosted On-Prem)

23. Which of the following VPN providers/products does the **Applicant** use? Please select all that apply. *Optional*

- ☐ Barracuda SSL VPN
- ☐ Check Point FireWall/VPN
- ☐ Cisco ASA SSL VPN
- ☐ Citrix SSL VPN
- ☐ ConnectWise VPN
- ☐ Cyberoam VPN
- ☐ Fortinet VPN
- ☐ NetMotion Mobility VPN
- ☐ OpenVPN
- ☐ Palo Alto GlobalProtect VPN
- ☐ Pulse Connect / Ivanti / Juniper VPN
- ☐ RDWeb / Remote Web Access
- ☐ SonicWALL VPN
- ☐ Sophos Cyberoam Appliance
- ☐ Sophos SSL VPN
- ☐ WatchGuard VPN
- ☐ ZyXEL SSL VPN
- ☐ Other

If other, please provide details on vendor, makes, and models of appliances in use:

24. Does the **Applicant** use a Managed Service Provider (MSP)? *Optional*

- ☐ Yes
- ☐ No
- ☐ Unknown

If yes, please provide the name(s) of MSP in use:

Security Controls *Continued*

25. Which of the following Inbound Email Security products (i.e. Secure Email Gateway (SEG)) does the **Applicant** use, if any? *Optional*

- ☐ No SEG in place
- ☐ Appriver
- ☐ Avanan
- ☐ Barracuda
- ☐ Darktrace
- ☐ Datto
- ☐ Google
- ☐ Inky
- ☐ Intermedia
- ☐ Ironscales
- ☐ Microsoft Defender for O365
- ☐ Mimecast
- ☐ Perception Point
- ☐ Proofpoint
- ☐ Vade
- ☐ Other/Unknown

If other or unknown,please provide details:

26. Which of the following Endpoint Detection & Response (EDR) products does the **Applicant** use, if any? *Optional*

- ☐ No EDR in place
- ☐ CrowdStrike Falcon Insight EDR
- ☐ Cybereason Endpoint Detection and Response (EDR)
- ☐ Cycraft XSensor
- ☐ Cynet AutoXDR
- ☐ Fortinet FortiEDR
- ☐ Huntress EDR
- ☐ IBM Security QRadar EDR
- ☐ MalwareBytes Endpoint Detection and Response (EDR)
- ☐ Microsoft Defender for Endpoint (E5)
- ☐ Palo Alto Networks Cortex XDR
- ☐ SentinelOne Singularity EDR
- ☐ Symantec Endpoint Detection and Response (EDR)
- ☐ Trellix Endpoint Detection and Response (EDR)
- ☐ Other/Unknown

If other or unknown, please provide details:

Security Controls *Continued*

27. If applicable, how are the EDR solutions managed? *Optional*

- ☐ Managed 24/7 by a third-party provider (e.g. MSSP or external IT vendor)
- ☐ Managed 24/7 by in-house security team
- ☐ Managed within business hours by in-house security team
- ☐ Deployed but not actively monitored
- ☐ Unknown

If EDR solutions are “managed by a third-party provider”, please provide the name of the third-party vendor:

Media

28. Does the **Applicant** post content under license from a third party (Including copyrighted or trademarked materials or images) to its websites, social media accounts, or promotional materials.

- ☐ Yes
- ☐ No
- ☐ N/A

29. Does the **Applicant** have a process in place that includes legal review of content prior to publishing on its websites, social media accounts, or other promotional materials?

- ☐ Yes
- ☐ No
- ☐ N/A

Optional Please describe any additional steps the **Applicant** takes to avoid the posting of improper or infringing content.

Insurance

30. In the last three (3) years, has the **Applicant** experienced in excess of $10,000 any **Cyber Event**, **Loss** or been the subject of any **Claim** made for a **Wrongful Act** that would fall within the scope of the **Policy** for which the **Applicant** is applying?

☐ Yes
☐ No

If yes, please provide details including corrective actions taken and, if available, prior carrier loss runs.

31. Is the **Applicant** aware of any fact, circumstance, situation, event or **Wrongful Act** which reasonably could give rise to a **Cyber Event**, **Loss** or a **Claim** being made against them that would fall within the scope of the **Policy** for which the **Applicant** is applying?

☐ Yes
☐ No

If yes, please provide details:

Signatures

The undersigned authorized representative (the **Applicant's** Chief Executive Officer, Chief Financial Officer, Chief Security Officer, Chief Technology Officer, Chief Information Officer, Risk Manager, General Counsel, or any functionally equivalent positions, regardless of title) of the **Applicant** declares that to the best of their knowledge and belief, after reasonable inquiry, the statements set forth in this **Application**, are true and complete and may be relied upon by the insurer providing, and reviewing, this **Application** for insurance.

Authorized Representative Title*
Authorized Representative Name
Authorized Representative Email
Authorized Representative Signature
Today's Date (MM/DD/YY)

***Signature Requirements:** The **Applicant's** Chief Executive Officer, Chief Financial Officer, Chief Security Officer, Chief Technology Officer, Chief Information Officer, Risk Manager, General Counsel, or any functionally equivalent positions, regardless of title.

Security Contact Information

At-Bay Stance Platform and At-Bay Stance Advisory Services are included with your insurance policy as part of your Embedded Security Fee and corresponding endorsement. Please provide the contact details of at least one individual who is a full-time employee of **Applicant** and is authorized to receive security notifications and engage with the At-Bay Security team. You may additionally include contact details such as a managed IT/security provider or other internal inbox. For more information about Stance offerings, please visit at-bay.com/security.

Required - Primary Security Contact & Full-Time Employee of **Applicant**

Security Contact Name 01	
Email	Phone Number

Security Contact Information *Continued*

Optional - Additional Security Contact

Security Contact Name 02	
Email	Phone Number

Optional - Additional Security Contact

Security Contact Name 03	
Email	Phone Number

Fraud & Legal Notice(s), Warnings and Disclosure(s)

If the information in any **Application** changes prior to the inception date of the **Policy**, the **Applicant** will notify the insurer of such changes, and the insurer may modify or withdraw any outstanding quotation. The insurer is authorized to make inquiry in connection with this **Application**.

Should the insurer issue a **Policy**, **Applicant** agrees that such **Policy** is issued in reliance upon the truth of the statements and representations in the **Application** or incorporated by reference herein, and any misrepresentation, omission, concealment or otherwise shall be grounds for the rescission of any **Policy** issued.

Signing of this **Application** does not bind the **Applicant** or the insurer to complete the insurance, but it is agreed that this **Application** and any information incorporated by reference hereto, shall be the basis of the contract should a **Policy** be issued, and is incorporated into and is part of the **Policy**.

All written statements, materials or documents furnished to the insurer in conjunction with this **Application** are hereby incorporated by reference into this **Application** and made a part hereof, including without limitation, any supplemental applications or questionnaires.

FRAUD NOTICE TO ALABAMA APPLICANTS
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 RESTITUTION, FINES, OR CONFINEMENT IN PRISON, OR ANY COMBINATION THEREOF.

FRAUD 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.

FRAUD 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.

FRAUD 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 OF THE THIRD DEGREE.

Fraud & Legal Notice(s), Warnings and Disclosure(s) *Continued*

FRAUD NOTICE TO NEW JERSEY APPLICANTS
ANY PERSON WHO INCLUDES ANY FALSE OR MISLEADING INFORMATION ON AN APPLICATION FOR AN INSURANCE POLICY IS SUBJECT TO CRIMINAL AND CIVIL PENALTIES.

FRAUD 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 FIVE THOUSAND DOLLARS AND THE STATED VALUE OF THE CLAIM FOR EACH SUCH VIOLATION.

FRAUD NOTICE TO OHIO APPLICANTS
ANY PERSON WHO, WITH INTENT TO DEFRAUD OR KNOWING THAT HE IS FACILITATING A FRAUD AGAINST AN INSURER, SUBMITS AN APPLICATION OR FILES A CLAIM CONTAINING A FALSE OR DECEPTIVE STATEMENT IS GUILTY OF INSURANCE FRAUD

FRAUD 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.

FRAUD NOTICE TO OREGON 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 MAY BE GUILTY OF A CRIME AND MAY BE SUBJECT TO FINES AND CONFINEMENT IN PRISON.

FRAUD 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.

FRAUD NOTICE TO KENTUCKY 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 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 SUBJECTS SUCH PERSON TO CRIMINAL AND CIVIL PENALTIES. FRAUD 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. SUBJECT TO FINES AND CONFINEMENT IN PRISON

Fraud & Legal Notice(s), Warnings and Disclosure(s) *Continued*

FRAUD NOTICE TO ALL OTHER 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.

Voluntary Consent to Electronic Insurance Transaction

Voluntary consent to electronic insurance transaction. In an effort to streamline how you do business with us, we are providing you with the option of receiving information, documents, notices, records, acknowledgement and other materials relating to and governing your organization's relationship and transactions with At-Bay, electronically.

Applicant, or its representative authorized to sign on its behalf, hereby consents to receive and deliver information, **Policy** documents, notices, records, disclosures, acknowledgements, and other materials relating to and governing **Applicant's** insurance coverage, relationship, and transactions with At-Bay, electronically, to the e-mail account(s) provided to us in this **Application** (or any updated email account(s) policyholder may subsequently provide). **Applicant** understands that its consent is voluntary. **Applicant** understands it has the right to withdraw its consent, at any time, and to request a paper copy of described notices or documents by contacting At-Bay: (650) 850-8008 and/or EmailChanges@at-bay.com.

The delivery and presentation of the documents to **Applicant** by electronic means, rather than sending paper, does not affect the validity, legal effect, or enforceability of these insurance transactions or **Policy**-related documents.