at bay

Cyber

Ransomware Supplemental Application

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 "**Applican**t" 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 Ed.08/2018).

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

01. Please complete **Applicant** details.

Name of **Applicant**
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) $

Security

02. Who is managing the **Applicant**'s information technology? Select all that apply.

- ☐ Internal IT
- ☐ Managed Service Provider (MSP / MSSP)
- ☐ No dedicated IT team
- ☐ Other

If "MSP/MSSP", please provide details:

If "Other", please provide details:

03. Who is managing the **Applicant**'s IT security (e.g., patch and configuration management, security monitoring, etc.)? Select all that apply.

- ☐ Internal IT/Security Team
  - ☐ Security monitoring occurs continuously (i.e. 24/7, weekends and holidays included)
  - ☐ Security monitoring occurs continuously during business hours (i.e. Mon-Fri, 8 AM - 5 PM)
- ☐ IT security is outsourced to an MSP that provides security services (e.g., Managed Detection and Response (MDR)
- ☐ No dedicated IT team or security

If utilizing MSP / MDR please identify vendor:

04. If all or part of the **Applicant**'s IT security is outsourced, what functions do outside provider(s) manage?

- ☐ Endpoint protection (e.g., Endpoint Detection and Response (EDR), etc.)
- ☐ Security monitoring (e.g., endpoint and/or network monitoring for malicious activity)
- ☐ Incident response
- ☐ Vulnerability management (e.g., patch and configuration management)
- ☐ Identity and access management (e.g., provisioning of user accounts and privileges, multi-factor authentication, etc.)
- ☐ Email security (e.g., investigation of phishing emails, etc.)
- ☐ Other (please list)

Please provide additional details:

05. Please describe the **Applicant**'s IT architecture.

- ☐ Exclusively on-premises
- ☐ Hybrid on-premises/cloud
- ☐ Cloud native with minimal or no on-premises systems (i.e. exclusive of employee workstations)

06. How is patch management handled for **Applicant's** IT environment?

- ☐ No formal patch management program
- ☐ Patches management is ad hoc with updates applied when the IT staff has time
- ☐ Patches are deployed manually by the IT staff on a defined schedule
- ☐ Patch management is automated with updates deployed when they become available

07. What is the **Applicant**'s timeframe for installing critical and high severity patches across the organization?

- ☐ Automated / Continuous
- ☐ Within 1 week
- ☐ Within 1 month
- ☐ Beyond 1 month

Please provide additional details:

08. Does the insured utilize a Security Information and Event Management solution (SIEM)? If Yes, what percentage of critical assets are being ingested into the solution?

- ☐ Yes
  - ☐ 90-100%
  - ☐ 75-90%
  - ☐ < 75%
- ☐ No

Access Management and Password

09. Does the **Applicant** use an identity provider / Single Sign-On (SSO) solution?

- ☐ Yes
- ☐ No
- ☐ Partially

Please specify product and/or deployment of identity provider / Single Sign-On (SSO) solution:

10. Please indicate where multifactor authentication (MFA) is being deployed (select all that apply).

- ☐ Remote Access (including VPNs)
- ☐ Email Access
- ☐ Critical Information / vital assets inside the network
- ☐ Privileged and administration accounts
- ☐ Independent Contractors and vendors
  - ☐ Accessing remotely
  - ☐ Accessing sensitive information / cloud / web applications

Please provide any applicable details:

11. How does the **Applicant** control privileged access for employee workstations?

- ☐ All employees have administrator privileges on their respective workstations
- ☐ Administrator privileges for employee workstations are available for IT members only (one set of credentials for both administrative and non administrative tasks)
- ☐ Administrator privileges for employee workstations are available for IT members only (separate credentials for administrative and non administrative tasks)

12. Please describe the **Applicant's** usage of Privileged Access Management (PAM) solution(s).

- ☐ Applicant does not use a PAM solution
- ☐ Applicant uses a PAM solution to control access to credentials for privileged accounts (e.g., domain administrator, database administrator, etc.)
- ☐ Applicant uses a PAM solution to control access to credentials for privileged accounts and also to monitor usage of privileges (e.g., deploying group policy settings, adding user accounts, etc.) in the IT environment

Network Security

13. What network security technology does the **Applicant** have in place? Select all that apply and list all applicable vendors.

☐ Traditional / Next-Gen Firewall

☐ Intrusion Detection / Prevention System

☐ Secure Web Gateway / Web Proxy / Network Filtering

☐ Other network security

Endpoint Security

14. What Endpoint Security solutions (e.g., EDR, antivirus, etc.) does the **Applicant** have in place? Select all that apply.

☐ BitDefender
☐ CarbonBlack
☐ Check Point Harmony Endpoint Protection
☐ CrowdStrike
☐ Cybereason
☐ Cycraft
☐ Cylance
☐ Cynet
☐ ESET
☐ FortiEDR
☐ Kaspersky
☐ Malwarebytes
☐ McAfee
☐ Microsoft Defender (standard)
☐ Microsoft Defender for Endpoint (enterprise)
☐ Palo Alto Cortex
☐ XDR Agent
☐ SentinelOne
☐ Sophos
☐ Symantec
☐ Trend Micro
☐ Trellix (formerly FireEye) Webroot
☐ Other

If Other, please provide details:

15. Describe the deployment of the **Applicant's** endpoint security solution(s) in the environment:

- ☐ No endpoint security solution
- ☐ Endpoint security solution deployed to some workstations but not others
- ☐ Endpoint security solution deployed to substantially all servers but not workstations
- ☐ Endpoint security solution deployed to substantially all workstations but not servers
- ☐ Endpoint security solution deployed to substantially all workstations and servers
- ☐ Multiple endpoint security solutions are deployed to maximize coverage across workstations and servers

16. Please describe the status of any End of Life hardware / software within the **Applicant's** environment (Select all that apply):

- ☐ No end of life hardware / software exists
- ☐ End of Life Hardware of Software does exist, however extended support is purchased where applicable
- ☐ End of Life Hardware or Software does exist, but is segmented from the network
- ☐ End of Life Hardware or Software does exist, but is not accessible via the internet

Please provide additional details:

Remote Access

17. If applicable, please choose which solutions the **Applicant** uses to enable remote access to its network (Select all that apply):

- ☐ Remote Desktop Protocol (RDP)

Please provide details:

- ☐ Virtual Private Network (VPN) solution including VPN solutions that are included as a feature on other devices (e.g. Fortinet VPN, Palo Alto Networks Global Protect, Cisco VPN using Cisco ASA or FTD)

Please provide details:

If applicable, how is the VPN infrastructure hosted?

- ☐ 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)

☐ Remote access software - RMM software (e.g. Citrix, N-Able, NinjaOne)

Please provide details:

☐ Remote access software - SASE / Zero Trust Network Access (e.g. Cato, ZScaler, Palo Alto Networks Prisma Access)

Please provide details:

☐ Other remote access solutions (e.g., TeamViewer, Splashtop, VNC, etc.)

Please provide details:

Operational Technology

18. Please describe the **Applicant**'s usage of Operational Technology (OT).

☐ Applicant does not use OT
☐ Applicant uses OT, and OT is on the same logical network as IT assets
☐ Applicant uses OT, and OT is on a separate logical network as IT assets (i.e. network segmentation enforced between IT and OT environments using firewalls / routers, VLANs, etc.)
☐ Applicant uses OT, and OT is on a separate physical network from IT assets (i.e. no direct connectivity is possible between IT and OT environments)

19. If applicable, please describe any remote access to the **Applicant**'s OT networks from the Internet.

☐ Remote access to OT networks is not available from the Internet
☐ Remote access to OT networks is available from the Internet, and users are required to authenticate with a username and password
☐ Remote access to OT networks is available from the Internet, and users are required to authenticate using multiple factors (i.e. MFA is enforced)

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