

Ransomware Supplemental Application

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 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
Applicant's primary industry
Applicant's primary website and email domains
Applicant's annual revenue (Most recently completed fiscal year) \$

Security

02. Who is managing the **Applicant's** network infrastructure? (Select all that apply)

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

Please provide details

Please provide details

Security *Continued*

03. Who is managing the **Applicant's** security? (Select all that apply)

Internal IT

No dedicated IT team or security team

Internal security team

Other

Managed Detection and Response (MDR)
or an external SOC provider

Please provide details

Please provide details

Managed Service Provider (MSP / MSSP)

Please provide details

04. If an MDR product is in use, is third party intervention allowed or is prior consent required?

Yes

No

If no, please provide additional details

05. If an MDR product is in use, does the provider have 24/7 visibility across all endpoints and critical network activity?

Yes

No

If no, please provide additional details

06. Please describe the **Applicant's** workload infrastructure.

Exclusively on-premises

Mostly cloud-based, with minimal or no on-premises

Hybrid on-premises/cloud

Security *Continued*

07. Please describe where the **Applicant's** workstations (e.g. laptops and desktops) are accessed.

Office only

Off premises (e.g. Employees homes)

Hybrid

08. Does the **Applicant** have a central patch management solution for the endpoints on its network?

Yes

No

09. 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

Access Management and Passwords

10. Does the **Applicant** enforce Single Sign-On (SSO) for all users?

Yes

No

Partially

Please specify product and/or deployment

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

Yes

No

Partially

If partially enforced, please describe

Access Management and Passwords *Continued*

12. Do you use a password manager software tool (e.g. 1password, Bitwarden)?

Yes

No

If yes, please specify product

If yes, is the password management automated and/or enforced for all users?.

Yes

No

If no, please specify

13. Does the **Applicant** permit end users administrator rights on their endpoints?

Yes

No

14. Does the **Applicant** have a Privileged Access Management (PAM) solution in place to control and monitor access to privileged accounts within the **Applicant's** organization?

Yes

No

If yes, please specify provider name

Network Security

15. 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

No network security in place

Endpoint Security

16. What Endpoint Security Technology does the **Applicant** have in place? (Select all that apply)

BitDefender

Kaspersky

Symantec

CarbonBlack

Malwarebytes

Trend Micro

Check Point Harmony
Endpoint Protection

McAfee

Trellix (formerly FireEye)

CrowdStrike

Microsoft Defender
(standard)

Webroot

Cybereason

Microsoft Defender for
Endpoint (enterprise)

Other

Cyrcraft

Palo Alto Cortex
XDR Agent

Please provide details.

Cylance

Cynet

SentinelOne

ESET

Sophos

FortiEDR

Endpoint Security *Continued*

17. If applicable, is the **Applicant's** EPP / EDR deployed on all domain controllers?

Yes

No

Remote Access

18. Does the **Applicant** allow remote access to its network?

Yes

No

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

Yes

No

20. If applicable, please choose which solutions the **Applicant** uses to secure all remote access activity to its network? *(Select all that apply)*

Remote Desktop Protocol (RDP)

Please describe measures to secure RDP

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

Please provide details

Virtual Private Network (VPN) Gateway
(e.g. Fortinet VPN, Palo Alto Networks
Global Protect, Cisco VPN using Cisco
ASA or FTD)

Please provide details

Remote access software - Zero Trust
Network Access (e.g. Cato, ZScale, Palo
Alto Networks Prisma)

Please provide details

Other remote access solution

Please provide details

Operational Technology

21. Does the **Applicant** utilize Operational Technology?

Yes

No

If yes, are IT and OT networks segregated from one another?

Yes

No

If yes, are OT networks remotely accessible via the internet?

Yes

No

If yes, is MFA enforced for all users attempting to remotely access the OT environment?

Yes

No

Signature

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.

* **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.

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