CORGI INSURANCE

CYBER INSURANCE POLICY

NAMED INSURED

Beagle Logistics LLC

POLICY PERIOD

January 1, 2026 - January 1, 2027

CORGI INSURANCE
100 Market Street
San Francisco, CA 94105

POLICY NO. COR-2026-CYB-0001

Cyber Insurance Policy

NOTICE: THIS POLICY CONTAINS ONE OR MORE COVERAGES. CERTAIN COVERAGES ARE LIMITED TO LIABILITY FOR CLAIMS FIRST MADE AGAINST THE INSURED AND REPORTED TO THE INSURER DURING THE POLICY PERIOD AS REQUIRED BY THIS POLICY. CLAIM EXPENSES SHALL REDUCE THE APPLICABLE LIMITS OF LIABILITY AND ARE SUBJECT TO THE APPLICABLE RETENTION(S). PLEASE READ THIS POLICY CAREFULLY.

POLICY DECLARATIONS

ITEM 1. **NAME INSURED** Beagle Logistics LLC

ADDRESS 310 W Bearcat Dr, South Salt Lake, UT 84115

ITEM 2. **POLICY PERIOD** From: January 1, 2026
To: January 1, 2027
12:01 A.M. Local Time at the address shown in Item 1.

ITEM 3. **POLICY LIMITS OF LIABILITY AND COVERAGES PURCHASED**

A. Aggregate Limit of Liability: $3,000,000 (Aggregate for all Claims, Losses, and Claim Expenses arising under this Policy during the Policy Period.)

B. The following Coverages are subject to the applicable Per Claim Limits and Aggregate Limits shown below. Unless otherwise stated, Claim Expenses are included within and reduce the applicable Limits of Liability.

COVERAGE	PER CLAIM SUBLIMIT OF LIABILITY INCLUDES CLAIM EXPENSES	AGGREGATE SUBLIMIT OF LIABILITY
Privacy Liability	$1,000,000	$1,000,000

Data Breach Response	$1,000,000	$1,000,000
Network Security Liability	$1,000,000	$1,000,000
Business Interruption	$1,000,000	$1,000,000
Cyber Extortion	$500,000	$500,000
Digital Asset Restoration	$500,000	$500,000
Regulatory Defense Coverage	$250,000	$250,000
Social Engineering Fraud	$250,000	$250,000

ITEM 4. RETENTION (INCLUDING CLAIM EXPENSES) All Coverages: $10,000 Each Claim
Business Interruption: 12-Hour Waiting Period

ITEM 5. ANNUAL PREMIUM $8,500 (or $9,250)

ITEM 6. TERRITORIAL LIMITS Worldwide

ITEM 7. SECURITY REQUIREMENTS As a condition of coverage, the Named Insured shall maintain:
- Multi-Factor Authentication (MFA)
- Endpoint Detection and Response (EDR)
- Encrypted Backups
- Security Awareness Training
- Incident Response Procedures

ITEM 8. NOTICE OF CLAIM The Insured shall provide written notice of any Claim, Security Failure, Privacy Event,or Cyber Event as soon as practicable and no than thirty (30) days after discovery.

I. DEFINITIONS

A. "Claim" means:
1. A written demand for monetary damages or other relief;
2. A civil, administrative, or regulatory proceeding commenced by the service of a complaint, notice of charges, or similar pleading;
3. An arbitration proceeding; or
4. A formal regulatory investigation arising from a covered Cyber Event.

B. "Claim Expenses" means reasonable and necessary legal fees, expert fees, forensic expenses, investigation costs, and other expenses incurred in the defense, investigation, adjustment, or settlement of a Claim

C. “Computer System" means any computer, server, network, cloud environment, application, endpoint device, software, or information technology resource owned, leased, operated, or used by the Insured.

D. “Cyber Event” means a Security Failure, Privacy Event, ransomware attack, malware infection, denial-of-service attack, unauthorized access, or compromise of a Computer System.

E. “Data Breach Response Costs” means reasonable and necessary costs incurred by the Insured to investigate, contain, respond to, and remediate a Privacy Event, including forensic services, legal counsel, notification expenses, call center services, and credit monitoring.

F. “Insured" means the Named Insured identified in the Declarations and its directors, officers, employees, and authorized representatives acting within the scope of their duties.

G. “Loss” means damages, settlements, judgments, Claim Expenses, breach response costs, forensic costs, cyber extortion payments, and other amounts covered under this Policy. Loss does not include fines, penalties, taxes, or matters deemed uninsurable under applicable law.

H. "Ransomware Event" means the encryption, restriction, or denial of access to a Computer System, Digital Asset, or data by malicious software, accompanied by a demand for payment or other consideration.

I. “Personal Information” means information that identifies or can reasonably identify an individual, including names, addresses, email addresses, government-issued identification numbers, financial account information, payment card information, and protected health information.

J. “Privacy Event” means the unauthorized access to, disclosure of, loss of, theft of, or misuse of Personal Information.

K. “Security Failure” means the failure of security controls resulting in unauthorized access, malware infection, ransomware deployment, denial of service, or compromise of a Computer System.

L. “Social Engineering Fraud” means the intentional deception of an employee through fraudulent communications designed to induce the transfer of money, securities, or confidential information.

M. "Digital Assets" means data, software, electronic records, databases, applications, and digital content stored on or accessible through a Computer System

NOTICE: THIS POLICY APPLIES TO CLAIMS FIRST MADE AGAINST THE INSURED AND REPORTED TO THE INSURER DURING THE POLICY PERIOD, SUBJECT TO THE TERMS, CONDITIONS, LIMITS OF LIABILITY, RETENTIONS, AND EXCLUSIONS SET FORTH HEREIN. TERMS APPEARING IN QUOTATION MARKS HAVE SPECIAL MEANINGS AS DEFINED IN THIS POLICY. PLEASE READ THIS POLICY CAREFULLY.

Ⅱ. COVERAGES

A. PRIVACY LIABILITY COVERAGE

"We" shall pay on behalf of the "Insured" all "Loss" and "Claim Expenses" that the "Insured" becomes legally obligated to pay in excess of the applicable Retention resulting from a "Claim" first made against the "Insured" during the Policy Period and reported to "Us" in accordance with this Policy, arising out of a "Privacy Event."

B. DATA BREACH RESPONSE COVERAGE

"We" shall pay on behalf of the "Insured" all "Data Breach Response Costs" incurred in excess of the applicable Retention as a result of a "Privacy Event" first discovered during the Policy Period and reported to "Us" in accordance with this Policy, including reasonable forensic investigation expenses, legal counsel fees, notification expenses, call center services, and credit monitoring services incurred in response to such "Privacy Event."

C. NETWORK SECURITY LIABILITY COVERAGE

"We" shall pay on behalf of the "Insured" all "Loss" and "Claim Expenses" that the "Insured" becomes legally obligated to pay in excess of the applicable Retention resulting from a "Claim" first made against the "Insured" during the Policy Period and reported to "Us" in accordance with this Policy, arising out of a "Security Failure."

D. BUSINESS INTERRUPTION COVERAGE

"We" shall pay on behalf of the "Insured" all "Loss" resulting from the necessary interruption of business operations caused by a covered "Cyber Event" affecting a "Computer System" during the Policy Period, in excess of the applicable Retention and subject to the applicable waiting period shown in the Declarations.

E. CYBER EXTORTION COVERAGE

"We" shall pay on behalf of the "Insured" all "Loss" incurred as a result of a "Ransomware Event" or other cyber extortion threat first discovered during the Policy Period and reported to "Us" in accordance with this Policy, including extortion payments, negotiation expenses, forensic services, and other reasonable costs incurred to respond to such event.

F. DIGITAL ASSET RESTORATION COVERAGE

"We" shall pay on behalf of the "Insured" all reasonable and necessary costs incurred to restore, recreate, recover, replace, or recollect "Digital Assets" damaged, destroyed, altered, corrupted, deleted, or encrypted as a result of a covered "Cyber Event" first discovered during the Policy Period and reported to "Us" in accordance with this Policy.

G. REGULATORY DEFENSE COVERAGE

"We" shall pay on behalf of the "Insured" all "Loss" and "Claim Expenses" incurred in connection with a regulatory proceeding arising from a covered "Privacy Event" or "Security Failure" first discovered during the Policy Period and reported to "Us" in accordance with this Policy, including reasonable legal defense costs and regulatory response expenses, to the extent insurable under applicable law.

H. SOCIAL ENGINEERING FRAUD COVERAGE

"We" shall pay on behalf of the "Insured" all direct financial loss resulting from a "Social Engineering Fraud" event first discovered during the Policy Period and reported to "Us" in accordance with this Policy, where an employee is intentionally deceived into transferring money, securities, or other financial assets based upon fraudulent instructions believed to be genuine.

Ⅲ. EXCLUSIONS

The coverage under this Policy shall not apply to any "Loss", "Claim Expenses", "Data Breach Response Costs", or other amounts arising out of or resulting, directly or indirectly, from:

A. Any "Cyber Event", "Privacy Event", "Security Failure", "Claim", or circumstance known to the "Insured" before the inception of this Policy.

B. Any fraudulent, dishonest, criminal, or intentionally wrongful act committed by the "Insured's" directors, officers, or executives.

C. Bodily injury, death, emotional distress, or damage to tangible property, except to the extent expressly covered under Digital Asset Restoration Coverage.

D. Liability assumed solely under a contract or agreement, unless such liability would have existed in the absence of the contract.

E. War, invasion, military action, cyber warfare, terrorism, or state-sponsored cyber operations.

F. Failure to maintain the minimum security requirements identified in the Declarations Page.

G. The knowing or intentional collection, use, sale, disclosure, or processing of "Personal Information" in violation of applicable law.

H. Fines, penalties, taxes, or amounts deemed uninsurable under applicable law.

I. Pollution, contamination, radioactive materials, or nuclear incidents.

Ⅳ. TERMS AND CONDITIONS

A. NOTICE OF CLAIM OR CIRCUMSTANCE THAT MAY LEAD TO A CLAIM

The "Insured" shall provide written notice to "Us" of any "Claim", "Cyber Event", "Privacy Event", or "Security Failure" as soon as practicable and no later than thirty (30) days after discovery.

The notice shall include, to the extent reasonably available:

1. A description of the event or circumstance;
2. The date the event was discovered;
3. The systems, data, or individuals affected; and
4. Any known or anticipated financial impact.

B. ASSISTANCE AND COOPERATION

The "Insured" shall provide all reasonable assistance and cooperation requested by "Us" in connection with the investigation, defense, settlement, and resolution of any "Claim", "Cyber Event", "Privacy Event", or "Security Failure" that may give rise to coverage under this Policy.

Such assistance shall include providing relevant records, documents, system logs, electronic data, and other information reasonably requested by "Us".

C. MITIGATION OF LOSS

The "Insured" shall take reasonable steps to prevent, mitigate, and minimize any "Loss" arising from a covered event, including preserving evidence, securing affected systems, and maintaining backup data where feasible.

D. OTHER INSURANCE

This Policy shall apply in excess of any other valid and collectible insurance available to the "Insured", unless such insurance is specifically written to apply in excess of this Policy.

E. SUBROGATION

In the event of any payment under this Policy, "We" shall be subrogated to all rights of recovery available to the "Insured" against any person or entity responsible for the covered "Loss". The "Insured" shall execute all documents and provide all reasonable assistance necessary to secure such rights.

F. ASSIGNMENT

No assignment of rights or interests under this Policy shall be valid without the prior written consent of "Us", except in connection with a merger, acquisition, or other corporate reorganization approved by "Us".

G. TERRITORY

Coverage under this Policy shall apply on a worldwide basis, subject to applicable law and the terms and conditions of this Policy.

Ⅴ. CLAIMS REPORTING PROCEDURE

In the event of a suspected "Cyber Event", "Privacy Event", "Security Failure", or "Claim", the "Insured" shall follow the procedures below:

1. **Incident Identification**

   Identify and document the suspected event, including affected systems, data, business operations, and individuals, if applicable.

2. **Immediate Mitigation**

   Take reasonable steps to contain and mitigate the event, preserve evidence, and prevent further damage.

3. **Notice of Claim**

   Provide written notice to "Us" in accordance with the Notice of Claim provisions contained in this Policy.

4. **Investigation**

   Cooperate with forensic investigators, legal counsel, claims professionals, and other parties reasonably assigned by "Us" to investigate the event.

5. **Remediation and Recovery**

   Implement corrective actions, restore affected systems, recover "Digital Assets", and address any identified vulnerabilities.

6. **Coverage Determination and Claim Resolution**

   Following completion of the investigation and coverage determination, covered amounts shall be paid in accordance with the terms, conditions, retentions, and limits of this Policy.