CORVUS

Application-free renewals from Corvus

Overview and Frequently Asked Questions

What's in this document

How it works PAGE 1

What is considered to be a material change PAGE 2

Biometric Information Subjectivity PAGE 3

Social Engineering and Cyber Crime Sublimit PAGE 3

Additional Definitions PAGE 4

Overview

Application-free renewals from Corvus do not require an application to receive bindable terms!

Step 1: To confirm their eligibility each account must meet the following requirements, which will be sent to you by email 90 days in advance of the renewal effective date:

1. The insured's revenues are either under $5M or if greater than $5M, they have not increased by more than 20% over the prior rated revenues. (Prior rated revenues will be included in the email).
2. Confirmation that the insured has reported all matters they have knowledge of that have or could potentially give rise to a claim or incident.
3. Confirmation that the insured does not collect, capture, purchase, receive through trade, or otherwise obtain biometric identifiers or biometric information.

©2024 Corvus Insurance Holdings Inc.

For risks that do not meet all of the requirements above, please reach out to your Corvus Underwriter, who may provide a quote contemplating any material changes.

Step 2: At 45 days prior to the renewal effective date, qualified renewals are provided with a bindable quote and the option to bind with a few clicks. Subject to our underwriting guidelines, the quoted terms, conditions, and premium will be provided with three (3) post-bind contingencies that are required before the policy may be issued.

1. A TRIA Waiver (included in the quote letter if TRIA coverage is rejected).
2. A Completed Surplus Lines Certificate (included in the quote letter).
3. Confirmation that the insured does not collect, capture, purchase, receive through trade, or otherwise obtain biometric identifiers or biometric information.

Upon receipt of instruction to bind, a formal binder will be issued. The policy will be issued thereafter once all post-binding subjectivities have been satisfied.

FAQ

What is considered to be a material change in exposure that would exclude an insured from eligibility for an application-free renewal?

A material change is considered when an Insured has either exceeded $25M in revenue or an Insured with revenue in excess of $5M has experienced an increase in revenue greater than 20% from the prior rated revenue. The prior rated revenue will be confirmed on both the renewal solicitation notification (90 days from the renewal effective date) and the quote letter email (45 days from the renewal effective date) to enable the Insured to compare their projected revenues for the next 12 months against the prior rated revenue figure.

The prior rated revenue figure will remain unchanged year-over-year as the rating base to allow the Insured to remain eligible for an application-free renewal, unless the Insured has a material change as described above.

Another example of a material change is if the Insured has knowledge of a matter that has or could potentially give rise to a claim or incident. Any such matter must be reported as soon as practicable to our claims team and to the Corvus Underwriter prior to 45 days from the renewal effective date, per the reporting instructions in the current policy.

©2024 Corvus Insurance Holdings Inc.

Finally, insureds that collect biometric information are another example of what is considered to be a material change. As noted above (in Step 1), please reach out to your Corvus Underwriter, who may provide a quote contemplating any material changes.

FAQ

Why is there a post-bind subjectivity for the collection of Biometric Information, and why is this viewed as a material change in exposure? What does it mean for insured's that have collected or continue to collect Biometric Information?

Due to an increase in claims (specifically class action matters) being filed for violations of the collection of biometric information, we are underwriting to this specific exposure. Unlike many competitors that have taken the position to completely exclude this from coverage, Corvus is continuing to provide coverage on a risk-by-risk basis if biometric information is either not collected or the required legal review occurs including policies & procedures for compliantly collecting, disclosing, retaining and destroying such information.

To effectively underwrite to this exposure as part of an application-free renewal we are including a post-bind contingency, and we are sharing a copy of the potential exclusion to be applied at policy issuance. Even when the exclusion is added at issuance, it will not apply to otherwise covered Loss resulting from a Security Breach or accidental release, unauthorized disclosure, loss, theft or misappropriation of protected personal information or Biometric Data covered under First Party Insuring Agreements.

If insureds do not have the required controls to ensure compliance (required controls meaning biometric information is either not collected or the necessary legal review occurs including of policies and procedures for compliantly collecting, disclosing, retaining and destroying such information) in place at the time of renewal, once they are implemented we can look at removing the exclusion mid-term with written confirmation of implementation and a current no known loss letter.

FAQ

Can the insured's Social Engineering and Cyber Crime limit be increased to $250k?

Below are the controls that must be confirmed by the Insured for us to consider increasing the Social Engineering and Cyber Crime sublimit to $250k for a potential additional premium:

©2024 Corvus Insurance Holdings Inc.

Controls to be confirmed:

1. Utilization of an email filtering solution.
2. Requirement of an out-of-band authentication prior to executing an electronic payment. (Out of band authentication is a secondary verification method with the requester of a funds transfer through a communication channel separate from the original request.)
3. Social engineering and phishing training for all employees at least annually.

   Training resources are available to our insureds:

   KnowBe4 — Discount can be found at **this link** and Free tools can be found at **this link.**

   Wizer — Free version can be found at **this link.**

4. Multi-factor authentication (MFA) in place for access to email.

   Moxfive — Assistance with MFA can be found at **this link.**

Increased sublimit is not available for the following classes of business: Banking/Finance/Funds Transfer, Credit Unions, Title and Escrow Agents, Loan Servicing/Mortgage Brokers, Financial and Investment Advisors, PE Firms, Grant Making/Scholarships, Employee Benefits, and Payroll Companies.

Additional Definitions

Segregated backups

Segregated backups are a strategic backup approach to secure a separate copy of backup data, with the goal of having a protected backup copy that will not be impacted by a ransomware attack. Segregated backups are not accessible through the insured's primary network/infrastructure and can include cloud backups, air gapped or immutable backups, tape backups that are disconnected at least each night or managed backup-as-a-service (BaaS) solutions. For more information, please visit **this link.**

Email filtering

Email filtering software is used to monitor inbound and outbound emails to prevent spam, phishing or malicious emails. Well-known vendors in this space include Mimecast, Proofpoint, and Barracuda. For more information, please visit **this link.**

©2024 Corvus Insurance Holdings Inc.

Out-of-band authentication	Out-of-band authentication is a verification process in which a transaction (wire transfer, electronic funds transfer, etc.) initiated via one delivery channel (email) must be verified via an alternative and independent delivery channel (phone) in order for the transaction to be completed. For example, calling the requestor/initiator at a previously verified phone number prior to making a payment or transferring funds. For more information, please visit **this link.**
Social engineering and phishing training	Social engineering & phishing training is a specific type of security awareness training that focuses on recognizing phishing/smishing/ spoofing emails, texts, phone calls, etc. and what people should do when they encounter them. Bad actors are constantly crafting new ways to get inside the infrastructure or network of their targets, and ensuring that personnel are trained, aware and actively looking out for these malicious attempts to perform nefarious activity will put the company in a better position to fight off intruders. For more information, please visit **this link.**
Multi-Factor Authentication (MFA)	Multi-Factor Authentication (MFA) is an authentication method that requires the user to provide two or more credentials in order to gain access to an application or system. Credentials may include something you know (a password/ username), something you have (smartphone or secure USB key), and/or something you are (biometrics such as fingerprint). For more information, please visit **this link.**
Biometric Data	Biometric data is any information relating to physical, physiological or behavioral characteristics that can be used to identify individuals, including but not limited to retina or iris scans, fingerprints, voiceprints, scans of hand or face geometry, genetic markers, or genetic testing.
Personally Identifiable Information (PII)?	PII is any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. This includes, but is not limited to; social security number, medical service or healthcare data, driver's license or state identification number, account, credit card, or debit card number.

This content is intended for general guidance and informational purposes only. This content is under no circumstances intended to be used or considered as specific insurance or information security advice. This content is not to be considered an objective or independent explanation of the matters contained herein. Corvus® reserves the right to change terms, eligibility, or availability of the Fly by Renewal process in our sole discretion. Policy quotes, terms and conditions, and premiums are made in accordance with Corvus® Insurance's underwriting guidelines. The policy, not general descriptions or material within this material, will form the contract between the insured and our insurance carrier partners. Coverage may not be available in all jurisdictions.

©2024 Corvus Insurance Holdings Inc.