**VOLUNTARY AGENT/BROKER DATA SECURITY QUESTIONAIRRE**

**Overview**

Third party due diligence is an important element of an overall cybersecurity program and should be conducted in a manner consistent with the risk appetite of each company. Many factors can affect the level of due diligence that a company undertakes when assessing the cybersecurity framework of any third party, particularly its agents or brokers, including: the jurisdiction that the agent or broker operates in; the size of the agent, the quantity and type of information they have access to, and the connectivity to each insurer. The importance of each factor in determining the diligence protocol may differ by carrier.

Nevertheless, it can be overwhelming for an agent or broker with multiple carrier relationships to receive numerous questionnaires that ask similar assessment questions. Therefore, we prepared the attached questionnaire to assist agents and brokers to prepare for carrier questionnaires. Carriers may consider using the questionnaire as drafted, as a basis for their own template questionnaire, or may amend the questionnaire to suit its specific requirements.

Additionally, this questionnaire is only one tool available in the overall assessment process. Some carriers may request System & Organization Controls (SOC) reports when available as a starting point. These documents may already be available and can provide insight into the type of controls and testing that an entity has in place. The SOC reports may not be the final step in the due diligence process but may identify whether a security questionnaire, specifically tailored or similar to the one provided here, is necessary.

Importantly, this is only a list of voluntary questions that a carrier may ask. Each individual carrier should assess the response to each question and determine the appropriate follow-up and corporate decisions to be made based on the responses. Nothing in this document should be interpreted as providing legal or risk mitigation advice, identifying cybersecurity best practices, or specifying carrier requirements.

Finally, the focus of this questionnaire is on data security, however, increasingly carriers are taking a holistic approach to third-party assessments and may incorporate additional questions related to issues such as business continuity.

**Disclaimer**

The following Cybersecurity Questionnaire has been published as of [Insert date] regarding the subject matter covered. Users taking any action based on such information should seek the advice of a competent professional taking into consideration the facts and circumstances of the user of the Cybersecurity Questionnaire. It is made available with the understanding that American Property Casualty Insurance Association (“APCIA”) is not engaged in rendering legal, risk assessment, insurance compliance, tax, accounting advice, or any other professional services. APCIA expressly disclaims all and any liability and responsibility to any user (whether a person or legal entity recipient or purchaser) of this Cybersecurity Questionnaire, in respect of anything and of the consequences of anything, done or omitted by any such user in reliance upon the whole or any part of the contents of this Cybersecurity Questionnaire.

While every effort has been made to ensure the following information is accurate, this Cybersecurity Questionnaire is offered only as a general template and may require further research. This document shall not serve as a legal opinion. APCIA assumes no responsibility for consequences resulting from the use of the information, errors or omissions, herein or in any respect for the content of such information. APCIA is not responsible for, and expressly disclaims all liability for, damages of any kind arising out of use, reference to, or reliance on such information.

Transmission or reproduction of the Cybersecurity Questionnaire for commercial purposes or for distribution as legal or risk assessment advice is strictly prohibited. Non-commercial transmission or reproduction for limited, internal use must include this complete disclaimer.