THIRD PARTY SERVICE PROVIDER QUESTIONNAIRE

Entity
Name & Title of Organizations Senior Officer:
Name of Organizations Cybersecurity/Technology Contact: Email: Phone:

Do you comply with any existing published cyber/data security standards? Is so, select all that apply.

- ☐ ISO/IEC family of standards (International Organization for Standardization)
- ☐ SOC2/3 and /or SOC for cybersecurity (method to keep data secure)
- ☐ NIST 7621r1 (small business information security fundamentals)
- ☐ NIST CSF (government cybersecurity framework)
- ☐ OWASP (Open Web Application Security Project)
- ☐ GDPR (European data protection regulation)
- ☐ Other _____

Have you undergone a cybersecurity vulnerability audit? Is so, when and by whom? _____	☐ Yes ☐ No
Do you encrypt data in transit? If so, what encryption tool/technology is used? _____	☐ Yes ☐ No
Do you encrypt data at rest? If so, what encryption tool/technology is used? _____	☐ Yes ☐ No
Do you employ access controls and policies designed to limit access to relevant information systems and Non-public information[1]? If yes, please describe: _____ _____ _____	☐ Yes ☐ No
Do you use multi-factor authentication to protect against unauthorized access to your Non-public information?	☐ Yes ☐ No

Do you have policies and procedures in place to notify our organization in the event of a cybersecurity event[2] directly impacting our information systems of non-public information? If yes, briefly describe: _____ _____ _____	◯ Yes ◯ No
Do you have procedures in place to respond to service disruptions resulting from natural disasters, human error, or intentional physical or cyber-attacks? If so, briefly describe: _____ _____	◯ Yes ◯ No
Do you understand and agree that the performance of services from you/your entity for our organization are subject to examination and oversight of the SC Department of Insurance?	◯ Yes ◯ No
I hereby attest that the above is true and accurate to the best of my knowledge	◯ Yes ◯ No

Name & Title of person completing form:	
Signature:	Date:

Disclaimer: This questionnaire is to be used solely as a tool to assist agencies in assessing the third party service providers they work with. It is not a substitute for agencies independently evaluating any business, legal or other issues, and is not a recommendation that a particular course of action be adopted. Agencies should read and follow all requirements set forth in the SC Insurance Data Security Act and all other applicable state/federal laws in the jurisdictions in which they do business. This questionnaire does not imply compliance with state/federal laws nor does it constitute legal advice.

[1] **Non-public information**: means information that is *not publicly available* information and is: (a) business-related information of a licensee the tampering with which, or unauthorized disclosure, access, or use of which, would cause a material adverse impact to the business, operations, or security of the licensee; (b) any information concerning a consumer which because of name, number, personal mark, or other identifier can be used to identify such consumer*, in combination with any one or more of the following data elements* (i) social security number; (ii) driver's license number or nondriver identification card number; (iii) account number, credit or debit card number; (iv) security code, access code, or password that would permit access to a consumer's financial account; or (v) biometric records; (c) any information or data, except age or gender, in any form or medium created by or derived from a health care provider or a consumer and that relates to: (i) the past, present, or future physical, mental or behavioral health or condition of a consumer or a member of the consumer's family; (ii) the provision of health care to a consumer; or(iii) payment for the provision of health care to a consumer.

[2]**Cybersecurity event -** means an event resulting in unauthorized access to or the disruption or misuse of an information system or information stored on an information system. The term "cybersecurity event" does not include the unauthorized acquisition of encrypted nonpublic information if the encryption, process or key is not also acquired, released or used without authorization. The term "cybersecurity event" also does not include an event with regard to which the licensee has determined that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed.