THIRD PARTY SERVICE PROVIDER QUESTIONNAIRE

Entity	IAAC, Inc & Affiliates
Name & Title of Organization Senior Officer	Brian R. Bixby, President
Name of Organization Cybersecurity/Technology Contact	Kathleen M. Glahn
Email	kglahn@biginy.org
Phone	315-432-4253

Are you a covered entity under the NYS Cybersecurity Regulation (23 NYCRR 500)? (i.e., do you hold any license issued by the NYS Department of Financial Services?)	☑ Yes ☐ No
If you are a covered entity, have you filed your annual certificate of compliance with the NYS Department of Financial Services?	☑ Yes ☐ No ☐ N/A

If you are a covered entity, please select any exemptions you qualify for:

- ■ 500.19 (a 1, 2, &/or 3) Limited Exemption
- ☐ 500.19 (b) Employee, agent, or representative of a covered entity
- ☐ 500.19 (c) Do not directly or indirectly maintain, utilize, control, or operate any information systems
- ☐ 500.19 (d) Covered entity under Article 70 of the NYS Insurance Law (captive insurance company)
- ☐ 500.19 (f) Subject to NYS Insurance law section 1110 (charitable annuity society), section 5904 (risk retention group not chartered in NY), or are an accredited reinsurer pursuant to 11 NYCRR 125 (reinsurer)

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

- ■ 23 NYCRR 500 (NYS Cybersecurity Regulation)
- ☐ ISO/IEC 27000 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? If so, when and by whom? Security Metrics performs external penetration testing quarterly. Qualys performs internal vulnerability scanning on network devices weekly.	☑ Yes ☐ No

Do you encrypt data in transit? If yes, please list encryption technology/tool used. TLS 1.2/1.3; Veeam Encryption for Cloud backups, Outlook/M365 Encryption.	☑ Yes ☐ No
Do you encrypt data at rest (stored data)? If yes, please list encryption technology/tool used. BitLocker, SalesForce Encryption for AMS, Veeam Encryption for backups	☑ Yes ☐ No
Do you employ access controls and policies designed to limit access to relevant information systems and Nonpublic Information[1]? If yes, please briefly describe. SonicWall SSL VPN utilizing Multi-factor authentication for outside connections, limited secure access to servers housing NPI, limited access to general work area.	☑ Yes ☐ No
Do you use multi-factor authentication or risk-based authentication to protect against unauthorized access to your Nonpublic Information (multiple passwords and codes to access the network)?	☑ 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 or Nonpublic Information? If yes, please briefly describe. Upon becoming aware of any breach that may have impacted your NPI we will provide you with notice.	☑ Yes ☐ No
Click here to attest that the above is true and accurate to the best of your knowledge.	☒
Name & Title of person completing form Eric Miller, Systems Administrator	
Date 1/1/2024	

DISCLAIMER:

Big I New York is providing this sample questionnaire solely as a tool to assist agencies, brokerages, and organizations in assessing the third party service providers you work with. This sample questionnaire is not a substitute for agencies, brokerages, and organizations independently evaluating any business, legal or other issues, and is not a recommendation that a particular course of action be adopted. State security breach notification and privacy laws, coupled with insurance laws and regulations, impose varying requirements on agencies, brokerages, or organizations. Therefore, it is extremely important for agencies, brokerages, and organizations to carefully review applicable laws and regulations in all jurisdictions where they do business in structuring their specific security policies and processes. We have worked from the requirements in New York Regulation 23 NYCRR 500 in formulating this sample questionnaire, because the New York regulation imposes some of the most specific requirements. If specific advice is required or desired, the services of an appropriate, competent professional should be sought. Any agencies, brokerages, or organizations that uses this sample questionnaire agrees that Big I NY will have no liability for anything related to the use of this tool or any issues that may arise related to the decisions that you make or the policy that is developed.

1. **Definition of NPI:** Nonpublic Information shall mean all electronic information that is not Publicly Available Information and is: (1) Business-related information of a Covered Entity 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 Covered Entity; (2) Any information concerning an individual, which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) driver' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records; (3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.
2. **Definition of cybersecurity event:** Any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.