Frank H Reis Inc dba The Reis Group

Third-Party Risk Assessment Questionnaire

Note: Nonpublic information as referenced herein is defined by the New York Department of Financial Services under 23 NYCRR 500.01(g).

1. Does your organization have a cyber security program in place designed to identify and assess internal and external threats to ensure the security and integrity of nonpublic information stored on your information systems?
   ☑ Yes ☐ No

2. As applicable, has your organization certified that it is compliant with all relevant state cyber security laws?
   ☑ Yes ☐ No

3. Does your organization have an information-security-focused independent audit performed periodically (e.g., SOC 2, ISO 27001, PCI DSS, etc.)?
   ☑ Yes ☐ No

4. Do you have a Cyber Liability Insurance Policy?
   ☑ Yes ☐ No

   4a. If "yes," does your Cyber Liability Insurance Policy include incident-response services?
   ☑ Yes ☐ No

5. Are procedures in place to provide notice to all Third Party Service Providers within 72 hours of confirming a cyber security event impacting your information systems or nonpublic information held by your organization?
   ☑ Yes ☐ No

6. Has your organization implemented security tools to protect your information systems and data (e.g., firewalls, intrusion prevention/detection systems, event/threat monitoring, etc.)?
   ☑ Yes ☐ No

7. Does your organization perform recommended maintenance for all network infrastructure and information systems, including security patches for servers, desktops, laptops and mobile devices?
   ☑ Yes ☐ No

—continued—

8. Do all remote-access connections made to your network use encrypted protocols (e.g., VPN, Citrix, RDP, VNC, wireless, etc.)?
   ☑ Yes ☐ No

9. Does your organization have a teleworking policy that includes securing any remote work areas, equipment and software to ensure secure connections to your network, protection of data and/or other security measures?
   ☑ Yes ☐ No

10. Do all of your information systems require a password with a minimum length of eight characters, complexity (e.g., uppercase letter, lowercase letter, number, and symbol) and require regular password changes?
    ☑ Yes ☐ No

11. Are procedures in place that require all computers be locked when left unattended?
    ☑ Yes ☐ No

12. Is multifactor authentication required for external access to your internal systems?
    ☑ Yes ☐ No

13. Is anti-malware software required to be installed and kept updated on all of your servers, desktops, laptops and mobile devices?
    ☑ Yes ☐ No

14. Does your organization limit physical access to your facilities, computer rooms, data centers and other sensitive areas to authorized individuals only?
    ☑ Yes ☐ No

15. Does your agency implement controls to monitor the activity of authorized users and detect unauthorized access, use of or tampering with nonpublic information held by your organization?
    ☑ Yes ☐ No

16. Are your information systems backed up regularly, encrypted and stored off-site?
    ☑ Yes ☐ No

—continued—

17. Does your organization encrypt the data you transmit and the data stored on your servers, desktops, laptops and mobile devices?
    ☑ Yes ☐ No

18. Are procedures in place to require that all nonpublic information transmitted via email be encrypted?
    ☑ Yes ☐ No

19. Are procedures in place to securely dispose of any nonpublic information held by your organization that is no longer necessary, except when it is required to be retained by law or regulation?
    ☑ Yes ☐ No

20. Does your organization capture audit logs and retain them for at least three years to enable the monitoring, analysis, investigation and reporting of unlawful, unauthorized or inappropriate system activity?
    ☑ Yes ☐ No

21. Does your organization provide regular cyber security awareness training for all of your employees?
    ☑ Yes ☐ No

22. Does your organization have a formal Incident Response Plan for your information systems that is tested at least annually?
    ☑ Yes ☐ No

23. Does your organization perform a security risk assessment for all third-party service providers, at least annually, to assess the continued adequacy of their cyber security practices?
    ☑ Yes ☐ No

24. Are vulnerability assessments and external penetration tests performed at least annually to identify security vulnerabilities in your information systems?
    ☑ Yes ☐ No

25. Have you had a material security breach within the past five years?
    ☐ Yes ☑ No

—continued—

Comments/explanations, if necessary:
Comment field

The Reis Group will not be issuing individual questionnaires. Please use the email below for any additional information. This Third Party Service Provider Questionnaire is also available at www.reisinsurance.com/3rdparty

Contact information
Address: 475 Washington Avenue, Kingston, NY 12401
Phone number: (845) 338-4656
Email address: fcasciaro@reisinsurance.com