



Greater New York Insurance Companies (GNY) must comply with New York’s cyber regulation, Regulation 500, issued by the Department of Financial Services. We must ensure that our third parties handling nonpublic information transmit, store, and handle that information securely in compliance with the regulation. This questionnaire will help GNY personnel to assess the risk posed by a third party to comply with the regulation.

GENERAL INFORMATION

Title:
Organization Name:
Email Address:
Phone #:

SECTION 1

- 1. How many employees are employed by your organization (independent contractors should be counted as an employee)?
2. Is your organization a covered entity which needs to comply with the NY Department of Financial Services Regulation 500 "Cybersecurity Requirements for Financial Services Companies"? Yes No
3. If #2 is yes have all required aspects of Regulation 500 been complied with? (if No, elaborate why) Yes No
4. Has the organization documented IT operations procedures (e.g. backup, archiving, retention, and disposal process and procedures)? (if Yes, please provide a copy of the policy) Yes No

5. Is a SOC 2 (or similar) report available to review regarding cybersecurity practices? Yes No

6. Detail access control practices (e.g. user management, user authentication, etc.). How are access privileges removed after termination? *(Please provide a copy of your onboarding and offboarding procedures)*

7. Provide a description of audit login process and procedures.

8. Provide a description of employee background checks process and procedures.

9. Are the segregated secure areas protected by adequate physical entry controls? Yes No
(i.e. locks, proximity card readers)

10. Describe the perimeter access controls for this facility. *(e.g., perimeter checkpoints, use of card access controls including log retention, package searches, CCTV, first floor breakage windows)*

11. Are all visitors required to sign a security log and be accompanied by an escort while in secured areas? Yes No

12. Detail the organization's physical surveillance controls over internal critically secure areas.

13. What tools are used to ensure that VPN and other remote connections to the internal network are secured? (e.g., SSL VPN or client-less third-party web solution) Provide a description of remote access policy.

14. Do you use a guest wireless network? (if Yes, detail the segmentation controls and authentication methods in place) Yes No

15. Does the organization maintain records of user access requests and corresponding authorizations and access modifications? Yes No

16. Detail the organization's network and/or host intrusion detection or intrusion prevention systems, including a description of host security controls.

17. How many failed authentication attempts are allowed before users are locked out?

18. Does the organization perform risk assessments of critical infrastructure? Yes No

19. Does the organization maintain a privacy notice and corresponding policy or procedure for the protection of information transmitted, processed, or maintained on behalf of customers? Yes No

20. Do cleaning/maintenance crews access your offices/data centers during off-hours? Yes No

21. If #20 is yes, how are they verified/monitored?

22. If #20 is yes, are they instructed not to let anyone into the space without getting prior approval? Yes No

23. Do you perform regular internal vulnerability scanning based on the Common Vulnerability Scoring System (CVSS) to identify and remediate technology issues? Yes No

24. Provide a description of network perimeter security (e.g. IDS, firewalls, etc.).

25. Cybersecurity program policies and procedures - provide a copy of the policy or provide a detailed summary.

26. What is the security awareness program for employees and third parties you utilize?

SECTION 2 IF QUESTION #1 WAS LESS THAN 10 THE REMAINING QUESTIONS ARE OPTIONAL

27. Does the organization use strong, multi-factor authentication techniques to control remote user access (i.e. VPN) to its network? Yes No

28. Does the organization perform periodic penetration tests of critical infrastructure? Yes No

29. If #28 is yes, when was the last penetration test performed and who performed the test? *(Please provide a copy of the summary of most recent results)*

30. Detail your patch management policy.

31. How does the organization utilize encryption to protect sensitive information (such as social security numbers and other personal information not publicly available)? Is sensitive information both in transit and at rest encrypted? If encryption is not utilized, elaborate what alternative controls are in place.

32. Does the organization utilize full-disk encryption and/or mobile device management solutions to encrypt all storage on mobile devices?	Yes	No
--	-----	----

33. If #32 is yes, what tools are used? If #32 is no, what other controls are in place instead of encryption?

34. Are all encryption keys and certificates adequately protected and managed?	Yes	No	NA
--	-----	----	----

35. Provide a description of information exchange process and procedures (e.g. SFTP, PGP, etc.).

36. Detail your security incident response policy, including notification/escalation process and procedures.

37. Is the policy reviewed annually and updated as necessary? Yes No

38. Are all employees, contractors, and consultants trained to report security events/weaknesses to the appropriate contact person and/or department? Yes No

39. Do the existing incident response procedures include guidance for early involvement of organization's Legal Counsel, HR Management, forensic specialist and/or law enforcement authorities (as applicable)? Yes No

40. Do the existing incident response procedures include guidance for internal and external reporting of any identified security breach or incident? Yes No

41. Detail your procedures for disaster recovery and business continuity - provide a copy of the relevant policy.

42. What is the frequency of risk assessments of the cyber security practices of third parties which you utilize?

43. Provide a summary of latest risk assessment(s) related to your third parties.

44. Provide a description of security audit process and procedures.

45. Provide examples of compliance attestation reports.

GNY Insurance Companies

200 Madison Ave., New York, NY 10016

ThirdPartyManagement@GNY.com