#	23 NYCRR 500 Policy	Description
1	Cybersecurity Program Reference 23 CRR-NY 500.02.1	Maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the organization's information systems.
2	Cybersecurity Policy Reference 23 CRR-NY 500.03.2	Ensure the implementation and maintenance of a written cybersecurity policy, approved by a Senior Officer or the ORGANIZATION_NAME board of directors.
3	Information Security Policy Reference 23 CRR-NY 500.03.3	Provide management direction in line with business objectives and relevant laws and regulations, demonstrate support for, and commitment to, information security through the issue and maintenance of information security policies across the organization.
4	Data Governance and Classification Reference 23 CRR-NY 500.03.4	Establish organizational policies, processes, and procedures for data governance and risk management, to ensure information receives an appropriate and consistent level of protection.
5	Asset Inventory and Device Management Reference 23 CRR-NY 500.03.5	Ensure management requires ownership and defined responsibilities for the protection of information assets.
6	Access Controls and Identity Management Reference 23 CRR-NY 500.03.6	Provide for limited access to facilities and organization assets, and to prevent unauthorized access to networked services, operating systems and information held in application systems.
7	Business Continuity and Disaster Recovery Planning & Resources Reference 23 CRR-NY 500.03.7	Ensure strategies and plans are in place to counteract interruptions to business activities, and to protect critical business processes from the effects of major failures of information systems or disasters, and to ensure their timely resumption.
8	Systems Operations and Availability Concerns Reference 23 CRR-NY 500.03.8	Ensure detection of system operations and availability in a timely manner.
9	Systems and Network Security Reference 23 CRR-NY 500.03.9	Ensure the protection of information in networks and protection of the supporting network infrastructure.

#	23 NYCRR 500 Policy	Description
10	Systems and Network Monitoring Reference 23 CRR-NY 500.03.10	Ensure information security events and networks are monitored and recorded to detect unauthorized information processing activities in compliance with all relevant legal requirements.
11	Systems Application Development and Quality Assurance Reference 23 CRR-NY 500.03.11	Ensure development of information systems and applications.
12	Physical Security and Environmental Controls Reference 23 CRR-NY 500.03.12	Prevent unauthorized physical access and interference to ORGANIZATION_NAME's premises and information.
13	Customer Data Privacy Reference 23 CRR-NY 500.03.13	Ensure data protection and privacy of customer information.
14	Vendor and Third-Party Service Provider Management Reference 23 CRR-NY 500.03.14	Manage the security of ORGANIZATION_NAME's information, and information assets are not reduced by the introduction of external party products or services.
15	Chief Information Security Officer (CISO) Reference 23 CRR-NY 500.03.15	Designate a qualified individual responsible for overseeing and implementing ORGANIZATION_NAME's cybersecurity program and enforcing its cybersecurity policy.
16	Penetration Testing and Vulnerability Assessments Reference 23 CRR-NY 500.03.16	Ensure ORGANIZATION_NAME conducts regular vulnerability assessments and penetration tests to assess the effectiveness of ORGANIZATION_NAME's cybersecurity program.
17	Audit Trail Reference 23 CRR-NY 500.03.17	Securely maintain systems and records based on its Risk Assessment.
18	Access Privileges Reference 23 CRR-NY 500.03.18	Limit user access privileges to information systems that provide access to Nonpublic Information and periodically review such access privileges.

#	23 NYCRR 500 Policy	Description
19	Application Security Reference 23 CRR-NY 500.03.19	Ensure the use of secure development practices for in-house developed applications utilized by ORGANIZATION_NAME, and procedures for evaluating, assessing or testing the security of externally developed applications.
20	Risk Assessment Reference 23 CRR-NY 500.03.20	Conduct a periodic Risk Assessment of the ORGANIZATION_NAME's Information systems sufficient to inform the design of the cybersecurity program.
21	Cybersecurity Personnel and Intelligence Reference 23 CRR-NY 500.03.21	Utilize qualified cybersecurity personnel, an Affiliate or a Third-party service provider sufficient to manage the ORGANIZATION_NAME's cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions.
22	Third-Party Service Provider Security Policy Reference 23 CRR-NY 500.03.22	Implement written policies and procedures designed to ensure the security of Information systems and Nonpublic Information that are accessible to, or held by, third-party service providers.
23	Multi-Factor Authentication Reference 23 CRR-NY 500.03.23	Implement effective controls which include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information systems.
24	Limitations on Data Retention Reference 23 CRR-NY 500.03.24	Develop policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information that is no longer necessary for business operations or for other legitimate business purposes of ORGANIZATION_NAME, except where it is required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.
25	Training and Monitoring Reference 23 CRR-NY 500.03.25	Implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access. To provide regular cybersecurity awareness training for all personnel.

#	23 NYCRR 500 Policy	Description
26	Encryption of Nonpublic Information Reference 23 CRR-NY 500.03.26	Implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.
27	Incident Response Plan Reference 23 CRR-NY 500.03.27	Establish a written incident response plan for responding to and recovering from cybersecurity events.
28	Notices to Superintendent Reference 23 CRR-NY 500.03.28	Notify the superintendent of any cybersecurity event with a “reasonable likelihood of materially affecting the normal operation within 72 hours.”
29	Confidentiality Reference 23 CRR-NY 500.03.29	Protect the confidentiality and integrity of Nonpublic Information subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable state or federal law.