Appendix C-1

APPENDIX C-1 INFORMATION SECURITY REQUIREMENTS
for Cloud Services

New York State Department of Civil Service
June 2025

The following requirements shall be effective as of the date the Contractor or Contractor Staff first receives, maintains, transmits, accesses or otherwise comes into contact with Confidential Information. These requirements are intended to describe the minimum standard for physical, technical and administrative controls affecting Confidential Information in relation to the Services being provided under the Agreement.

The Department may suspend access to Department Systems or Data at any time if the Department, in its sole discretion, believes Contractor is not complying with any of its obligations herein.

Definitions
All capitalized terms herein shall have the meaning as set forth in this Appendix. If not defined herein will have the meaning as set forth in the resulting Contract including the Appendices and Attachments thereto, or if not defined therein will have the meaning as defined in 45 C.F.R. Parts 160-164.

1. Compliance

Contractor agrees to preserve the confidentiality, integrity and accessibility of Data with administrative, technical and physical measures that conform to Federal, State and Department mandates, and the security controls as stated herein, based upon the nature of the Project Services provided, the Data involved, and/or the location where such Project Services are provided. Accordingly, Contractor warrants, covenants and represents that it shall fully comply with or exceed the requirements in all New York State Information Technology Cybersecurity Policies, Standards and Procedures which The Department is required to follow by law. The current versions of these policies and standards are located at https://its.ny.gov/policies. The list of applicable policies and standards is included in Table 1.

Contractor is responsible for assessing and monitoring Subcontractor control environments for compliance with the standards as documented herein. The Department reserves the right to immediately revoke system or access privileges where such privileges pose an undue risk to the State.

2. Acceptable Use of Information Technology Resources

Contractor, including all Contractor Staff, accessing the State's non-public Information Technology Resources in the course of their work for the Department are required to comply with New York State Information Technology Policy NYS-P14- 001 – Acceptable Use of Information Technology Resources, as amended from time to time, prior to accessing any non-public New York State Information Technology resources.

Access to the State's Networks, Systems, Data, or Facilities is provided to support the official business of the Department. Any use inconsistent with the Department's business activities and administrative objectives is considered unacceptable or inappropriate use.

The Department reserves the right to change its policies and rules at any time, with regard to the acceptable use of Department Networks, Systems, Data or Facilities. Non-compliance with these provisions or unacceptable use of Department Networks, Systems or Facilities may result in the revocation of system privileges, termination of the Agreement with Department, and/or criminal and/or civil penalties.

3. Information Security Program

3.1. Contractor must maintain a written Information Security Program ("WISP") including documented policies, standards, and operational practices that meet or exceed the requirements and controls set forth herein to the extent applicable to the Project Services and identify an individual within the organization responsible for its enforcement. Contractor's WISP shall address, at a minimum, all security requirements as listed in these requirements, as amended from time to time, and comply with all state and federal data security and privacy laws applicable to the Department. This documentation will be reviewed by Contractor's security official, or its designee, at least annually and shall be updated periodically with changes to organization, technology, or Services. When implementing security controls Contractor shall take a risk-based approach. Any control exceptions which represent risk will be formally documented, monitored, and periodically reviewed.

3.2. Upon request by the Department, Contractor's WISP shall be made available to review by the Department or the Department's representative. Contractor shall apply appropriate sanctions against Contractor Staff who fail to comply with security policies and procedures.

3.3. Contractor shall have processes and procedures in place so that

Security Incidents will be reported through appropriate communications channels as quickly as possible. Contractor shall periodically test, review, and update such processes and procedures. All Contractor Staff shall be made aware of their responsibility to report any Events prior to being granted access to any Confidential Information. If at any time during the Agreement, Contractor becomes aware of an Event or that it or any of its Subcontractors will or do not meet the obligations described within these requirements, Contractor will immediately notify the Department.

3.4. Contractor shall periodically conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and Availability of Confidential Information. The assessment must be reviewed by Contractor's security official and used to inform the Contractor's information security program.

3.5. Upon request, the Contractor shall identify to the Department the security official who is responsible for the development and implementation of the Contractor's policies and procedures.

4. Right to Assess, Audit and Certify

4.1. Where the Contractor hosts, maintains, processes, or has access to Department Confidential Information, an independent SOC 2 Type 2 Attestation Report is required. The Department, at its discretion, may accept a comparable industry-recognized security certification or attestation in lieu of a SOC 2 Type 2 report. If an alternative security certification or attestation is accepted, then such certification shall be substituted for all references to SOC 2 within this Agreement.

- If the Contractor possesses a SOC 2 Type 2 Attestation Report applicable to the Project Services and/or systems in scope as of the Effective Date of the Agreement and maintains it throughout the term of the Agreement, then such attestation report, at the Department's discretion, shall satisfy the requirement for a formal security controls assessment identified in Section 4.2. Documentary evidence of the SOC 2 Type 2 report must be provided upon request, including the auditor's opinion, management's assertion, description of the system, testing procedures and results across all Trust Services Criteria, and any corrective action plans. Possession of a SOC 2 Type 2 attestation report does not waive the Department's rights to perform audits or

assessments under Section 4.1 or other rights established in this Agreement.

- If the Contractor does not possess a SOC 2 Type 2 Attestation Report or an approved alternative security certification as of the Effective Date of the Agreement, the Contractor shall:
    - Complete and submit a SOC 2 Readiness Assessment to the Department within 90 days of the Effective Date of the Agreement;
    - Obtain and provide a SOC 2 Type 2 Attestation Report from an independent CPA firm within 18 months of the Effective Date of the Agreement; and
    - Provide supporting documentation, including any management responses and corrective action plans, within 30 days of receipt of the attestation report.
- If the Contractor has initiated the process to obtain a SOC 2 Type 2 Attestation Report prior to the Effective Date of the Agreement, the Contractor shall notify the Department in writing of any known gaps or exceptions identified in a readiness assessment or draft findings, along with associated remediation plans.
- Within 30 days of discovery, the Contractor shall report any security findings or incidents identified through SOC 2-related audits or assessments that materially impact the confidentiality, integrity, or availability of Department data. The Contractor shall also provide the Department with any related corrective actions or follow-up reports as requested.
- If at any time during the term of the Agreement the SOC 2 Type 2 attestation is withdrawn, the Contractor shall notify the Department within 72 hours of learning of the issue and provide a written explanation and remediation plan.

4.2. From time-to-time Contractor may be requested to respond to, inform and provide updates regarding specific high-risk security gaps or exposures that exist for new or emerging security vulnerabilities that are

made publicly known for systems, applications, hardware devices, etc. In all instances Contractor will provide a response to any Department inquiry within five business days and will provide specific details as to the questions asked to ensure that the Department can appropriately evaluate the risk or exposure to the Confidential Information while still protecting the systems, applications, hardware devices etc. from further vulnerabilities.

5. Encryption

5.1. Contractor shall apply encryption methodology that, at minimum, conforms to the New York State Encryption Standard (NYS-S14-007) or other industry comparable standard (ex. NIST).

5.2. Cryptographic key management procedures must be documented and include references to key lifecycle management (including provisioning, distribution, and revocation) and key expiration dates.

5.3. Access to encryption keys must be restricted to named administrators. Encryption keys must be protected in storage. For example, methods of acceptable key storage include encrypting keys or storing encryption keys within a hardware security module (HSM). Data-encrypting keys should not be stored on the same systems that perform encryption/decryption operations.

5.4. Except as otherwise agreed to in writing by the Contractor and Department, Confidential Information must be encrypted while in transit and at rest across at least the following types of assets:

- Public shared Networks
- Non-wired Networks
- Cloud Services
- Desktop and portable computing devices
- Mobile devices
- Portable media
- Back-ups
- Application or Network servers
- ‘Plug & play’ storage devices

6. Network and Systems Security

6.1. Contractor shall utilize and maintain a commercially available, industry standard malware detection program which includes an automatic update function to ensure detection of new malware threats.

6.2. Contractor shall maintain an intrusion detection or prevention system that detects and/or prevents unauthorized activity traversing the Network.

6.3. Contractor shall have technical controls to detect, alert, and prevent the unauthorized movement of Data from Contractor's control (commonly referred to as Data Loss Prevention).

6.4. Networks or applications that contain Confidential Information must be separated from public Networks by a firewall to prevent unauthorized access from the public Network.

6.5. At managed interfaces, Network traffic is denied by default and allowed by exception (i.e., deny all, permit by exception).

6.6. Contractor shall establish security and hardening standards for Network devices, including Firewalls, Switches, Routers, Servers, and Wireless Access Points (baseline configuration, patching, passwords, and access control).

6.7. At a minimum, Contractor shall engage a qualified third party to perform annual penetration testing of all systems, infrastructure, and applications that are used to process, store, or transmit Confidential Data. Contractor must provide the Department with summary results and a remediation plan at the Department's request.

6.8. If Contractor provides products or Services related to the Agreement through a Department portal or mobile applications, especially those which are internet-facing, or use Department domains, the Department's portal, mobile applications and domain are subject to Department scanning and assessments. Contractor agrees to remediate vulnerabilities identified during this process in a manner and timeline acceptable to the Department.

6.9. Contractor shall ensure that no unencrypted Confidential Information is stored in any system that is internet facing.

6.10. Contractor shall use secure means (i.e., HTTPS, FTPS) for all electronic

transmission or exchange of System, user and application information with the Department.

7. System and Application Controls

7.1. All Confidential Information must be securely stored at all times to prevent loss and unauthorized access or disclosure.

7.2. Laptop and workstation systems that access Confidential Information remotely must utilize endpoint protection which includes a personal firewall and anti-malware protection.

7.3. Operating systems and application software used must be currently supported by the manufacturer.

7.4. Current versions of operating system and application software must be maintained, and patches applied in a timely manner for all systems and applications that receive, maintain, process, or otherwise access Confidential Information.

7.5. Confidential Information must not be used in any non-production environment such as testing or quality assurance unless de-identification of the Data has been performed. In the event that de-identification is not practical or feasible, compensating controls must be in place protecting the Data to the same level of protection as afforded to the production environment. Confidential Information must not be placed into a nonproduction cloud computing environment unless deidentified or compensating controls are in place protecting the Data to the same level of protection as afforded to the production environment.

7.6. Confidential Information must be segmented from non-Department Information so that appropriate controls are in place to identify the Data as Department's in all instances, including backup and removable media, and to appropriately restrict access only to users authorized to view the Data. Data must be deleted when it is no longer required.

8. Software Development Lifecycle

8.1. The Contractor shall agree to maximize the number of security features and controls of any software development throughout the term of this Contract according to general industry standards, including, but not be limited to, the following terms and conditions. These provisions apply to the base product as well as any customizations to the product under this Contract.

8.2. The development process must use either secure system development life cycle and secure coding practices standards as provided for in NYS-S13-001 Secure System Development Life Cycle Standard and the Secure Coding Standard NYS-S13-002, or comparable industry standard best practices.

8.3. Contractor must use both an automated and manual source code analysis tool to detect and remediate security defects in code prior to production deployment.

8.4. Contractor must have policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for the Project Services it provides to Department.

8.5. Contractor must have controls in place to prevent unauthorized access to its or Department's application, program, or object source code and ensure that access is restricted to authorized personnel only.

8.6. National identifiers or Social Security Numbers must not be utilized as User IDs for logon to applications.

9. Physical Controls for the Protection of Confidential Information

9.1. All Confidential Information received or created in paper form must be protected from viewing by unauthorized persons.

9.2. A clean desk policy will be enforced to ensure proper safeguarding of all hard copy Confidential Information.

9.3. Visitor logs documenting all individuals who are not Contractor Staff who gain access to the facility where Confidential Information is processed will be maintained.

9.4. Confidential Information shall not leave control of the Contractor without the written approval of Department.

9.5. Servers, enterprise data storage devices, backup tapes and media, and other computing devices that contain Confidential Information used to support Network communications must be located in a secure and restricted access location.

10. Access Control Related to Project Services

10.1. Physical and logical access will be granted to the minimum Confidential Information necessary to meet the requirements of the user's scope of responsibilities.

10.2. Only those individuals providing Project Services to the Department, or those who are responsible for administering, managing, or working in systems that contain Confidential Information, shall be authorized to access systems containing Confidential Information.

10.3. All Contractor Staff that are no longer required or authorized to access Confidential Information or systems that contain Confidential Information must have access promptly disabled.

10.4. Access to Confidential Information and systems that contain Confidential Information must be access controlled through the use of individual user IDs and passwords that substantially meet the NYS Authentication Tokens Standard NYS-S14-006

10.5. Standard complexity rules and password lifetimes or similar industry standards.

10.6. If it is suspected that a password has been compromised, the password must be immediately changed or reset.

10.7. Processes must be in place to create audit trails capable of determining who has accessed Confidential Information and/or systems that contain Confidential Information.

10.8. Remote access to systems or Networks that contain Confidential Information must use multi-factor authentication and a connection with Approved Encryption as defined in Section 5 above.

10.9. The Department reserves the right to immediately terminate remote access connections to Department or State Networks and Systems.

10.10. Upon request, Contractor shall provide reports within 72 hours for:

- List of all individuals with access to Confidential Information and/or systems that contain Confidential Information and the level of access granted;

- List of activity associated with any user ID who has access to Confidential Information; and

- Account management capabilities, such as account lockouts for unsuccessful logon attempts, remote access allowances, specific success and failure events, and management of elevated privilege accounts must be enforced.

11. Data Protection

Contractor must protect Confidential Information from unauthorized access, use, alternation, disclosure, or dissemination. The Contractor must, in accordance with applicable law and the instructions of the Department, maintain such Data for the time period required by applicable law, exercise due care for the protection of Data, and maintain appropriate data integrity safeguards against the deletion or alteration of such Data. If any Data is lost or destroyed because of any act or omission of the Contractor or any non-compliance with the obligations of this Contract, then Contractor shall, at its own expense, use its best efforts to reconstruct such Data as soon as feasible. In such event, Contractor shall reimburse the Department for any costs incurred by the Department in correcting, recreating, restoring or reprocessing such Data or in providing assistance therewith.

12. Data Return and Destruction

At the expiration or termination of the Agreement, at the Department's option, the Contractor must provide the Department with a copy of the Data, including metadata and attachments, in a mutually agreed upon, commercially standard format. Thereafter, except for Data required to be maintained, shall destroy Data from its systems and wipe all its data storage devices to eliminate any and all Data from Contractor's systems. The sanitization process must comply with New York State Security Policy NYS-S13-003. If immediate purging of all data storage components is not possible, the Contractor will certify that any Data remaining in any storage component will be safeguarded to prevent unauthorized disclosures. Contractor must then certify to the Department, in writing, that it has complied with the provisions of this paragraph.

13. Offshore Security Requirement

Confidential Information, including Protected Health Information, is not permitted to be hosted, maintained, stored, processed or otherwise accessed outside CONUS (“offshore”).

14. Contingency Planning

Contractor will have documented Business Continuity and Disaster Recovery plans in place that include Information security controls. Such plans will be tested at least annually.

15. Incident Response

15.1. Contractor will have a documented Incident Response Plan. Such plan will be tested at least annually and documentation of said testing will be provided to the Department upon request.

15.2. Incident response roles and responsibilities must be clearly outlined between Contractor and Department as appropriate.

16. Payment Card Industry Data Security Standard

If, in performing Project Services to or on behalf of Department, Contractor acts as a Merchant or payment card processor as defined by the Payment Card Industry Data Security (PCI DSS) standard, then Contractor agrees to comply with the applicable PCI DSS requirements.

17. Litigation Holds

The Contractor must provide a detailed mechanism for how litigation holds will be implemented. This description shall include how metadata will be created, accessed, and stored in a cloud environment.

18. Cloud Services

In addition to the above security requirements the following security provisions will apply to any State Data that is being hosted or maintained in a cloud environment (i.e., Cloud services). The provisions are related to security only and do not address maintenance and support or service levels.

18.1. FedRAMP and CAIQ

- All cloud services provided pursuant to this Contract shall comply with the standards set forth by the Cloud Security Alliance and/or Federal Risk and Authorization Management Program (FedRAMP) (https://www.fedramp.gov) for cloud services, and other applicable

Federal and/or New York State laws, regulations, and requirements.

- The Contractor must follow the National Institute of Standards and Technology (NIST) 800-53 guidelines for implementing system security and privacy controls and provide results of the Cloud Security Alliance Consensus Assessments Initiative Questionnaire (CAIQ) survey within 30 days of Contract approval, for the State's review. Thereafter on an annual basis, on the anniversary of the Contract Award, Contractor will provide a current CAIQ for the States review. The form is available at Cloud Security Alliance (https://cloudsecurityalliance.org/). The completion of this requirement is at the Contractor's expense with no additional cost to the State.

18.2. General Cloud Security

- Contractor's and its Subcontractor(s)' cloud services environment and/or applications must be available on a 24 hours per day, 365 days per year basis, providing around-the- clock service to New York State users of such systems.

- Contractor and its Subcontractor(s) must provide the State with reasonable advance notice of any major upgrades or system changes that are being performed.

- The Contractor shall maintain an up-to-date system contingency plan and assign personnel to coordinate joint contingency planning, training, and testing activities. In addition, Contractor shall have, and produce upon request, appropriate disaster recovery plans or processes to respond to events.

- Contractor will provide to the State backup and recovery procedures, and disaster recovery plans to ensure State Data is protected and is recoverable in case of a system failure.

- The following requirements are applicable to Contractor's and its Subcontractor(s)' development, testing and live production environments, for the cloud services provided to the State under this Contract:

- Contractor and its Subcontractor(s) shall establish and maintain appropriate environmental, safety, and facility procedures, data security procedures, and other safeguards against the destruction, corruption, loss, or alteration of the cloud services and any State Data to prevent unauthorized access, alteration or interference by third parties of the same.

- Contractor and its Subcontractor(s) shall utilize industry best practices and technology (including appropriate firewall protection, intrusion prevention tools, and intrusion detection tools) to protect, safeguard, and secure their cloud services systems and State Data against unauthorized access, use, and disclosure. Contractor and its Subcontractor(s) shall constantly monitor for any attempted unauthorized access to, or use or disclosure of, any of such materials and shall immediately take all necessary and appropriate action in the event any such attempt is discovered, within 72 hours after the discovery , or as agreed to by the State, notifying the State of any material or significant breach of security with respect to any such materials which impacts State Data.

- When software vulnerabilities are revealed and addressed by a Contractor patch, Contractor will obtain the patch from the applicable entity and categorize the urgency of applying the patch as either “critical” or “non-critical” in nature.

- The determination of the critical versus non-critical nature of patches is solely at the reasonable discretion of the Contractor in consultation with the State.

- Contractor will apply all critical security patches, hot fixes, or service packs as they are tested and determined safe for installation.

- Contractor and its Subcontractor(s) shall maintain and implement procedures to logically segregate State Data from Contractor’s data and data belonging to Contractor’s other customers.

- Security for any State Data hosted by is the responsibility of Contractor and will not require customization by the State.

- Contractor shall ensure that a sufficient number of personnel of suitable experience, training, and skills are assigned in accordance with the cloud services. Contractor shall have general control and discretion to determine the methods by which Contractor performs and maintains its hosting or other cloud services; provided however, that Contractor shall comply with all terms and conditions herein and that Contractor shall be fully responsive regarding all State requests regarding all operational methods regarding Contractor's cloud services as they relate to the State.

- Contractor and its Subcontractor(s) must track and control all access entering and exiting its facilities used to provide the State with cloud services under this Contract.

- Contractor and its Subcontractor(s) must apply standard software and hardware maintenance to its equipment as needed to address anomalies and security concerns, including software hot-fixes and service packs, third-party software used by Contractor, and its Subcontractor(s) including operating system, backups, antivirus software, and any application software, hardware firmware, and BIOS updates with updates tested internally prior to install.

18.3. Data Backup and Storage Management Services

- Contractor shall backup State Data for data recovery purposes.

- Contractor shall backup all State Data to a location at a separate and distinct datacenter for disaster recovery purposes. Failover to an alternate site is to be available at all times with little or no notice.

- In order to maintain uptime, critical services must be transferred in the event of a prolonged outage at the primary site. The alternate site must be located geographically separated from the primary site. Contractor's production facility and disaster recovery facility shall be located within the contiguous 48 states of the United States (CONUS) and no State Data shall be hosted outside of this geographic area. State Data shall be stored at the Contractor's production facility and at the disaster recovery facility for a number of specific days mutually agreed to by the Parties in a specific Transaction Document.

- Contractor will assist the State, at no cost to the State, in the restoration of State Data that has been deleted or corrupted.

18.4. Audit Report

Within 30 days of Contract approval, Contractor will provide, at Contractor's expense, an independent third-party audit of controls related to the security, availability, or processing integrity of a system or the confidentiality or privacy of the information processed by that system for all systems used to perform the services under the resulting Contract showing no deficiencies. Thereafter on an annual basis, at the Contractor's expense. A full version of the audit report will be provided to the State, within 30 days of the anniversary date of the Contract. A Service Organization Control (SOC) 2 Type 2 audit report or approved equivalent sets the minimum level of a third-party audit. Any deficiencies identified in

the audit report or where the Contractor is found to be noncompliant with Contract safeguards, must be remedied, within 90 days of the issue date of the audit report with proof of remediation provided to the State. The completion of this requirement is at the Contractor's expense with no additional cost to the State.

18.5. Development, Testing and Live Production Environments

All requirements are applicable to the Development, Testing, and Live Production Environments. Development and testing environments may be a scaled version of production if appropriate to the testing and development being performed.

18.6. Audit Logs

- Audit logs must capture all access to State Data (log information to include username, event type, event operation, event details, successful/unsuccessful authentication events, system start/stop, hardware attachment/detachment, system alerts and error messages, and other security events, unsuccessful attempts to access/modify/delete data being logged, or data in the event table). A minimum of 92 days of Audit logs must be retained.

- The technical and professional activities required for establishing, managing, and maintaining the environment are the responsibilities of the Contractor.

18.7. Hosting Requirements

Contractor agrees that it shall perform the hosting services in a manner consistent with the following requirements:

- Host all State Data and maintain and implement procedures to logically segregate and secure State Data from Contractor's data and data belonging to Contractor's other customers, including other governmental entities.

- Establish and maintain appropriate environmental, safety, and facility procedures; data security procedures; and other safeguards against the destruction, corruption, loss, or alteration of the hosting Services and any State Data, and to prevent unauthorized access, alteration, or interference by third parties of the same.

- Utilize industry best practices and technology (including appropriate firewall protection, intrusion prevention tools, and intrusion detection tools) to protect, safeguard, and secure the System and State Data against unauthorized access, use, and disclosure. Contractor shall constantly monitor for any attempted unauthorized access to, or use or disclosure of, any of such materials and shall immediately take all necessary and appropriate action in the event any such attempt is discovered, promptly notifying the State of any material or significant breach of security with respect to any such materials.

18.8. Vulnerability Scanning

The State will also have the option to request a third-party perform vulnerability scanning. Contractor must address all critical or severe (priority and secondary level) vulnerabilities found during scanning in a reasonable timeframe as agreed upon with the State.

Table 1

Policy / Standard	Policy No.	Section 3.0 Scope
Advertisements, Endorsements and Sponsorships on State Entity Websites	NYS-G24-002	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Information Security	NYS-P03-002	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Plan to Procure	NYS-P08-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Authority to Establish Enterprise Information Technology Policies, Standards, and Guidelines	NYS-P08-002	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Domain Names for State Government Agencies	NYS-P08-003	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Accessibility of Information Communication Technology	NYS-P08-005	Employees of SE (State Entities) and ITS, and all third parties (such as local governments, consultants, vendors, and contractors)
Guidance for the Use of SSNs by State Government Entities	NYS-P10-004	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Use of Social Media Technology	NYS-P11-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Information Security Exception Policy	NYS-P13-001	Employees of SE (State Entities) and all third parties (such as consultants, vendors, and contractors)
Acceptable Use of Information Technology Resources	NYS-P14-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Digital Identity	NYS-P20-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
International Access to NYS Systems or Data	NYS-P23-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Technology Exceptions	NYS-P23-002	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Acceptable Use of Artificial Intelligence Technologies	NYS-P24-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Contact Web Page	NYS-S05-002	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Continuing Professional Education Requirements for Information Security Professionals	NYS-S10-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Secure System Development Life Cycle	NYS-S13-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Secure Coding	NYS-S13-002	Employees of SE (State Entities) and ITS, and all third parties (such as local governments, consultants, vendors, and contractors)
Sanitization/Secure Disposal	NYS-S13-003	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Cyber Incident Response	NYS-S13-005	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Information Security Risk Management	NYS-S14-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Information Classification Standard	NYS-S14-002	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Security Logging	NYS-S14-005	Employees of SE (State Entities) and ITS, and all third parties (such as local governments, consultants, vendors, and contractors)
Authentication Tokens	NYS-S14-006	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Encryption	NYS-S14-007	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Secure Configuration	NYS-S14-008	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Mobile Device Security	NYS-S14-009	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Remote Access	NYS-S14-010	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Enterprise Mobile Management Technical Standard	NYS-S14-011	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Bring Your Own Device (BYOD)	NYS-S14-012	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Account Management/Access Control	NYS-S14-013	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Patch Management	NYS-S15-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Vulnerability Management	NYS-S15-002	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
802.11 Wireless Network Security	NYS-S15-003	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
New York State Universal Web Navigation	NYS-S16-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Notification Standard for Certain Types of Regulated Data	NYS-S17-003	Employees of SE (State Entities) and all third parties (such as consultants, vendors, and contractors)
Digital Identity	NYS-S20-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Establishing Technology Solutions & Standards	NYS-S23-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)

Policy / Standard	Policy No.	Section 3.0 Scope
Advertisements, Endorsements and Sponsorships on State Entity Websites	NYS-G24-002	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Information Security	NYS-P03-002	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Plan to Procure	NYS-P08-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Authority to Establish Enterprise Information Technology Policies, Standards, and Guidelines	NYS-P08-002	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Domain Names for State Government Agencies	NYS-P08-003	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Accessibility of Information Communication Technology	NYS-P08-005	Employees of SE (State Entities) and ITS, and all third parties (such as local governments, consultants, vendors, and contractors)
Guidance for the Use of SSNs by State Government Entities	NYS-P10-004	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Use of Social Media Technology	NYS-P11-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Information Security Exception Policy	NYS-P13-001	Employees of SE (State Entities) and all third parties (such as consultants, vendors, and contractors)
Acceptable Use of Information Technology Resources	NYS-P14-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Digital Identity	NYS-P20-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
International Access to NYS Systems or Data	NYS-P23-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Technology Exceptions	NYS-P23-002	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Acceptable Use of Artificial Intelligence Technologies	NYS-P24-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Contact Web Page	NYS-S05-002	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Continuing Professional Education Requirements for Information Security Professionals	NYS-S10-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Secure System Development Life Cycle	NYS-S13-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Secure Coding	NYS-S13-002	Employees of SE (State Entities) and ITS, and all third parties (such as local governments, consultants, vendors, and contractors)
Sanitization/Secure Disposal	NYS-S13-003	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Cyber Incident Response	NYS-S13-005	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Information Security Risk Management	NYS-S14-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Information Classification Standard	NYS-S14-002	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Security Logging	NYS-S14-005	Employees of SE (State Entities) and ITS, and all third parties (such as local governments, consultants, vendors, and contractors)
Authentication Tokens	NYS-S14-006	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Encryption	NYS-S14-007	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Secure Configuration	NYS-S14-008	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Mobile Device Security	NYS-S14-009	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Remote Access	NYS-S14-010	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Enterprise Mobile Management Technical Standard	NYS-S14-011	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Bring Your Own Device (BYOD)	NYS-S14-012	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Account Management/Access Control	NYS-S14-013	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Patch Management	NYS-S15-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Vulnerability Management	NYS-S15-002	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
802.11 Wireless Network Security	NYS-S15-003	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
New York State Universal Web Navigation	NYS-S16-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Notification Standard for Certain Types of Regulated Data	NYS-S17-003	Employees of SE (State Entities) and all third parties (such as consultants, vendors, and contractors)
Digital Identity	NYS-S20-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)
Establishing Technology Solutions & Standards	NYS-S23-001	Employees of SE (State Entities) and all third parties (such as local governments, consultants, vendors, and contractors)