NEW YORK STATE | Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

Office of Information Technology Services Guideline	**No:** ITS-P19-002
ITS Policy: **Cloud Computing Policy**	**Updated:** 02/12/2025
	Issued By: NYS Office of Information Technology Services **Owner:** Chief Information Office

1.0 Purpose and Benefits

This policy outlines the requirements for the appropriate and secure use of cloud computing systems and resources within the New York State (NYS) Cloud.

The NYS Cloud is a hybrid cloud exclusively owned, hosted, and managed by the NYS Office of Information Technology Services (ITS). It is a mixed computing environment where applications are run using a combination of network, compute, store, and services hosted in both public, private, government, and/or commercial cloud providers and on-premises in a secure, resilient, and zero emission data center facility.

This framework supports fully managed, monitored, and secure network, compute, storage, and native cloud services required for ensuring the confidentiality, integrity, and availability of all ITS and ITS client agency business applications.

2.0 Authority

Section 1 of Executive Order No. 117[1], issued January 2002, charges the State Chief Information Officer with overseeing and supervising the management and operations of the Office of Information Technology Services (ITS). *Section 102(2) of the State Technology Law* gives the Director of ITS responsibility for the administration of ITS. Details regarding this authority can be found in NYS ITS Policy, *NYS-P08-002 Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines*.

[1] All references to Executive Order 117 refer to that which was originally issued by Governor George E. Pataki on January 28, 2002 and continued by Executive Order 5 issued by Governor Eliot Spitzer on January 1, 2007, Executive Order 9 issued by Governor David A. Patterson on June 18, 2008, Executive Order 2 issued by Governor Andrew M. Cuomo on January 1, 2011 and Executive Order 6 issued by Governor Kathy Hochul on October 8, 2021.

3.0 Scope

This policy applies to ITS and ITS supported agencies (client agencies).

The NYS Cloud is the primary cloud computing service for ITS and all ITS client agencies, providing secure application hosting services and integrated share services for user identity, network domain naming, IT Service Management (ITSM), monitoring, backup and recovery, and security logging.

Cloud deployments must adhere to all ITS-issued policies and standards. Consideration will also be given to data classification, target architecture and cloud readiness, hosted location (on-prem, gov cloud, or commercial), backup and recovery, exit strategy, and total cost of ownership.

4.0 Information Statement

This policy requires the exclusive use of the NYS Cloud for all cloud-based service offerings by ITS and its client agencies, including but not limited to the following:

- Infrastructure as a Service (IaaS)
- Platform as a Service (Paas)
- Software as a Service (SaaS) offerings that are offered by ITS
- Anything as-a-Service (XaaS)

The NYS Cloud may include services in public or private facilities, including FedRAMP authorized environments, based upon security or other legal compliance requirements.

4.1 ITS as a Cloud Broker

As the State's Cloud Broker, ITS will source, integrate, and be the account owner for any third-party cloud delivering IT services for the State. ITS client agencies cannot independently procure third-party cloud services without the express written approval of ITS.

4.2 Information Owner Responsibility

All information security requirements, including identifying geographic residency, are the responsibility of the agency Information Owners (see "Determining the Information Owner" in the NYS-S14-002 Information Classification Standard).

Placement of data at rest will be based on the information security requirements identified by the Information Owners consistent with ITS policies, standards, and guidelines. Compliance may limit the use of services or require that data reside at specific facilities.

4.3 Identity

Cloud deployments must use an ITS approved identity provider for all application access and/or NY.GOV ID for any external personal, government, or business account application access. Identity and access management must adhere to the NYS-P20-001 Digital Identity Policy and any associated standards which can be found at https://its.ny.gov/policies.

4.4 Security

All Cloud deployments must comply with NYS-P03-002 Information Security Policy, NYS-P14-001 Acceptable Use of Information Technology Resources, and all associated standards which can be found at https://its.ny.gov/policies. Any additional controls required by applicable Federal or State law, rule, or regulation (e.g., IRS Publication 1075) must also be incorporated.

Additionally, all Cloud deployments must be developed and reviewed in alignment with NYS-S13-001 Secure Systems Development Lifecycle. All security logs must be forwarded to the New York Security Operations Center (NYSOC) and adhere to the NYS-S14-005 Security Logging Standard.

4.5 Exit Strategy

Off premise cloud deployments utilizing a third-party government or commercial cloud must have a defined exit strategy. The exit strategy must be inclusive of procedures to export data in a usable format, as agreed to by ITS.

4.6 Contract Terms

Contracts for cloud services must contain, at a minimum, the following provisions:

- All data provided to the vendor is owned by the State
- The vendor may only use data for the purposes of the contract or purchase
- Data must be kept confidential unless otherwise authorized
- Contractor may not limit or prevent access by the State to data for any reason during the term of the contract, except for planned interruptions, maintenance, or other similar activities
- Upon termination of the contract, the data, in a usable format as determined by ITS, must be accessible for a period of time, and all copies of the data held by the vendor must be destroyed or returned
- The vendor is aware of its obligations related to breaches or unauthorized access to data

Attachment 1 contains sample language that may be used by SEs for cloud procurements. Based on the specific scope of the contract, agencies may need to

add additional requirements to this sample language, including requirements related to regulated data.

5.0 Compliance

This policy shall take effect upon publication. Compliance is required with all enterprise policies and standards. Client agencies with current cloud services not in compliance with this policy as of its latest revision date must become compliant before renewing any contract for those cloud services. ITS may amend its policies and standards at any time; compliance with amended policies and standards is required.

If compliance with this policy is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, client agencies shall submit a written request for an exception to the CIO. The CIO will issue a written approval or denial of the request.

6.0 Definitions of Key Terms

Except for terms defined in this policy, all terms shall have the meanings found in the ITS Glossary.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Chief Information Office
Reference: ITS-P19-002
NYS Office of Information Technology Services
State Capitol, ESP, P.O. Box 2062
Albany, NY 12220-0062
Telephone: (518) 402-7000
Email: CIO@its.ny.gov

The State of New York Enterprise IT Policies may be found at the following website:
https://its.ny.gov/policies

8.0 Revision History

This policy document should be reviewed consistent with the requirements set forth in NYS-P08-002 Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines.

Date	Description of Change	Reviewer
06/01/2020	Issued policy	Chief Technology Office

Date	Description of Change	Reviewer
02/12/2025	Updated Policy	Chief Technology Office

9.0 Related Documents

NYS-S14-002 Information Classification Standard

NYS-P20-001 Digital Identity Policy

NYS-P03-002 Information Security Policy

NYS-P14-001 Acceptable Use of Information Technology Resources

NYS-S13-001 Secure Systems Development Lifecycle

NYS-S14-005 Security Logging Standard

Attachment 1

Sample Cloud Terms

These cloud terms provide minimal requirements that should be contained in all State contracts for cloud services. Agencies should consider their specific use cases to determine additional requirements.

SAMPLE LANGUAGE - NONDISCLOSURE & CONFIDENTIALITY

Contractor shall maintain the security, nondisclosure, privacy, and confidentiality of all information in accordance with the following clauses in the performance of its activities under the Contract. Contractor shall ensure that its agents, employees, officers, partners, and subcontractors, if any, are fully aware of the obligations arising under the Contract and shall take all commercially reasonable steps to ensure their compliance to prevent unauthorized use, access, or disclosure of NYS Confidential Information. Failure by Contractor or its agents, employees, officers, partners, or subcontractors to fully comply with these requirements shall be deemed a failure to meet Contractor's obligations under the Contract and may result in ITS suspending, canceling, and/or terminating the Contract for cause or to pursue any other legal or equitable remedies available.

a. Definitions. "*New York State ('NYS') Facilities*": As used in the Contract, the term "*NYS Facilities*" shall mean any real property, tangible personal property, or electronic or virtual systems, or any part(s) or component(s) thereof, used in the conduct of New York State's business operations, including, but not limited to, physical office or computing space, computer(s) or computer systems, telecommunications or network infrastructure (e.g., utility closet(s), conduits, hubs, switches, routers), and supporting NYS Facilities and systems (e.g., mechanical, power, cooling, security, fire protection, water), regardless of owner.

"New York State ('NYS') Confidential Information": For purposes of the Contract, any information that [Agency] or the State, regardless of form or medium of disclosure (e.g., verbal, hard copy, or electronic) or source of information (e.g., [Agency], other state agencies, electronic systems, federal government, or third-party contractors) provides to the Contractor, its agents, employees, officers, partners, and subcontractors or which Contractor, its agents, employees, officers, partners, and subcontractors obtains, discovers, derives, or otherwise becomes aware of as a result of Contractor's performance other than:

a. information that is previously rightfully known to the receiving Party without restriction on disclosure;

b. information that is or becomes, from no act or failure to act on the part of the receiving Party, generally known in the relevant industry or is in the public domain; and

c. information that is independently developed by Contractor without use of NYS Confidential Information.

"Contractor": For purposes of the Contract, obligations of the Contractor who is a Party to the Contract with [Agency] and refers to collectively, as well, Contractor's agents, employees, officers, partners, or subcontractors.

"State." For purposes of the Contract shall be interpreted to including New York State executive agencies (e.g., ITS, DTF, OTDA, DOH).

"Information Security Incident." For purposes of the Contract shall mean any allegation or suspicion held by or brought to the attention of a State employee or Contractor involving inappropriate or unauthorized access to, or disclosure of, NYS Confidential Information or NYS Facilities.

b. Data Ownership, Non-Disclosure, and Confidentiality. NYS Confidential Information is owned exclusively by New York State, will remain the property of the State throughout its use under the Contract, and shall not be released to any third-party by Contractor unless as required by applicable law or a court of competent jurisdiction, or unless Contractor has first obtained explicit written permission from a duly authorized individual employed by the State. Contractor is permitted to use NYS Confidential Information solely for the purposes set forth in the solicitation and the Contract, and for no other purpose. At no time shall the Contractor access, use, or disclose any NYS Confidential Information (including, but not limited to, personal, financial, health, or criminal history record information or other sensitive criminal justice information) for any other purpose. Further, NYS Confidential Information must be fully accessible at all times to the State during the term of the Contract and at the Contract's conclusion. Contractor may not limit or prevent access by the State to Confidential Information for any reason during the term of the Contract, except for planned interruptions, maintenance, or other similar activities.

The Contractor is strictly prohibited from releasing or using NYS Confidential Information for any purposes other than those purposes defined herein or authorized in writing by the State. Contractor agrees that NYS Confidential Information shall not be distributed, used, repurposed, transmitted, exchanged, or shared across other applications, environments, or business units of the Contractor or otherwise passed to other contractors, agents, subcontractors, or any other interested parties, except as expressly and specifically agreed to in writing by the State. Contractor shall indemnify and hold [Agency] and the State harmless from any loss or damage to the State resulting from the disclosure by the Contractor of such NYS Confidential Information, in accordance with the terms and conditions of the Contract. Contractor, including Contractor's agents, employees, officers, partners, or subcontractors, may be required to execute all nondisclosure agreements identified in the solicitation, either before or upon arrival at NYS Facilities or, if in the State's sole discretion, Contractor will otherwise have access to critical State networks, equipment, or NYS Confidential Information.

c. Compliance with NYS Information Security Policies and Procedures. Contractor warrants, covenants, and represents that it shall comply fully with all security procedures of the State communicated to it in the performance of the Contract, including NYS Information Security policies and standards, and their successors posted on the

ITS website. At the State's discretion, it may, at any time during the term of the Contract, request that Contractor provide documentation validating its adherence to these security policies and standards. Contractor must deliver such documentation within thirty (30) days of a request by the State or as mutually agreed to, in writing, by the Parties.

Contractor, to the extent the following meets or exceeds the NYS Information Security policies and standards described above, shall use industry standard security measures, including standard encryption protocols, to protect and guard the availability and security of all NYS Confidential Information, and adhere to all the State's security policies. Contractor shall be strictly prohibited from using NYS Confidential Information in any fashion other than that defined herein. There may be instances whereby the State will communicate security procedures necessitated by the State's operations. Contractor will use reasonable efforts to implement same. In the event Contractor does not implement or communicates that it cannot or will not implement such security procedures, the Parties will reasonably work to resolve such dispute pursuant to the Contract's Dispute Resolution process to the extent such dispute does not adversely impact the State's legal obligations.

Contractor warrants that its Contractor Staff are properly informed and trained regarding industry standard security measures, NYS Information Security policies and standards, and are prohibited from disclosing NYS Confidential Information to any persons without a need to know.

d. Protection and Transmission of NYS Confidential Information. Contractor shall use appropriate means to preserve and protect NYS Confidential Information. This includes, but is not limited to, use of stable storage media, regular data backups and archiving, password protection of volumes, and data encryption. Consistent with the NYS Encryption Standard, to the extent doing so is applicable based on the specific services provided by Contractor to [Agency] under the Contract, the Contractor must encrypt NYS Confidential Information at rest, on file storage, on database storage, or on back-up media, and in transit in accordance with Local, State, and Federal laws, rules, regulations, ordinances, policies, standards, and guidelines. Contractor must use secure encrypted means (e.g., HTTPS, SFTP) for all electronic transmission or exchange of system, user, and application data with the State. Encryption at rest shall specifically use a currently valid FIPS approved cryptographic modules. The secure means used for electronic transmission or exchange of system, user and application data with the State shall be HTTPS, TLS version 1.3 or higher, or TLS 1.2 using only currently valid and non-depreciated ciphers.

Contractor agrees that to the extent it has been authorized in writing to use such storage, any and all NYS Confidential Information will only be stored, processed, and maintained solely on designated target devices, and that no NYS Confidential Information at any time will be processed on or transferred to any portable computing device or any portable storage medium.

Contractor shall also comply fully with all requirements of the Contract pertaining to security requirements specific to the services Contractor is providing to the State under

the Contract. In addition to the specific security provisions required herein, Contractor shall also use, to the extent the following meets or exceeds NYS Information Security polices and standards, commercially reasonable best efforts to address and remediate any vulnerabilities associated with the types of application development or configuration services it is providing under the Contract which appear on the CWE/SANS list of the "TOP 25 Most Dangerous Programming Errors" (http://www.sans.org/top25errors/). When a vulnerability scan is being conducted as required by applicable NYS Information Security policies and standards and reveals software application vulnerabilities or any other security risks attendant to a provided solution, Contractor is responsible for ensuring those vulnerabilities and risks are remediated to [Agency]'s reasonable satisfaction, including, but not limited to, complying with the requirements of ITS Standard NYS-S15-002, Vulnerability Management, or any successor standard..

e. Physical Transport of NYS Confidential Information. To the extent the State agrees under the Contract that Contractor may physically transport any NYS Confidential Information, such physical transport may only occur upon the written direction and approval of the State and must comply with all applicable Local, State, and Federal laws, rules, regulations, ordinances, policies, standards, and guidelines. This includes, but is not limited to, transport between the Contractor's offices, to and from subcontractors, and to the State.

f. Data Storage, Access, and Location - Off Shore Restrictions. Contractor agrees that: (a) all NYS Confidential Information shall remain within and may not be stored, or accessed from, outside of the Contiguous United States (CONUS) and (b) unless expressly agreed to in writing by a State authorized signatory adhering to established State practices, Contractor shall not have remote access into NYS Facilities.

All access to NYS Confidential Information and NYS Facilities, physical or virtual, must be conducted within CONUS and have adequate security systems in place to protect against the unauthorized access to NYS Confidential Information stored therein or NYS Facilities. The Contractor shall not send or permit to be sent to any location outside of the CONUS any NYS Confidential Information related to the Contract.

To the extent support by Contractor requires replication of a set of conditions such as a software crash event, Contractor shall replicate that set of conditions in its own environment when providing support, while communicating with State technical personnel. For software development activities, such as patches, updates, or adding new functionality, Contractor shall conduct that software development within its own development, quality assurance, and production environments, and, when ready, shall package and provide it through an agreed-to Internet-based location, from which State technical personnel will download such software, and install and test it in the State's information technology environment. Contractor must provide the results of vulnerability scans conducted on the code prior to the State accepting changed in the code.

Upon prior written approval of [Agency], to the extent Contractor requires access to State system or application audit logs for support and troubleshooting, Contractor will

maintain such logs only within CONUS, will take the strictest measures to ensure such logs do not contain NYS Confidential Information including production data, and will maintain such logs in a secure environment subject to audits by the State.

g. Separation of Duties / Access Controls. The Contractor must ensure that all NYS Confidential Information that it holds under the Contract is stored in a controlled access environment to ensure data security and integrity that adheres to all applicable Local, State, and Federal laws, rules, regulations, ordinances, policies, standards, and guidelines. Contractor will provide the State a list of the physical locations where Contractor has stored any NYS Confidential Information at any given time and will update that list if the physical location changes. All Contractor facilities must have adequate security systems in place to protect against the unauthorized access to such facilities and data stored therein. Access into and within such facilities must be restricted by Contractor through an access control system that requires positive identification of authorized individuals as well as maintains a log of all accesses (e.g., date and time of the event, type of event, user identity, component of the information system, outcome of the event). The Contractor shall have a formal procedure in place for granting computer system access to NYS Confidential Information and to track access. Contractor access to NYS Confidential Information for any types of projects outside of those approved by [Agency] are prohibited.

[Agency] requires the Contractor to follow security best practices by adhering to the principle of least privilege and adhering to separation of job duties, and limiting Contractor Staff knowledge of NYS Confidential Information to that which is absolutely needed to perform job duties. Upon request, Contractor will provide documentation to the State clearly defining the security roles and access levels for each of its staff working with NYS Confidential Information with a level of specificity objectively reasonable to and approved by the State. Only those individuals who have successfully completed all required security clearance and background check requirements, including training, shall have access to NYS Confidential Information.

SAMPLE LANGUAGE - BREACHES OF NYS CONFIDENTIAL INFORMATION

a. Compliance with the NYS Information Security Breach and Notification Act (ISBNA). In accordance with the Information Security Breach and Notification Act (ISBNA) (NYS General Business Law, §889-aa and §889-bb; NYS Technology Law, §208), Contractor shall be responsible for complying with the provisions of the ISBNA and the following terms contained herein with respect to any Private Information (as defined in ISBNA) received by Contractor under the Contract that is within the control of the Contractor either on the State's information technology systems or the Contractor's information technology systems (System). In the event of a breach of the security of the System (as defined by the ISBNA) Contractor shall immediately commence an investigation, in cooperation with the State, to determine the scope of the breach and restore the security of the System to prevent any further breaches. Contractor shall also notify the State of any breach of the security of the System immediately following discovery of such breach. Notice of such breach will be sent to:

Agency:
[Agency Contact]

ITS CISO:
Chief Information Security Office
Harriman Campus, 1220 Washington Avenue
Bldg. #5, FL. 4
its.sm.ciso@its.ny.gov

Except as otherwise instructed by the State, Contractor shall, to the fullest extent possible, first consult with and receive authorization from ITS prior to notifying any individuals, the Department of State (DOS), the NYS Division of State Police, the NYS Office of the Attorney General (OAG), or any consumer reporting agencies of a breach of the security of the System or concerning any determination to delay notification due to law enforcement investigations.

Nothing herein shall in any way impair the authority of the OAG to bring an action against Contractor to enforce the provisions of ISBNA or limit Contractor's liability for any violations of the ISBNA or any other applicable statutes, rules, or regulations. In the event that the Contractor is advised by a law enforcement agency pursuant to GBL §899-aa(4) to delay the notice under GBL §899-aa(3), the Contractor shall provide the notice under GBL §899-aa(3) to the State not more than twenty-four hours after the Contractor has been advised by the law enforcement agency that notice under GBL §899-aa(3) can be provided.

In accordance with ISBNA, Contractor is responsible for complying with the following terms with respect to any Private Information (as defined in the ISBNA) received by or on behalf of the State under the Contract. Contractor:

- Shall supply [Agency] with a copy of its breach notification policy, which shall be modified to be in compliance with this provision.
- Must encrypt any database fields and backup tapes that contain Private Information, as set forth in the ISBNA.
- Must ensure that the State's Private Information is encrypted in transit to/from Contractor's systems.
- In general, Contractor must ensure that Private Information is not displayed to users on computer screens or in printed reports; however, specific users who are authorized to view the private data elements and who have been properly authenticated may view/receive such data.
- Must monitor for breaches of security to any of its systems that store or process the State's Private Information.
- Shall take all steps as set forth in ISBNA to ensure Private Information shall not be released without authorization from the State.

- In the event a security breach occurs as defined by ISBNA, notify the ITS Chief Information Security Officer (CISO) by telephone within four (4) hours of becoming aware of the breach and commence an investigation in cooperation with the State to determine the scope and cause of the breach, and to prevent the future recurrence of such security breaches.
- Coordinate all communication regarding the data breach with the ITS CISO and the State.
- Take immediate and necessary steps needed to restore the information security system to prevent further breaches and take corrective action in the timeframe required by the State. If Contractor is unable to complete the corrective action within the required timeframe, in addition to any other remedies available, the State may contract with a third-party to provide the required services until corrective actions and services resume in a manner acceptable to the State, or until the State has completed a new procurement for a replacement service system. The Contractor will be responsible for the cost of these services during this period.

Contractor shall be responsible for providing all notices required by the ISBNA and for all costs associated with providing said notices.

The State reserves the right to require commercially standard credit monitoring for any and all individuals affected by the data breach at the sole expense of the Contractor for a period to be determined by the State, but not less than twelve (12) months, which shall begin thirty (30) days following the notice of offer from the Contractor of such credit monitoring to those affected individuals, which shall be within a reasonable time following the identification of such affected individuals. The State reserves the right to require notice by regular or electronic mail.

b. non-ISBNA Breaches. In addition to any responsibilities of Contractor under the Contract for reporting breaches of Private Information under ISBNA, Contractor must immediately report to [Agency] any breaches, Information Security Incidents, or unauthorized uses or disclosures of any NYS Confidential Information whether it consists of Personal Information or otherwise. Notice of such breaches or incidents shall be sent to:

[Agency Contact]

ITS Chief Information Security Office
Harriman Campus, 1220 Washington Avenue
Bldg. #5, FL. 4
its.sm.ciso@its.ny.gov

Contractor shall ensure that the Contractor Staff charged with carrying out services under the Contract are aware of Contractor's obligations to the State hereunder. Contractor's Staff browsing, viewing, altering, appending, or modifying the NYS Confidential Information in violation of Contractor's own security policies shall be deemed to have breached the security of the system for the purposes of the Contract.

c. Preventing Unfair Advantage - Contractor Internal Breaches. Contractor further represents and warrants that it is aware that New York State procurement laws require a "level playing field" prohibiting an unfair advantage to any particular vendors on State IT procurements. Contractor acknowledges that to the extent it performs services under the Contract, Contractor's personnel may become aware of NYS Confidential Information consisting of data elements that are collected from government agencies regarding IT planning and potential future purchasing, and that even without actual government agencies' data, knowing exactly what is collected could give the impression of an unfair advantage to Contractor for future state IT procurements. Contractor shall use its most stringent commercially reasonable best efforts to create a "firewall" between those of its Contractor Staff and its business units which are permitted to perform services under the Contract and all other personnel and business units of Contractor including those involved in seeking state IT procurements to ensure NYS Confidential Information is not divulged to any of Contractor's personnel who are not strictly needed to perform services under the Contract and approved by the State to do so. Any divulging of such NYS Confidential Information to Contractor's personnel who are not strictly needed to perform services under the Contract and approved by the State to do so shall be deemed a security breach under the Contract. In addition to any other remedies available to the State for such security breach, Contractor understands that if such security breaches occur Contractor may be deemed a non-responsible vendor under the State's procurement laws and forbidden from contracting on any New York State procurements related to any of the NYS Confidential Information which was breached.

SAMPLE LANGUAGE - DATA TRANSPARENCY, ACCESSIBILITY, MIGRATION, and DESTRUCTION AT END OF CONTRACT

a. Data Migration. Contractor shall ensure that the services it performs and the solutions it designs under the Contract are performed in such a way so as to ensure easy migration of any NYS Confidential Information held by Contractor as required by the State. This may include:

- Contractor keeping NYS Confidential Information, including State policy and profile information, separate from processes of any software itself and maintaining that information in a format that allows the State to easily transfer it to an alternative application platform;
- Contractor making its Application Programming Interfaces (APIs) available to the State; and
- Contractor reformatting data and/or applications at Contractor's own expense in order to easily allow the State to switch to alternative software providers or move the NYS Confidential Information back in-house at the State.

b. Data Return and Destruction - In General. During any period of suspension of services or of the Contract, the Contractor will not take any action to intentionally erase any NYS Confidential Information.

At the expiration or termination of the Contract, the Contractor shall implement an orderly return of State assets and the subsequent secure disposal of State assets. The State shall be entitled to any post-termination assistance generally made available by Contractor with respect to the services it provides unless a unique alternative data retrieval arrangement has been established between the Parties in writing.

At the State's option, the Contractor must provide the State with a copy of the NYS Confidential Information, including metadata and attachments, in a mutually agreed upon, commercially standard format at no additional charges to the State, and give the State continued access to NYS Confidential Information for no less than ninety (90) days beyond the expiration or termination of the Contract. Thereafter, except for data required to be maintained by Local, State, and Federal laws, rules, regulations, ordinances, policies, standards, or guidelines or the Contract, Contractor shall destroy NYS Confidential Information from its systems and wipe all its data storage devices to eliminate any and all NYS Confidential Information from Contractor's systems. The sanitization process must be in compliance the NYS Security Standard, NYS-S13-003, and its successors, and, where required, other sanitization and disposal standards. If immediate purging of all data storage components is not possible, the Contractor will certify that any NYS Confidential Information remaining in any storage component will be safeguarded to prevent unauthorized disclosures until such purging is possible. Contractor must then certify to the State, in writing, that it has complied with the provisions of this paragraph including providing any supporting documentation as required. The State may withhold payment to Contractor if NYS Confidential Information is not released to the State in accordance with the preceding sections.

c. Data Return and Destruction - Regulated Data. New York State considers the protection of sensitive data and NYS Confidential Information and business systems to be of the upmost importance. The NYS Confidential Information collected and maintained by State and local government agencies is protected by Local, State, and Federal laws, rules, regulations, ordinances, policies, standards, and guidelines. Access to and use of NYS Confidential Information is limited to authorized government employees and legally designated agents, for authorized purposes only.

To the extent that Contractor has access to Local, State, or Federal government regulated data pursuant to their responsibilities under the Contract, Contractor agrees that it will abide by the requirements of those Federal, State, and Local laws, rules, regulations, ordinances, policies, standards, and guidelines, and will require in writing its agents, employees, officers, partners, or subcontractors to similarly abide by any such requirements including the execution of any documents or agreements required to be executed, certifying their compliance with same.

Contractor must, in accordance with applicable law and the instructions of the State: maintain such regulated data for the time period required by applicable law, rule, regulation, ordinance, policy, standard, or guideline; exercise due care for the protection of data; and maintain appropriate data integrity safeguards against the deletion or alteration of such data. In the event that any regulated data is lost or destroyed because of any act or omission of the Contractor or any non-compliance with the obligations of the Contract, then Contractor shall, at its own expense, use its best efforts in

accordance with industry standards to reconstruct such data as soon as feasible. In such event, Contractor shall reimburse the State for any costs incurred by the State in correcting, recreating, restoring, or reprocessing such data or in providing assistance therewith.

In the event that it becomes necessary for Contractor to receive NYS Confidential Information which Local, State, or Federal laws, rules, regulations, ordinances, policies, standards, and guidelines prohibit from disclosure, Contractor hereby agrees to return or destroy, adhering to the standards outlined in the above section, all such NYS Confidential Information that has been received from the State when the purpose that necessitated its receipt by Contractor has been completed. In addition, Contractor agrees, after termination of the Contract, not to retain any NYS Confidential Information which Local, State, and Federal laws, rules, regulations, ordinances, policies, standards, and guidelines prohibit from disclosure

Notwithstanding the foregoing, if the return or destruction of the regulated data or NYS Confidential Information is not feasible, Contractor agrees to extend the protections of the Contract for as long as necessary to protect the regulated data or NYS Confidential Information and to limit any further use or disclosure of that regulated data, or NYS Confidential Information. If Contractor elects to destroy the regulated data or NYS Confidential Information, it shall use reasonable efforts to achieve the same and notify the State accordingly. Contractor agrees that it will use all appropriate safeguards to prevent any unauthorized use or unauthorized disclosure of NYS Confidential Information which Local, State, and Federal laws, rules, regulations, ordinances, policies, standards, and guidelines prohibit from disclosure.

d. Data Retention. Notwithstanding any other obligation under the Contract Contractor agrees that it will preserve NYS Confidential Information in a manner that complies with all applicable Local, State, and Federal laws, rules, regulations, ordinances, policies, standards, and guidelines for the purposes of ensuring applicable data records retention obligations are met.