

EXHIBIT 2

SECURITY, NON-DISCLOSURE/CONFIDENTIALITY, PRESS RELEASES

TERMS AND CONDITIONS

The Contract may be terminated by the State for cause for a material breach of the terms and conditions herein.

1. Nondisclosure & Confidentiality

Except as may be required by applicable law or a court of competent jurisdiction, the Contractor, its officers, agents, employees, and subcontractors, if any, shall maintain strict confidence with respect to any Confidential Information to which the Contractor, its officers, agents, employees, and subcontractors, if any, have access. This requirement shall survive termination of the Contract. For purposes of the Contract, all State information of which Contractor, its officers, agents, employees, and subcontractors, if any becomes aware during the course of performing services for the State shall be deemed to be confidential information (oral, visual or written). Notwithstanding the foregoing, information that falls into any of the following categories shall not be considered Confidential Information:

1. information that is previously rightfully known to the receiving party without restriction on disclosure;
2. information that 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
3. information that is independently developed by Contractor without use of Confidential Information of the State.

Contractor shall indemnify and hold the State harmless from any loss or damage to the State resulting from the disclosure by the Contractor, its officers, agents, employees, and subcontractors of such Confidential Information.

2. Federal or State Requirements

Contractor will comply with federal and state law and regulations regarding personal, private and sensitive data.

In the event that it becomes necessary for Contractor to receive Confidential Information, which Federal or State statute or regulation prohibits from disclosure, Contractor hereby agrees to return or destroy all such 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 not to retain any Confidential Information which Federal or State statute or regulation prohibits from disclosure after termination of the Contract.

Notwithstanding the foregoing, if the return or destruction of the Confidential Information is not feasible, Contractor agrees to extend the protections of the Contract for as long as necessary to protect the Confidential Information and to limit any further use or disclosure of that Confidential Information. If Contractor elects to destroy 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 Confidential Information, which Federal or State statute or regulation prohibits from disclosure.

Contractor agrees that it shall immediately report to the State the discovery of any unauthorized use or unauthorized disclosure of such Confidential Information of any New York State Agency information directly to that New York State Agency. The State may terminate the Contract if it determines that Contractor has violated a material term of this section. The terms of this section shall apply equally to Contractor, its agents and subcontractors, if any. Contractor agrees that all subcontractors, if any and agents shall be made aware of and shall agree to the terms of this section.

3. Off Shore restrictions

Confidential Information accessed by or provided to Contractor during the course of performing services for the State must not be stored or accessed outside of CONUS.

4. Access to Regulated Data

New York State considers the protection of sensitive and confidential information and business systems to be of the utmost importance. The information collected and maintained by state and local government agencies is protected by a myriad of Federal and State laws and regulations. Access to and use of sensitive and confidential information is limited to authorized government employees and legally designated agents, for authorized purposes only.

The chart in Appendix J - PRIMARY SECURITY AND PRIVACY MANDATES, reflects several significant federal and state laws, rules and regulations, policies, standards and guidelines that providers doing business with the State must be aware of and comply with if applicable to the services being provided. Links to further guidance are included in the Appendix. The list is intentionally US-centric, and is not intended to be all-inclusive. Further, since laws, regulations, requirements and industry guidelines change, consulting definitive sources to assure a clear understanding of compliance requirements is critical. Many NYS agencies may have additional program compliance requirements that must be considered in addressing compliance. (e.g., DMV Privacy Act, Public Service Law, etc.).

To the extent that Contractor, its employees, agents or subcontractors have access to Federal, State or Local government regulated data pursuant to their responsibilities under the Contract, Contractor agrees that it will abide by, and will require in writing its employees, agents or subcontractors to similarly abide by any such requirements including the execution of any documents certifying their compliance with such requirements.

5. Press Releases

Contractor agrees that no brochure, news/media/press release, public announcement, memorandum or other information of any kind regarding the Contract shall be disseminated in any way to the public, nor shall any presentation be given regarding the Contract without the prior written approval by the Director or his/her designee, which written approval shall not be unreasonably withheld or delayed provided, however, that Contractor shall be authorized to provide copies of the Contract and answer any questions

relating thereto to any State or Federal regulators or, in connection with its financial activities, to financial institutions for any private or public offering.

6. General Security Provisions

Contractor shall comply fully with all information security procedures and policies of the State including but not limited to the following:

- Acceptable Use of Information Technology Resources Policy
- Information Security Policy
- Security Logging Standard
- Information Security Risk Management Standard
- Information Security Controls Standard
- Sanitization/Secure Disposal Standard
- Mobile Device Security Standard
- Remote Access Standard
- Secure System Development Life Cycle Standard
- Secure Configuration Standard
- Secure Coding Standard

ITS Security Policies and Standards may be found at <http://www.its.ny.gov/tables/technologypolicyindex.htm/security>

Contractor shall comply fully with all NYS/ITS fingerprinting and background check procedures, which are communicated to the Contractor by the State during the performance of the Contract.

Contractor warrants its employees, agents and subcontractors are properly informed and trained regarding generally accepted information security practices and NYS information security policies and standards <https://www.its.ny.gov/tables/technologypolicyindex> and are prohibited from disclosing confidential information to any persons without a need to know.

Contractor shall also comply fully with all requirements of this Contract pertaining to security requirements specific to the services Contractor is providing to ITS under this Contract. If any software application or vulnerability security scanning undertaken hereunder reveals vulnerabilities or any other security risks attendant to the provided solution Contractor is responsible for ensuring those vulnerabilities and risks are promptly remediated to ITS's reasonable satisfaction.

In addition to the specific security provisions required herein, Contractor shall also use commercially reasonable best efforts to address and remediate any vulnerabilities associated with the types of configuration services it is providing under this Contract which appear, as of the date any modification or upgrade request is made by ITS, on the CWE/SANS list of the "TOP 25 Most Dangerous Programming Errors." See: <http://www.sans.org/top25errors/>

a) Compartmentalization of Job Duties

Contractor, its employees, agents and subcontractors shall have robust compartmentalization of job duties, and limit staff and subcontractor knowledge of State Data to that which is absolutely needed to perform job duties.

b) Encryption

Contractor shall use industry standard security measures, including standard encryption protocols in compliance with the NYS ITS Encryption Standard, NYS-S14-007 <https://www.its.ny.gov/document/encryption-standard>, to protect and guard the availability and security of all State Data. If the requirements set forth in the RFP and/or contract are not the same as the NYS ITS policies, then the more restrictive policy applies. Contractor shall be strictly prohibited from using State Data in any fashion other than that defined herein or authorized in writing by ITS.

All NYS data will be encrypted including, but not limited to,

- 1) Data in transit
- 2) Data at rest

c) Data Ownership, Transparency, Accessibility, Location, Transport, Protection and Destruction

- 1. Data Ownership:** All State data is owned exclusively by the State and will remain the property of the State. Contractor is permitted to use data solely for the purposes set forth in the RFP and the Contract, and for no other purpose. At no time shall the Contractor access, use, or disclose any confidential information (including personal, financial, health, or criminal history record information or other sensitive criminal justice information) for any other purpose. The Contractor is strictly prohibited from releasing or using data or information for any purposes other than those purposes specifically authorized by the State. Contractor agrees that State data 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.
- 2. Migration:** Contractor's services performed under this Contract will ensure easy migration of the State's Data including its Confidential Information under this Contract by providing its solution in a manner designed to do so. This may include Contractor keeping State Data separate from processes of the software itself and maintaining that information in a format that allows ITS to easily transfer it to an alternative application platform. Contractor will make its Application Programming Interfaces (APIs) available to ITS.
- 3. Data Access and Location:** Data Access and Location– the Contractor must ensure that all State Data related to this Contract is stored in a controlled access environment to ensure data security and integrity. All access to State data, physical or virtual, must be conducted within CONUS and have adequate security systems in place to protect against the unauthorized access to the facilities and data stored therein. The Contractor shall not send or permit to be

sent to any location outside of the CONUS, any State data related to this Contract. Contractor will provide the State a list of the physical locations where the data is stored at any given time and will update that list if the physical location changes. Access into and within the facilities must be restricted through an access control system that requires positive identification 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 the data and to track access. Access for projects outside of those approved by the State or ITS is prohibited.

4. Physical Data Transport: The Contractor shall use, if applicable, reputable means to physically transport State data. Deliveries must be made either via hand delivery by an employee of the Contractor or by restricted delivery via courier (e.g., FedEx, United Parcel Service, United States Postal Service) with shipment tracking and receipt confirmation. This applies to transport between the Contractor's offices, to and from subcontractors, and to the State.

5. Data Protection and Transmission: Contractor shall use appropriate means to preserve and protect State data. This includes, but is not limited to, use of stable storage media, regular data backups and archiving, password protection of volumes, and data encryption. Contractor must, in accordance with applicable law and the instructions of the State, 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. In the event that 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 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.

Contractor agrees that any and all State data will be stored, processed and maintained solely on designated target devices, and that no State data at any time will be processed on or transferred to any portable computing device or any portable storage medium, unless that device or storage medium is a necessary and approved component of the authorized business processes covered in the contract/agreement and or any addendum thereof, or the Contractor's designated backup and recovery processes, and is encrypted in accordance with all current federal and State statutes, regulations and requirements, to include requirements for data defined as confidential, financial information, personal private and sensitive information (PPSI), personally identifying information (PII) or personal health information (PHI) by statute or regulations. The Contractor shall encrypt data at rest, on file storage, database storage, or on back-up media, and in transit in accordance with state and federal law, rules, regulations, and requirements. The solution shall provide the ability to encrypt data in motion and at rest in compliance with state or federal law. Contractor shall use secure means (HTTPS) for all electronic transmission or exchange of system, user and application data with the State.

6. Data Return and Destruction: At the expiration or termination of the Contract, at the State's option, the Contractor must provide ITS with a copy of the State data, including metadata and attachments, in a mutually agreed upon, commercially standard format and give the State continued access to State data for no less than ninety (90) days beyond the expiration or termination of the Contract. Thereafter, except for data required to be maintained by law or this contract, Contractor shall destroy State data from its systems and wipe all its data storage devices to eliminate any and all State data from Contractor's systems. The sanitization process must be in compliance NYS Security Policy NYS-S13-003, <https://www.its.ny.gov/document/sanitizationsecure-disposal-standard>, and, where required, CJIS sanitization and disposal standards. 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 ITS, in writing, that it has complied with the provisions of this paragraph. The State may withhold payment to Contractor if State data is not released to ITS in accordance with the preceding sections.

d) Information Security Breach and Notification Act

In accordance with the Information and Security Breach Notification Act (ISBNA) (Chapter 442 of the Laws of 2005, as amended by Chapter 491 of the Laws of 2005), a Contractor with ITS shall be responsible for all applicable provisions of the ISBNA and the following terms herein with respect to any "private information" (as defined in the ISBNA) received by or on behalf of ITS under this Contract.

1. Contractor shall supply ITS with a copy of its notification policy, which shall be modified to be in compliance with this provision, as well as ITS's notification policy.
2. Contractor must encrypt any database fields and backup tapes that contain private information, as set forth in the ISBNA.
3. Contractor must ensure that private information is encrypted in transit to/from their systems.
4. In general, contractor must ensure that private information are 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.
5. Contractor must monitor for breaches of security to any of its systems that store or process private information owned by ITS.
6. Contractor shall take all steps as set forth in ISBNA to ensure private information shall not be released without authorization from ITS.
7. In the event a security breach occurs as defined by ISBNA Contractor shall notify ITS within 4 hours of becoming aware of the breach and commence an investigation in cooperation with ITS to determine the scope of the breach pursuant to the Notice requirements in Section 24 below.
8. Contractor shall also take immediate and necessary steps needed to restore the information security system to prevent further breaches.
9. Unless the Contractor is otherwise instructed, Contractor is to first seek consultation and receive authorization from ITS prior to notifying the individuals whose personal identity information was compromised by the breach of security, the New York Attorney General; the NYS Division of State Police; and

the Department of State's Division of Consumer Protection or any consuming reporting agencies of a breach of the information security system or concerning any determination to delay notification for law enforcement investigations.

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

Data Breach - Required Contractor Actions

Unless otherwise provided by law, in the event of a Data Breach, the Contractor shall:

1. Notify the ITS EISO by telephone as soon as possible, but in no event more than two (2) hours from the time the Contractor either has knowledge of a Data Breach;
2. Consult with and receive authorization from the ITS as to the content of any notice to affected parties prior to notifying any affected parties to whom notice of the Data Breach is required;
3. Coordinate all communication regarding the Data Breach with the ITS EISO and Authorized User(s);
4. Cooperate with ITS in attempting (a) to determine the scope and cause of the breach; and (b) to prevent the future recurrence of such security breaches; and
5. Take corrective action in the timeframe required by the ITS. If Contractor is unable complete the corrective action within the required timeframe, in addition to any other remedies available, ITS may contract with a third party to provide the required services until corrective actions and services resume in a manner acceptable to the ITS, or until the ITS has completed a new procurement for a replacement service system. The Contractor will be responsible for the cost of these services during this period.

Nothing herein shall in any way (a) impair the authority of the OAG to bring an action against Contractor to enforce the provisions of the New York State Information Security Breach Notification Act (ISBNA) or (b) limit Contractor's liability for any violations of the ISBNA or any other applicable statutes, rules or regulations.

e) Secure Development, Configuration and Lifecycle

The Contractor shall agree to maximize the security 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. Contractor warrants, covenants and represents that it shall comply fully with the applicable NYS Policies, Standards and Guidelines during the term of this Contract including, but not limited to, the NYS Security Standard on Secure System Development Life Cycle - NYS-S13-001, NYS Secure Coding Standard - NYS-S13-002 and the NYS Secure Configuration, NYS Secure Configuration Standard-NYS-S14-008 located at: <https://www.its.ny.gov/document/secure-coding-standard>

and <https://www.its.ny.gov/document/secure-configuration-standard> including any successor policies standards and guidelines.

The Contractor shall take all actions necessary to protect information regarding security issues and associated documentation, to help limit the likelihood that vulnerabilities in operational software are exposed.

Consistent with the provisions of the Contract, the Contractor shall use the highest applicable industry standards for sound secure software development practices to resolve all security issues as quickly as possible. The “highest applicable industry standards” shall be defined as the degree of care, skill, efficiency, and diligence that a prudent person possessing technical expertise in the subject area and acting in a like capacity would exercise in similar circumstances.

1) Security Review

(a) Independent Review

Before releasing any major upgrade releases to its Software to the State, the Contractor shall have the Software reviewed for security flaws at Contractor’s expense. The scope of this review would include assessing the software for security flaws from the perspective of the deployed application / architecture. The scope does not mean code review, but rather is focused on the deployed web application instance.

The State reserves the right to perform its own independent application security review in addition to the Contractor’s review.

(b) Review Coverage

Security review shall cover all aspects of the Software delivered, including third-party modules, units, integration points, components, and libraries. The review coverage will include all aspects of the application layer that are externally facing or part of the service infrastructure will be assessed.

(c) Vulnerability Scanning and Penetration Testing

The Contractor agrees that, before any Software is released to the State or Authorized User, the Contractor will perform application vulnerability scanning and penetration testing.

The Contractor shall provide to the State written documentation of the results of any scans and tests along with a mitigation plan. The Contractor agrees that vulnerabilities identified by the vulnerability scanning and penetration testing shall be mitigated within a reasonable period of time to avoid any risk to the State.

(d) Scope of Review

At a minimum, the review shall cover the most common software vulnerabilities. The review shall include a combination of vulnerability scanning, penetration testing, and static analysis of the source code. This will be a combination of vulnerability scanning and pen testing, not static source code analysis.

e) Issues Discovered

Overall application security ratings with aggregate number of flaws found will be reported to both the State and the Contractor. Detailed reports of specific vulnerability instances within the application will only be provided to the Contractor. Discovered vulnerabilities and / or flaws that are discovered will be documented with a best effort at outlining required remediation in each area.

2) Security Issue Management

(a) Identification

Contractor shall track all security issues uncovered during the security review and the entire development life cycle, whether a requirements, design, implementation, testing, deployment, or operational issue. The risk associated with each security issue will be evaluated and documented. Security issues in the deployment of the application will be documented. These include vulnerabilities both in the software and architecture that is assessed.

(b) Investigation and Resolution of Security Issues

If security issues are discovered or reasonably suspected, Contractor shall perform an investigation to determine the nature of the issue.

The issue shall be considered "novel" if it is not covered by the security requirements and is outside the reasonable scope of security testing.

If novel, Contractor and State agree to scope the effort required to resolve the novel security issue(s), and to negotiate in good faith to achieve an agreement to perform the required work to address them.

If not novel, Contractor shall use all commercially reasonable efforts consistent with sound software development practices, taking into account the severity of the risk, to resolve all security issues not considered novel as quickly as possible.

(c) Remediation

Security issues that are identified before software is released to the State shall be fixed by the Contractor before releasing the Software. Security issues discovered after release shall be handled per the terms of the Contract. Steps and / or guidance on how to remediate will be outlined in the report delivered to NYS.

3) Assurance

(a) Certification

With execution of the Contract, the Contractor will provide to the State a copy of the Contractor's secure coding best practices policy. Upon delivery of the Software to the State the Contractor shall certify to the State in writing that the Contractor complied with the policy in the performance of its obligations under the Contract as well as certify that all security activities have been performed, and all identified security issues have been documented and resolved. Any exceptions to the certification status shall be fully documented with the delivery.

- 4) Personnel and Organization
 - (a) Contractor will assign responsibility for security to a single senior technical resource, to be known as the project Security Architect. The Security Architect will certify the security of each deliverable.
 - (b) Contractor will be responsible for verifying that all members of the development team have been trained in secure programming techniques.
 - (c) Contractor agrees to perform appropriate background investigation of all development team members.