

ITS-IFB-2016-091WJ
Onsite Confidential Data Destruction
Exhibit 2 – Information Security Requirements

ID	Requirement
	Privacy & Security
Data Ownership	All State data is owned exclusively by the State and will remain the property of the State for the sole use on this Contract. Data means "..." . Only ITS or entities authorized in writing by ITS will determine the terms and conditions of access to the data. All State Data shall be considered Confidential Information subject to the terms of this Contract and shall not be released to any third party without explicit written permission from the ITS Director or designee.
Compliance with Security Policies & Procedures	Contractor agrees to preserve the confidentiality, integrity and accessibility of State data with administrative, technical and physical measures that conform to federal, State and Agency mandates, and generally recognized industry standards and practices, to include the National Institute of Standards and Technology (NIST) 800-53 guidelines for implementing system security and privacy controls. Accordingly, Contractor must comply with State security policies and procedures, including but not limited to:
	· 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
Compliance with State & Federal Laws, Rules, Regulations, and Policies	Contractor must also comply with State and Federal laws, rules, regulations, and policies, as well as all State and Authorized User policies regarding compliance with various confidentiality and privacy laws, rules and regulations, including but not limited to NYS Technology Law, Health Insurance Portability and Accountability Act (HIPAA); the Health Information Technology for Economic and Clinical Health Act (HITECH); IRS Publication 1075; Code of Federal Regulations, Title 42: Public Health, Part 2 – Confidentiality of Alcohol and Drug Abuse Patient Records; Family Educational Rights and Privacy Act (FERPA); the federal Driver’s Privacy Protection Act of 1994 (DPPA); the Criminal Justice Information Services (CJIS) Security Policy.

ITS-IFB-2016-091WJ
Onsite Confidential Data Destruction
Exhibit 2 – Information Security Requirements

Right to Inspect	<p>The State has the right to review Contractor’s procedures, practices and controls related to the protection of Agency data and information assets. Upon request, Contractor will make available for review policies, procedures, practices and documentation related to the protection of State data and information assets, including but not limited to related to information security governance, network security, risk and compliance management policies and procedures, personnel security background screening/checks and vetting procedures, secure systems/software development protocols, change/release management, testing, quality assurance, vulnerability management, secure disposal/sanitization and documentation. Contractor may be asked to provide a recent independent audit report on security controls prior to formal awarding of any contract resulting from this IFB or at any time during the Contract term. The State and any regulatory authority having jurisdiction over the State or Authorized Users shall have the right to send its officers and employees into the offices and plants of the Contractor for inspection of the facilities and operations used in the performance of any work under the resulting Contract. On the basis of such inspection, specific measures may be required in cases where the Contractor is found to be noncompliant with Contract safeguards.</p>
Training & Qualifications	<p>The Contractor represents and warrants that all Contractor staff have received general security awareness training, as well as specific training related to the State data, in compliance with State and Federal requirements. Contractor staff may be required to execute an ITS Nondisclosure Contract, either before or upon arrival at the work site or if in ITS’s sole discretion the employee(s) will otherwise have access to critical State networks, equipment or data. “Contractor Staff” includes all officers, agents, employees and subcontractors of the Contractor who shall perform Services under this Contract or have access to State data. All Contractor Staff, shall possess the necessary qualifications, training, licenses, and permits as may be required within the jurisdiction where the Services specified are to be provided or performed, and shall be legally entitled to work in such jurisdiction. All persons, corporations, or other legal entities that perform Services under the Contract on behalf of Contractor shall, in performing the Services, comply with all applicable Federal and State laws concerning employment in the United States.</p>
Handling of Data	<p>Contractor is permitted to use data solely for the purposes as described in the IFB and its resulting 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) or 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.</p>
	<p>Contractor agrees that any and all data provided or exchanged shall be used expressly and solely for the authorized purposes enumerated in the contract/agreement and or any addendum thereof. Data shall not be distributed, used, repurposed or shared across other applications, environments, or business units of the contractor. Contractor agrees that no State data of any kind shall be transmitted, exchanged 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.</p>

ITS-IFB-2016-091WJ
Onsite Confidential Data Destruction
Exhibit 2 – Information Security Requirements

	<p>Contractor agrees that all Contractor staff, or approved subcontractors [Note: carefully consider if subcontracting should be allowed, and terms and conditions associated with same.] with access to State data shall cooperate in executing a written confidentiality/nondisclosure agreement and/or security addendum under applicable confidentiality and privacy laws, rules, and regulations, upon request by the State or any Authorized User.</p>
	<p>Confidentiality: Except as may be required by applicable law or a court of competent jurisdiction, the Contractor, its agents, employees, officers, partners and subcontractors shall maintain strict confidence with respect to any Confidential Information to which the Contractor, its agents, employees, officers, partners or subcontractors have access. This provision shall survive termination of this Contract. Contractor shall indemnify and hold ITS, and the State harmless from any loss or damage to the State resulting from the disclosure by the Contractor, its agents, employees, officers, partners or subcontractors of such Confidential Information, in accordance with the terms and conditions of this Contract.</p>
	<p>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.</p>
	<p>Data Transmission: Contractor shall use secure means (HTTPS) for all electronic transmission or exchange of system, user and application data with the State.</p>
	<p>Data Protection: The Contractor shall use appropriate means to preserve and protect the 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. The Contractor must, in accordance with applicable law and the instructions of the Agency, 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 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.</p>
	<p>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</p>

ITS-IFB-2016-091WJ
Onsite Confidential Data Destruction
Exhibit 2 – Information Security Requirements

	<p>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.</p>
	<p>Destruction: At the Expiration or Termination of the Contract, at State’s option, the Contractor will provide ITS with a copy of the State data in a mutually agreed upon, commercially standard format at no additional charges. After provision of a copy of the State data, the Contractor will either: (a) destroy State data; or (b) export and return, at no additional cost to ITS, in part or in its entirety at ITS’s option including metadata and attachments, which is accessible to ITS and capable of being used by ITS. Contractor will then destroy, except for the documents required to be maintained , any copies of the State data from Contractor’s system. Under either option (a) or (b) above, Contractor will certify in writing destruction of State’s data. If ITS does not advise Contractor of what ITS wants Contractor to do with State’s data, Contractor will continue to hold it for 90 days while making reasonable efforts to contact and secure an answer from ITS. ITS has the right to withhold payment to Contractor if State’s data is not released to ITS in accordance with the preceding sections. The Contractor will be required to wipe all data storage devices to eliminate any and all data by the State. 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.</p>
<p>Suitability Determinations, Security Clearances and Background Checks</p>	<p>The Contractor must comply with all State and Federal onboarding and security clearance requirements, at its own expense. The Contractor is responsible for completing background checks and when specified by the State, security clearances. Contractor is also responsible, at its own expense, for making suitability determinations on its contractor staff prior to the staff member performing any work in connection with this Contract. For purposes of this provision, a “suitability determination” is a determination that there are reasonable grounds to believe that an individual will likely be able to perform the Contract requirements without undue risk to the interests of the State. Upon request of the State, the Contractor shall certify to the State that the background checks and suitability determinations required by this provision have been completed for all employees performing work in connection with this Contract. The State may require that the Contractor replace personnel at the discretion of the State. The State may also require the execution of a nondisclosure agreement with each individual assigned to provide work, background checks, and fingerprint checks of Contactor personnel with access to State information. Fees in connection with fingerprints required hereunder are to be paid by Contractor.</p>

ITS-IFB-2016-091WJ
Onsite Confidential Data Destruction
Exhibit 2 – Information Security Requirements

	Failure of a security clearance or non-compliance with this Section will disqualify any Contractor Staff, from performing any Services on this Project. All expenses, including travel and lodging, associated with the onboarding and security clearance process including fingerprinting of Contractor Staff are the responsibility of the Contractor and are not reimbursable. If Contractor Staff are removed from working under the resulting Contract, they may be subject to all onboarding and security clearance requirements if they are returned to performing Services under the contract. The State also reserves the right to conduct a security background check or otherwise approve any employee, Subcontractor or agent furnished by Contractor performing work on this Contract or having access to State data and to refuse access to or require replacement of any personnel at its discretion for any reason. The State reserves the right to reject and/or bar from a State facility for cause any employee, Subcontractor, or agents of the Contractor.
	The Contractor shall, at the State's option, conduct an annual security risk assessment, performed by an independent third-party security Contractor, to verify that the Contractor's environment(s) is secure and that applicable systems meet applicable standards described herein.
Risk Assessment	The Contractor shall provide a certified copy of the Security Risk Assessment to the State within 30 days of completion (assuming State exercises the option to conduct such an assessment). Issues identified in the Risk Assessment should be addressed with a plan for resolution, and resolved within 90 days of the Risk Assessment.
Insurance	Contractor, at its sole cost and expense, will obtain, keep in force, and maintain an insurance policy (or policies) that provides express coverage for privacy and data security breaches, to include coverage for reasonable costs in investigating and responding to privacy and/or data breaches with the following minimum limits: \$X,XXX,XXX Each Claim and \$X,XXX,XXX Aggregate.
Security	Contractor must protect State data from unauthorized access, use, alteration, disclosure, or dissemination. Contractor shall implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of data. Contractor shall ensure that such security measures are regularly reviewed and revised to address evolving threats and vulnerabilities. All facilities used to store and process data will employ commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, use, alteration, disclosure, or dissemination.
	If cloud based services are a component of the solution or services to be provided by Contractor, Contractor must comply with the standards set forth by Cloud Security Alliance and/or FedRAMP (https://www.fedramp.gov) for cloud services, and other applicable federal and/or New York State laws, regulations and requirements.
	In the event of a security incident the Contractor shall immediately notify the State. The Contractor shall then commence an investigation to determine the scope of the incident,

ITS-IFB-2016-091WJ
Onsite Confidential Data Destruction
Exhibit 2 – Information Security Requirements

	<p>and advise the State of the results of that initial investigation. The Contractor and the State shall together determine whether there has been a breach of security, and restore security to prevent any further incidents. Except as otherwise instructed by ITS, the Contractor shall, to the fullest extent possible, first consult with and receive authorization from ITS prior to notifying any individuals, the State Consumer Protection Board, or the 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. The Contractor shall fully cooperate with the State in investigation of any breach, security incident or vulnerability, to include cooperation with activities necessary for the State to determine the need for notification and/or to provide the notification(s) required. Within twenty-four (24) hours of the notification by the Contractor, the Contractor must report to the State the steps taken or proposed to be taken in response to any instance of unauthorized access. The Contractor must also notify the State of the steps taken to prevent similar instances in the future as soon as is practicable after the unauthorized access is discovered.</p>
	<p>Contractor shall comply with the provisions of the New York State Information Security Breach and Notification Act (General Business Law Section 889-aa; State Technology Law Section 208). Contractor shall be liable for the costs associated with such breach if caused by Contractor's negligent or willful acts or omissions or the negligent or willful acts or omissions of Contractor's agents, officers, employees or subcontractors. The following terms herein with respect to any "private information" (as defined in the ISBNA) or other confidential or sensitive data received by or on behalf of ITS under this Contract.</p>
	<p>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.</p>
	<p>2. Contractor must encrypt any database fields and backup tapes that contain private, confidential, or sensitive information.</p>
	<p>3. Contractor must ensure that private, confidential, or sensitive information is encrypted in transit to / from their systems.</p>
	<p>4. In general, contractor must ensure that private, confidential, or sensitive information is not displayed to users on computer screens or in printed reports; however, specific users who are authorized to view the private, confidential, or sensitive data elements and who have been properly authenticated may view/receive such data.</p>
	<p>5. Contractor must monitor for breaches of security to any of its systems that store or process private, confidential, or sensitive information owned by ITS.</p>
	<p>6. Contractor shall take all steps as set forth in ISBNA to ensure private, confidential, or sensitive information shall not be released without authorization from ITS.</p>
	<p>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.</p>
	<p>8. Contractor shall also take immediate and necessary steps needed to restore the information security system to prevent further breaches, as well as immediately preserve any potential forensic evidence relating to the incident.</p>

ITS-IFB-2016-091WJ
Onsite Confidential Data Destruction
Exhibit 2 – Information Security Requirements

	<p>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.</p>
	<p>10. Contractor shall be responsible for providing all notices required by law and for all costs associated with providing said notices.</p>
	<p>This policy and procedure shall not impair the ability of the Attorney General to bring an action against the Contractor to enforce all provisions of the ISBNA or limit the Contractor's liability for any violations of the ISBNA. In the event of a breach of the security of the system (as defined by ISBNA) caused by Contractor's negligent or willful acts or omissions, or the negligent or willful acts or omissions of Contractor's agents, officers, employees or subcontractors, Contractor shall be responsible for all costs associated with providing the notice required by the ISBNA. In the event that the security of personal information is breached in violation of the ISBNA, from a system maintained by the Contractor, then the Contractor shall be responsible for providing notice of breach to the person(s) to whom such information pertains. In the event that the Contractor is authorized to share such information with another entity, the Contractor must hold its recipient responsible for providing such notice. Prior approval from ITS is required before any notifications are made to such persons. In addition to any responsibilities of Contractor under the Contract for reporting breaches of personal information Contractor must immediately report to ITS any breaches of any of the state's Confidential Information whether it consists of personal information or otherwise.</p>
	<p>Contractor shall ensure that the personnel charged with carrying out services under this Contract are aware of Contractor's obligations to ITS hereunder. Contractor's staff browsing, viewing, altering, appending or modifying the 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 this Contract.</p>
	<p>The Contractor shall be solely liable for costs associated with any data breach associated with services provided through this contract, including but not limited to notification and any costs incurred or damages assessed.</p>
Contingency Plans	<p>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.</p>

ITS-IFB-2016-091WJ
Onsite Confidential Data Destruction
Exhibit 2 – Information Security Requirements

Subcontracting	The Contractor shall extend all requirements set forth herein by contract to all subcontractors used by Contractor. Contractor agrees that all Contracts between the Contractor and its Subcontractors shall be by bona fide written Contract. All such contracts shall contain provisions specifying: (i) that the work performed by the Subcontractor must be in accordance with the terms of the Contract, including but not limited to Appendix A; (ii) that the subcontractor must pass through all terms and conditions of the Contract, including but not limited to Appendix A, to any lower tier subcontracts; (iii) that nothing contained in the subcontract shall impair the rights of the State; (iv) that nothing contained in such subcontract or under the Contract shall create any contractual relationship between the Subcontractor and the State; (v) that subcontractors shall maintain and protect against any unauthorized disclosure all records with respect to work performed under the subcontract in the same manner as required of the Contractor; (vi) that the State shall have the same authority to audit the records of all subcontractors as it does those of the Contractor; and (vii) that the subcontractor shall cooperate with any investigation, audit, or other inquiry related to the Contract or any litigation relating thereto.
	The Contractor shall not in any way be relieved of any responsibility under the Contract by any subcontract.
	The Contractor shall inform each Subcontractor fully and completely of all provisions and requirements of the Contract, including those relating either directly or indirectly to the Deliverables to be provided and the materials to be furnished or Services provided pursuant to its respective subcontract, and every such subcontract shall expressly stipulate that all labor performed and materials furnished pursuant thereto shall strictly comply with the requirements of the Contract.
	Failure to disclose the identity of any and all Subcontractor(s) used by the Contractor as required hereunder may, at the sole discretion of the State Project Manager, result in a disqualification of the Subcontractor, if not immediately cured, or may result in termination of the Contract for cause. The Contractor, within three business days of the State Project Manager’s request, shall file with the State a copy of any subcontract.
	The Contractor shall pay all Subcontractors for and on account of Services and/or Deliverables provided by such Subcontractors in accordance with the terms of their respective subcontracts. If and when required by the State, the Contractor shall submit satisfactory evidence that it has made such payment.
	The Contractor shall be solely responsible to the State and Authorized Users for the acts or defaults of its Subcontractor(s) and of such Subcontractors' officers, agents, and employees, each of whom shall for this purpose, be deemed to be the agent or employee of the Contractor to the extent of its subcontract. Any Deliverable provided or furnished by a Subcontractor shall be deemed for purposes of the Contract to be provided or furnished by the Contractor.

ITS-IFB-2016-091WJ
Onsite Confidential Data Destruction
Exhibit 2 – Information Security Requirements

Public Information	Disclosure of items related to this Contract shall be permitted consistent with the laws of the State of New York and specifically the Freedom of Information Law (FOIL) contained in Section 87 of the Public Officers Law. The State shall take reasonable steps to protect from public disclosure any of the records relating to this procurement that are otherwise exempt from disclosure under that statute. Information constituting trade secrets or critical infrastructure information, for purposes of FOIL, must be clearly marked and identified as such upon submission. If the Contractor intends to request an exemption from disclosure under FOIL for trade secret materials or critical infrastructure information, the Contractor shall, at the time of submission, request the exemption in writing and provide an explanation of: (i) why the disclosure of the identified information would cause substantial injury to the competitive position of the Consultant; or (ii) why the information constitutes critical infrastructure information which should be exempted from disclosure pursuant to §87(2) of FOIL. Acceptance of the identified information by the State does not constitute a determination that the information is exempt from disclosure under FOIL. Determinations as to the availability of the identified information will be made in accordance with FOIL at the time a request for such information is received by the State.
Legal Requests	The Contractor shall disclose to ITS a description of their roles and responsibilities related to electronic discovery, litigation holds, discovery searches and expert testimonies. The Contractor shall disclose its process for responding to subpoenas, service of process and other legal requests.