Exhibit A- Data Security Terms and Conditions

1. Data Security Terms and Conditions

To the extent that Contractor has received an award for RFP 2469, for Board of Elections Online Voter Registration Intake System, the following terms and conditions shall apply.

For the duration of this Agreement, the Online Voter Registration Intake System shall conform to the specifications, documentation, performance standards (including applicable license duration, warranties, guarantees, Service Level Agreements, service commitments, and credits) as defined in the RFP and this document.

1.1 Protection of Data and Software

Contractor is responsible for providing security for all Data and software related to the services the Contractor is providing under the Agreement.

All Data security provisions agreed to by SBOE and Contractor within this Agreement may not be diminished for the duration of this Agreement without prior written agreement by the parties amending this Agreement.

1.2 Security Policies and Notifications

1.2.1 State Security Policies and Procedures

The Contractor and its personnel shall review and be familiar with all State security policies, procedures and directives currently existing or implemented during the term of the Contract, including NYS Information Technology Policy NYS-P03-002 Information Security Policy (or successor policy).

1.2.2 Security Incidents

Contractor shall address any Security Incidents in the manner prescribed in NYS Information Technology Policy NYS-P03-002 Information Security Policy, https://its.ny.gov/document/information-security-policy, (or successor policy), including the New York State Cyber Incident Reporting Procedures incorporated therein or in such successor policy.

1.3 Data Breach - Required Contractor Actions

In accordance with the New York State Information and Security Breach Notification Act (ISBNA) (Chapter 442 of the Laws of 2005, as amended by Chapter 491 of the Laws of 2005), the Contractor 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 SBOE under this Agreement.

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

1. Notify SBOE or their designated contact person(s), by telephone as soon as possible, but in no event more than 24 hours from the time the Contractor confirms the Data Breach;
2. Consult with and receive authorization from SBOE 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, either by statute or by SBOE;
3. Coordinate all communication regarding the Data Breach with SBOE (including possible communications with third parties);
4. Cooperate with SBOE and any contractor working on behalf of SBOE 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 such corrective actions that the Contractor deems necessary to contain the Data Breach. Contractor shall provide written notice to SBOE as to all such corrective actions taken by the Contractor to remedy the Data Breach. Unless otherwise agreed to in the this Agreement, if Contractor is unable to complete the correctiveaction within the required timeframe, then (i) the SBOE may contract with a third party to provide the required services until corrective actions and services resume in a manner acceptable to SBOE, or until SBOE has completed a new procurement for a replacement service system; (ii) and the Contractor will be responsible for the reasonable cost of these services during this period.

Nothing herein shall in any way (a) impair the authority of the SBOE 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.

1.4 Data Ownership, Access and Location

1.4.1 Data Ownership

The SBOE shall own all right, title and interest in Data.

1.4.2 Access to Data

The SBOE shall have access to its Data at all times, through the term of the This Agreement, plus theapplicable period as specified in Section 1.10 Expiration, Termination or Suspension of Services, below.

The SBOE shall have the ability to import or export Data in piecemeal or in its entirety at the SBOE's discretion at no charge to SBOE. This includes the ability for SBOE to import or export Data to/from other Contractors.

1.4.3 Contractor Access to Data

The Contractor shall not copy or transfer Data unless authorized by SBOE. In such an event the Data shall be copied and/or transferred in accordance with the provisions of this Section. Contractor shall not access any Data for anypurpose other than fulfilling the service. Contractor is prohibited from Data Mining, cross tabulating, monitoring SBOE's Data usage and/or access, or performing any other Data analytics other than those required within the This Agreement. At no time shall any Data or processes (e.g. workflow, applications, etc.), which either are owned or usedby SBOE be copied, disclosed, or retained by the Contractor or any party related to the Contractor. Contractors are allowed to perform industry standard back-ups of Data. Documentation of back-up must be provided toSBOE upon request. Contractor must comply with any and all security requirements within this Agreement.

1.4.4 Data Location and Related Restrictions

All Data shall remain in the Continental United States(CONUS). Any Data stored, or acted upon, must be located solely in Data Centers in CONUS. Services which directly or indirectly access Data may only be performed from locations within the CONUS. All Data in transit must remain in CONUS and be encrypted in accordance with Section 1.6, Encryption, below.

1.4.5 Support Services

All helpdesk, online, and support services which access any Data must be performed from within CONUS. At no time will any "Follow the Sun" support, utilizing geographic locations outside CONUS, be allowed to access Data directly, or indirectly.

1.5 Transferring of Data

1.5.1 General

Except as required for reliability, performance, security, or availability of the services, the Contractor will not transfer Data unless directed to do so in writing by SBOE. All Data shall remain in CONUS.

At the request of SBOE, the Contractor will provide the services required to transfer Data from existing Databases to physical storage devices, to facilitate movement of large volumes of Data.

1.5.2 Transfer of Data at End of Contract and/or This Agreement Term

At the end of the Contract, Contractor may be required to facilitate transfer of Data to a new Contractor. This transfer must be carried out as specified by SBOE in this Agreement.

1.5.3 Transfer of Data; Charges

Contractor cannot charge for the transfer of Data.

1.5.4 Transfer of Data; Contract Breach or Termination

Notwithstanding Section 1.5.3 - Transfer of Data; Charges, in the case of Contract breach or termination for cause of the Contract, all expenses for the transfer of Data shall be the responsibility of the Contractor.

1.5.5 Transfer Format

Transfers may include, but are not limited to, conversion of all Data into or from an industry standard format or providing an application programming interface.

1.6 Encryption

Data must be encrypted at all times unless specifically outlined otherwise in this Agreement. At a minimum,encryption must be carried out at the most current NYS Encryption Standard (NYS-S14-007), (or successor policy with key access restricted to SBOE only, unless with the express written permission of SBOE.

All Data in transit must be handled in accordance with ITS Policy NYS-S14-007, https://its.ny.gov/document/encryption-standard, (or successor) or the National Institute of Standards and Technology (NIST) Federal Institute Processing Standard (FIPS-140-2) or Transport Layer Security (TLS1 or TLS2 or successor).

This Agreement shall specify the respective responsibilities of SBOE and the Contractor for the encryption of Data.

1.7 Requests for Data by Third Parties

Unless prohibited by law, Contractor shall notify SBOE in Writing within 24 hours of any request for Data (including requestor, nature of Data requested and timeframe of response) by a person or entity other than SBOE, and the Contractor shall secure Written acknowledgement of such notification from SBOE before responding to the request for Data.

Unless compelled by law, the Contractor shall not release Data without SBOE's prior Written approval.

1.8 Security Processes

Contractor shall cooperate with all reasonable SBOE requests for a Written description of Contractor's physical/virtual security and/or internal control processes. The SBOE shall have the right to reject any Contractor's RFP response or terminate this Agreement when such a request has been denied.

1.9 Upgrades, System Changes and Maintenance/Support

The Contractor shall give a minimum of five business days advance written notice to the designated SBOE contact of any upgrades, system changes and maintenance/support actions that may potentially impact services described in this Agreement.

Upgrades, system changes, and maintenance/support actions which are required by system vulnerabilities or emergency situations shall be carried out by the Contractor immediately to protect the system. SBOE shall be notified by the Contractor as soon as possible after the change has taken place.

Contractor shall provide documentation of upgrades, system changes and maintenance/support actions upon request from SBOE.

1.10 Expiration, Termination or Suspension of Services

1.10.1 Return of Data

The Contractor shall return Data in a format agreed upon within this Agreement or as agreed to with SBOE. This can, if specified within this Agreement, be carried out by providing an application programming interface or other such efficient electronic tools. The Contractor must certify all Data has been removed from its systems, where applicable, and removed from backups within timeframes established in this Agreement or as agreed to with SBOE.

1.10.2 Suspension of Services

During any period of suspension of service, SBOE shall have full access to all Data at no charge. This can, if specified within this Agreement, be carried out by providing an application programming interface or other such efficient electronic tools. The Contractor shall not take any action to erase and/or withhold any SBOE Data, except as directed by SBOE.

1.10.3 Expiration or Termination of Services

Upon expiration or termination of this Agreement, the Contractor shall not take any action to erase and/orwithhold any Data, except as directed by the SBOE.

1.11 Secure Data Disposal

When requested by SBOE, the Contractor shall destroy Data in all of its forms, including all back-ups. Data shall be permanently deleted and shall not be recoverable, according to NYS Information Technology Standard S13-003 Sanitization Secure Disposal Standard, https://its.ny.gov/document/sanitization-secure-disposal-standard, or successor and S14-003 Information Security Controls, https://its.ny.gov/document/information-security-controls, or successor. Certificates of destruction, in a form acceptable to SBOE, shall be provided by the Contractor to SBOE.

1.12 Access to Security Logs and Reports

Upon request, the Contractor shall provide access to security logs and reports to SBOE in a format as specified in this Agreement.

1.13 Contractor Performance Audit

The Contractor shall allow SBOE to assess Contractor's performance by providing any materials requested in this Agreement (e.g., page load times, response times, uptime, and fail over time). The SBOE may perform this Contractor performance audit with a third party at its discretion, at SBOE's expense.

1.14 Compliance with Federal, State and Local Regulations

If required in this Agreement, Contractor will provide verification of compliance with specific Federal, State and local regulations, laws and IT standards that the Authorized User is required to comply with.

1.15 Authentication Tokens

This Agreement may require authentication tokens for all systems. For more details, please see NYS Information Policy Standard S14-006 Authentication Tokens Standard, https://its.ny.gov/document/authentication-tokens-standard, or successor.

1.16 Modification to Cloud Service Deployment Model, Service Model, and/or Initial Functionality Within this Agreement

As Cloud services can be flexible and dynamic, delivery mechanisms may be subject to change. This may result in changes to the deployment model, service model, functionality, or SKU. The State and SBOE require notification of any such changes to ensure security and business needs are met.

Any changes to the deployment model, service model, functionality, or SKU (e.g., PaaS to IaaS) must be provided to SBOE via the Contract Modification procedure.

In addition, notification must be provided to SBOE for review and acceptance, prior to implementation. Any changes to this Agreement will require SBOE to re-assess the risk mitigation methodologies and strategies and revise this Agreement as needed.

1.17 Application Programming Interface (API) or Self-Service Electronic Portal

Except as otherwise provided for in this document, Contractor may offer an API or self-service electronic portal for such purposes as allowing SBOE to access security logs, reports, and audit information, to import or export Data, and for such other purposes as agreed to in this Agreement.