APPENDIX N-1

SECURITY AND CONFIDENTIALITY TERMS

TABLE OF CONTENTS

The Security and Confidentiality Terms set forth in this Appendix N-1 are made part of the Agreement between the Contractor and each Contracting State Agency (CSA).

Note: The terms and conditions applicable to security, privacy, confidentiality and compliance are found in the body of the RFP along with this Appendix N, N-1 and in State specific Appendices. The more stringent and comprehensive standards set forth among such documents must be met by the Contractor. Any notifications or communications thereunder are to be made by the Contractor to the CSA who is impacted.

DEFINITIONS

For purposes of this Appendix N-1 the following terms shall have the following meanings:

"**Protected Information**" means data or information to which the Contractor is given access which the CSA creates, receives, or maintains, which is, pursuant to federal and/or state laws, rules, regulations, policies or agreements, deemed confidential, personal, private and/or sensitive. Such data or information may be present or stored in any form or medium and includes, but is not limited to:

a. Data or information obtained from sources outside of the NCS;
b. Data or information maintained in and/or obtained from NCS-owned applications, systems, networks and/or databases;
c. Data or information identifying an individual, particularly where such disclosure could result in an unwarranted invasion of personal privacy;
d. Computer codes or other electronic or non-electronic data or information, the disclosure of which could jeopardize the compliance stature, security or confidentiality of the CSA's information technology solutions, applications, systems, networks or data;
e. Any other material designated by the CSA as being "Confidential," "Personal," "Private," or otherwise "Sensitive."

"**Authorized Persons**" means the Contractor's employees, subcontractors or other agents who are authorized and have a business justification to access Protected Information to enable Contractor to perform the services pursuant to the Agreement.

"**Information Security Incident**" means any allegation or suspicion held by or brought to the attention of the CSA employee or Authorized Persons involving inappropriate or unauthorized access to, or disclosure of, Protected Information.

"**Information Security Breach**" means the unauthorized access by a non-Authorized Person of Protected Information as defined by the laws, rules, and regulations of the CSA, such as the New York State Information and Security Breach Notification Act (General Business Law Section 899-aa; State Technology Law Section 208.

"**CSA Contact**" means the person or persons designated in writing by the CSA to receive Information Security Incident or Information Security Breach notifications.

"**Continental United States (CONUS)**" – the 48 contiguous States and the District of Columbia

"**Follow-the-Sun**" – Follow-the-sun is a type of global workflow in which tasks are passed around daily between work sites that are many time zones apart. 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 be allowed to access Data directly, or indirectly, from outside CONUS.

DATA TO BE DISCLOSED

While a listing of specific data elements and/or information required to effectuate the Agreement may be more specifically set out in the solicitation, the obligations set out apply not only to such data elements and/or information but to all Protected Information, as defined herein.

PURPOSE OF DATA

Contractor represents that it is requesting and/or providing Protected Information solely for purposes specified in this solicitation. Each CSA will release Protected Information to Contractor exclusively for this purpose. Contractor shall use the Protected Information only for the authorized purposes specified in this Agreement.

OWNERSHIP OF DATA

Contractor agrees that each CSA shall be deemed the "owner" of Protected Information disclosed by the CSA to Contractor under this Agreement including for purposes of complying with the requirements of the laws, rules, and regulations of the CSA, such as the NYS General Business Law Section 899-aa.

DATA EXCHANGE DETAILS

Prior to the CSA's sharing of any data pursuant to this Agreement, Contractor and the CSA shall work together to provide and establish a secure, encrypted (both at rest and in transit) method of data exchange for any transfer of such data which shall, at a minimum, comport with the standards set by Federal Information Processing Standards Publication (FIPS) and National Institute of Standards and Technology (NIST) publications with reference to Security Categorization of Moderate as detailed in FIPS-199, FIPS -200, NITS SP 800-171B, NITS 800-53 R4, as all may be amended, and where required by any additional heightened compliance obligations applicable to and necessitated by the data involved in any such exchange. Each CSA's Chief Information Security Office (CISO), as the CSA deems appropriate, be provided with details of such proposed method of exchange for review and approval. The Parties agree that they will work together to create and keep current a Technical Service Description, to be made part of this Agreement, which sets forth the details of the Protected Information which the CSA shall furnish to Contractor, including, at a minimum, the frequency of the disclosure, timing, technical details of the method of data exchange (including all relevant details), and the format of any response as between the Parties.

DATA PROTECTION

Safeguarding of Protected Information shall be an integral part of the business requirements and activities of the Contractor to ensure there is no inappropriate or unauthorized use or exposure of Protected Information at any time. Contractor shall safeguard the confidentiality, integrity, and availability of Protected Information and comply with the following conditions:

a. Implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure, or theft of Protected Information. Such security measures shall comply with industry best practices and shall, at a minimum, comply with those requirements set forth by Federal Information Processing Standards Publication (FIPS) and National Institute of Standards and Technology (NIST) publications with reference to Security Categorization of Moderate as detailed in FIPS-199, FIPS -200, NITS SP 800-171B, NITS 800-53 R4, as all may be amended, and must comply with all applicable state and federal law, rules, regulations, and policies.
b. All Protected Information shall be encrypted at rest and in transit, in accord with, at a minimum, the standard set forth by Federal Information Processing Standards Publication (FIPS) and National Institute of Standards and Technology (NIST) publications with reference to Security Categorization of Moderate as detailed in FIPS-199, FIPS -200, NITS SP 800-171B, NITS 800-53 R4, as all may be amended, all applicable state and federal law, rules, regulations, and policies and, as appropriate, industry best practices.
c. At no time shall any Protected Information be copied, disclosed or retained by the Contractor for any purpose other than performing the services under this Agreement.

d. Contractor and Authorized Persons shall not disseminate, use, or permit the dissemination or use of Protected Information in any manner not described in this Agreement without express prior written consent from the CSA.
e. Host all Protected Information and maintain and implement procedures to logically segregate and secure Protected Information from Contractor's data and data belonging to the Contractor's other customers, including other governmental entities.
f. All data center(s) used to perform the services under the resulting contract must, at a minimum, meet or exceed tier 3 standards for redundancy and resilience, which can be found at the Uptime Institute website.
g. The Contractor must carefully, thoroughly, and thoughtfully vet all software solutions and hardware used to verify that they are compliant with the requirements set forth each CSA and fulfill the compliance obligations for the protection of the CSA's Protected Information. This vetting process shall also extend to all software solutions and hardware used by Authorized Persons.

DATA SECURITY

The Contractor shall meet, at a minimum the NIST Cybersecurity Framework v 1.1, (NIST CSF 1.1), as it may be amended, with particular attention to Data Security (PR.DS). The Contractor shall immediately disclose its non-proprietary security processes and technical limitations to the CSA such that adequate protection for Protected Information is attained. At a minimum Contractor represents and warrants that the security requirements and processes shall comport with the NIST CSF 1.1 and all security standards and protocols set by NITS SP 800-171B, NITS 800-53 R4, with reference to Security Categorization of Moderate as detailed in FIPS-199, as all may be amended, . In addition, the Contractor shall also comply with any state and/or federal laws, rules, regulations and/or policies that are applicable to the data being exchanged under this Agreement, including any heightened compliance obligations. The system and procedure that the Contractor will maintain for handling, storage, use, and destruction of Protected Information governed by this agreement will be sufficient to allow the CSA and/or its designee(s) to audit compliance with this Agreement.

DATA LOCATION

Contractor shall provide its services to the CSA and the CSA's end users solely from data centers physically located within the continental United States (CONUS), meaning the 48 contiguous States and the District of Columbia. Storage of Protected Information at rest shall be located solely in data centers in the United States. The Contractor shall not store, access, maintain, or process Protected Information on a mobile or portable device. The Contractor will store and maintain Protected Information in a place and manner that is physically secure from unauthorized access (e.g., locked cabinets or storage room) and will store and process electronic Protected Information in such a way that it will be secure from unauthorized access by any means.

CONTRACT AND DATA CENTER AUDIT

The Contractor shall allow the CSA and any other authorized government agency to audit the Contractor's compliance with the security procedures set forth in this section. Contractor shall perform an independent audit of its data centers which contain Protected Information at least annually, and provide the CSA states a copy of such audit report. Any non-critical deficiencies identified in the audit report or where the Contractor is found to be noncompliant with Agreement safeguards must be remedied, within 90 days of the issue date of the audit report with proof of remediation provided to the CSA. Critical deficiencies must be immediately remedied within a timeframe that the CSA approves. The completion of these requirements is at the Contractor's expense with no additional cost to the CSA.

The contractor will maintain a formal policy and procedures for the handling, storage, use, and destruction of Protected Information governed by this Agreement following NIST SP 800-88 Rev. 1, as same may be amended, with reference to Security Categorization of Moderate for which must be sufficient to allow the CSA and/or its designee(s) to audit compliance with this Agreement.

The contractor will permit the CSA, or its agent, to enter upon Contractor's premises at reasonable times to inspect and review their safeguards and procedures for protecting the confidentiality, privacy, security, and compliance of the Protected Information. The Contractor will also cooperate with the CSA, or its agent, in

connection with any request for access to staff, information, or material related to the CSA confidentiality, privacy, security, or compliance review, audit, or monitoring visit.

The contractor will provide, at Contractor's expense, an independent third-party audit of all data center(s) used to perform the services under the resulting Contract showing no deficiencies. Thereafter on an annual basis, at the contractor's expense, a full version of the audit report will be provided to the State, within 30 days of the anniversary date of the Agreement. A Service Organization Control (SOC) 2 Type 2 audit report or approved equivalent sets the minimum level of a third-party audit.

ACCESS

The contractor will limit access to Protected Information to Authorized Persons who have a legitimate business justification for access to such data for the purposes described in this Agreement.

For Protected Information with heightened compliance requirements, including but not limited to Unemployment Insurance Benefit information, Federal Parent Locator Services information, Federal Tax information, and Social Security Association information, Contractor will provide a listing of such Authorized Persons to each CSA at intervals determined by the CSAs. The contractor will ensure that this list is kept current with any additions, changes, or removal of Authorized Persons needing access.

Access to Protected Information by Authorized Persons shall be closely monitored by Contractor and shall be removed in the event such access is no longer justified by a legitimate business need or where the person separates from service. Such removal must be immediate but in no event later than the close of business on the date of the triggering event.

Notice of all such changes will be sent to the individual(s) identified in each CSA's state appendix.

The contractor may not assign or subcontract the Agreement, its obligation or interest hereunder, without the express, written consent of the CSA. Any assignment or subcontract made without such consent will be null and void and will constitute grounds for immediate termination of the Agreement by the CSA.

Contractor expressly represents and agrees that it will not re-disclose Protected Information provided by the CSA under this Agreement to third parties, including contractors or subcontractors, without the prior, written approval from the CSA. Authorized Persons shall not disseminate, use, or permit the dissemination or use of Protected Information in any manner not provided for in this Agreement without the express prior, written consent from the CSA.

The Contractor will undertake precautions to limit access to disclosed Protected Information to Authorized Persons only. The Contractor will adopt safeguards and procedures to limit dissemination only to Authorized Persons with a legitimate business need/purpose related to the purpose of this project as set out in this Agreement.

TRAINING

The Contractor will ensure that all Authorized Persons who have access to any Protected Information for authorized purposes set forth in this Agreement have been instructed in a manner approved by the CSA regarding the confidential nature of the Protected Information, the safeguards required to protect such data, and the sanctions in applicable state, federal, and local laws, rules, regulations and/or policies for unauthorized disclosure of Protected Information. The Contractor will annually sign an acknowledgment that all Authorized Persons with access to Protected Information have been instructed in a manner approved by and as set out above. The Contractor will provide this acknowledgment upon request to the CSA and prior to the disclosure of any Protected Information hereunder and annually, as required, to continue the disclosure of Protected Information hereunder.

CONFIDENTIALITY AGREEMENTS

Contractor shall require Authorized Persons to sign a confidentiality and non-disclosure agreement provided by the CSA in relation to access to Protected Information. Such signed agreements must be obtained prior to Authorized Persons commencing work. Contractor shall maintain such agreements for the duration of the audit period as set out in this Agreement and for the duration of any state, federal, and local laws, rules, regulations and policies applicable to the Protected Information being exchanged under this Agreement, whichever is longer, and shall provide them to the CSA upon request.

BACKGROUND INVESTIGATION AND FINGERPRINTING

Contractor shall have a written personnel security policy that ensures a background investigation is completed for any individual who will need access to perform his/her job duties to Protected Information with heightened compliance obligations. The policy will identify the process, steps, and timeframes for determining whether an employee may be granted access to such Protected Information. The results of the background check will be reviewed by the Contractor to determine whether the applicant is suitable for access to such Protected Information. Suitability is defined as having verified citizenship or residency and no prior criminal offense or offenses where the nature of the offense creates a risk of misuse of such Protected Information as defined within this Agreement. Written background investigation policies and procedures must be provided to the CSA for review and approval. Policies and procedures, as well as a sample of completed background investigations, must be available for inspection upon request by the CSA or its agents.

NOTIFICATION OF LEGAL REQUESTS

The Contractor shall immediately inform the CSA in writing upon receipt of any legal, investigatory, or other mode or method of demand (including, but not limited to, FOIL or FOIA requests, electronic discovery, litigation holds, and discovery searches) for access to Protected Information that is not otherwise authorized under this Agreement and shall take and vigorously pursue all necessary legal action to prevent any disclosure including, but not limited to, moving to quash subpoenas issued for such information. The Contractor will keep the CSA's General Counsel or other designated personal fully and timely notified of all developments related to such legal actions and their response thereto, and provide appropriate, robust legal assistance as may be required, as requested by the CSA. The notification shall be directed to that individual identified in each CSA's state appendix.

REPORT OR PUBLICATION

Contractor will ensure that any study, report, publication, or other disclosure for which Protected Information shared by each CSA is the basis and which is permitted under this Agreement is limited to the reporting of aggregate, de-identified data, which means it will not contain any information that might lead to the identification of a private person or entity. Each CSA shall have the right to review and approve any such study, report, publication, or other disclosure prior to disclosure or publication.

RETURN/DESTRUCTION OF PROTECTED INFORMATION

In the event of termination or expiration of the Agreement, Contractor shall immediately implement an orderly return of all Protected Information, whether in digital or any other form, in a mutually agreeable format at a time agreed to by the parties and/or at the direction of each CSA. Thereafter, the Contractor shall, unless otherwise advised in writing by the CSA, immediately destroy and/or sanitize, as appropriate to the medium, such data and any extracts, copies, or backups of same thoroughly and irretrievably. The method for the sanitization of data shall, at a minimum, comport with the standards set by NIST SP 800-88 Rev. 1, as same may be amended, with reference to Security Categorization of Moderate. Contractor shall thereafter certify in writing and provide proof that these actions have been completed within 30 days of termination or expiration of this Agreement or within seven days of the request of an agent, employee or officer of the CSA, at the discretion of the CSA. The Contractor will not make, retain, copy, duplicate, or otherwise use any copies of Protected Information after completion of the purpose for which the data disclosed is served without prior written permission from the CSA.

DATA RETENTION

Notwithstanding any other obligation under this Agreement, Contractor agrees that it will preserve the Protected Information in a manner that complies with all applicable federal, state and local laws, rules, regulations, and policies for the purposes of ensuring applicable data records retention obligations are met.

COMPLIANCE WITH INFORMATION SECURITY BREACH NOTIFICATION ACT AND OTHER LAWS

Contractor represents and warrants that its collection, access, use, storage, disposal and disclosure of Protected Information does and will comply with all applicable federal, state and local privacy, confidentiality, security, data protection and compliance laws, rules, regulations, policies, and directives. Contractor warrants that it will comply with each CSA's Breach Notification laws. The contractor ensures that it and all Authorized Persons will be in compliance with the aforementioned state, federal, and local laws, rules, regulations, policies, and directives.

VULNERABILITY SCANNING

The Contractor must perform appropriate and required environment vulnerability scanning in accordance with Industry best practices and standards. The Contractor must address all high and medium vulnerabilities found during scanning in a reasonable timeframe as agreed upon with each CSA.

The CSAs will have the option to perform application scanning and webserver scanning, as needed. The Contractor must address all high and medium vulnerabilities found during scanning in a reasonable timeframe as agreed upon with each CSA.

When software vulnerabilities are revealed and addressed by a vendor patch, the Contractor will obtain the patch from the applicable vendor and categorize the urgency of application as either "critical" or "non-critical" in nature. The determination of the critical versus non-critical nature of patches is solely at the reasonable discretion of all affected CSAs in consultation with the Contractor. The Contractor will apply all critical security patches, hotfixes, or service packs as they are tested and determined safe for installation after consultation with all affected CSA.

INFORMATION SECURITY INCIDENT AND INFORMATION SECURITY BREACH

If the Contractor or any Authorized Person becomes aware of or has knowledge of either any potential Information Security Incident (Security Incident) or Information Security Breach (Security Breach), then the Contractor shall within 30 minutes of becoming aware or having knowledge of any potential Security Incident or Security Breach, notify the Point of Contact (CSA POC) for each affected CSA listed below of the Security Incident or Security Breach via the email address noted, and each CSA will direct what further action is necessary for response to the same. At such time, Contractor shall provide all affected CSA POCs with the name and contact information for an employee of Contractor who shall serve as Contractor's primary security contact and shall be available to assist all affected CSA POCs 24 hours a day, seven days per week, in keeping all affected CSAs fully and timely notified of all developments relating to any such potential or actual Security Incident or Security Breach utilizing the following contact information:

For the Commonwealth of Massachusetts
To be provided at time of contract negotiations.

For the State of Connecticut
To be provided at time of contract negotiations.

For the State of Maine
To be provided at time of contract negotiations.

For the State of New Hampshire
To be provided at time of contract negotiations.

For the State of New York
OTDA General Counsel
40 North Pearl Street 16 C
Albany, NY 12243
(518) 474-9502
otda.sm.iso@otda.ny.gov

For the State of Rhode Island
To be provided at time of contract negotiations.

For the State of Vermont
To be provided at time of contract negotiations.

Should an Information Security Incident or Security Breach occur, immediately following the requisite notification to all affected CSAs, Contractor shall 1) promptly investigate and utilize best efforts and IT industry best practices to determine the cause(s) of same and devise a proposed resolution and report the cause(s) and suggested remedies to all affected CSAs; (2) promptly implement necessary remedial measures as for all affected CSAs deems necessary; (3) document responsive actions taken, including any post-incident review of events and actions taken to make changes in business practices to prevent similar instances in the future; 4) provide reports within the timeframes as requested by any affected CSA; 5) promptly notify all affected CSAs of the steps taken to prevent similar instances in the future; and 6) take any other action as may be directed by all affected CSAs.

Notification and Assistance to Affected Persons

Contractor shall be responsible for:

a. Promptly notifying individuals whose Protected Information was compromised by an Information Security Breach ("Affected Persons") or, as the affected CSA deems appropriate, an Information Security Incident. The Contractor is to first seek consultation and receive authorization from the affected CSA prior to issuing such notifications. The affected CSA shall approve the content of and the method by which such notifications must be provided (e.g., regular mail, e-mail, and/or website posting);
b. If requested by the affected CSA and/or required by law, provide credit monitoring services, identity theft consultation and restoration, identity theft insurance, public records monitoring, toll free number and call center, payday loan monitoring, and any other services deemed reasonably necessary by the affected CSA to Affected Persons for a minimum of one year or longer, as determined by the affected CSA, (together referred to as "Affected Persons Assistance");
c. Costs. The Contractor shall bear all costs associated with providing Affected Persons Assistance. Each affected CSA may reduce any Contractor invoice by an amount attributable to the Contractor's failure to satisfactorily provide Affected Persons Assistance.

BUSINESS CONTINUITY AND DISASTER RECOVERY

The Disaster Recovery system shall be accessible by all users 24 hours a day, seven days a week, 365 days a year and available 99.982% of the time (uptime) per month and must not be rendered inoperable for any longer period for the purposes of maintenance, upgrades or hardware additions. Each CSA will work with the Contractor to provide a listing of all essential functions related to the Agreement that must be sustained and maintained for the duration of the agreement. The Contractor shall have no less than one redundant data centers separated by at least 100 miles and on separate network fiber and separate power grids.

Contractor shall failover application to alternate hardware to perform planned maintenance, patches, code revisions, etc. to one instance, thoroughly test, then switch back to the upgraded instance before repeating the planned maintenance, patch, code revision, etc. on the second instance.

The Contractor will provide each CSA with a business continuity and disaster recovery plan. This plan will include detailed precautions to minimize the effects of any disaster or interruption of service so that each CSA

can rapidly continue to operate and resume mission-critical functions. Each CSA will work with the Contractor to provide an analysis of business processes and continuity needs. The Contractor will provide technical support staff with the skills required to interface with all applications, networks, hardware, and software during planning and preparation for disaster recovery and business continuity testing and/or during any declaration of an actual disaster. Minimum recovery time objective (RTO) and recovery point objective (RPO) will be determined by each CSA and should these vary, the most stringent/comprehensive periods shall be applicable to all.

SUSPENSION/TERMINATION

Each CSA agrees to provide Protected Information pursuant to this Agreement subject to the representations and agreements by the Contractor contained in this document. Each CSA will suspend the Agreement and the further disclosure of any Protected Information hereunder if: (i) Contractor fails to comply with any provision of this Agreement or (ii) the CSA's General Counsel believes in good faith that the Contractor has violated its obligations to maintain the confidentiality, privacy, security and/or compliance status of such data or limit properly limit dissemination of such data. Such suspension will continue until corrective action, approved by the suspending CSA, has been taken. In the absence of prompt and satisfactory corrective action, the CSA may, at its sole discretion, terminate the Agreement. Upon termination, the Contractor must immediately return all Protected Information obtained by the Contractor or Authorized Persons under the Agreement pursuant to the terms and conditions of the Return/Destruction of Protected Information section within this Agreement.

GENERAL TERMS

In addition to suspension or termination of the Agreement as provided herein, Each CSA reserves the right to undertake, without limitation, any other action under the Agreement, or state or federal law, rule, or regulation, to enforce the Agreement and secure satisfactory corrective action and/or return and/or destruction of the Protected Information furnished hereunder, including seeking damages, penalties, and restitution from Contractor or its affiliates as permitted under law.

The Contractor's and Authorized Person's confidentiality and related assurances and obligations hereunder shall survive the termination or expiration of the Agreement.

CLOUD COMPUTING PROVISIONS

All privacy, confidentiality, security and compliance requirements set out in this Agreement shall apply to any cloud computing solution proposed for use by the Contractor to accomplish any obligation under this Agreement.