1. Contractor acknowledges that all records and other information maintained by the Illinois Student Assistance Commission (“ISAC”) regarding the agency, any institution or person are confidential (“Confidential Data”) and shall be protected from unauthorized use and/or disclosure under this Agreement.

2. Contractor acknowledges that the data it receives from and on behalf of ISAC is confidential and Contractor agrees to comply with all State and Federal requirements with respect to the protection of privacy, security and dissemination of the data including, but not limited to, the following laws:

**The Personal Information Protection Act** (“PIPA”) (815 ILCS 530). PIPA requires state agencies, their contractors, and other data collectors to notify affected individuals after a breach of the security of the data collector’s data system occurs. PIPA specifies how and when individuals must be contacted. PIPA requires contractors implement and maintain reasonable security measures to protect personal information data records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

**The Data Processing Confidentiality Act** (30 ILCS 585).

Section 1. Whenever any State agency governed by confidentiality requirements as to information in its possession gives, contracts out, or otherwise transmits such information in a form suitable for electronic data processing to any contractor, electronic data processing center, or other user outside such agency, for any purpose whatsoever, such agency shall notify the receiver of such data in writing of the agency's confidentiality requirements, including any penalties provided for their violation.

Section 2. It shall thereupon become the duty of the individual or entity who receives such data for electronic processing or storage to keep or use the same pursuant to the confidentiality requirements of the transmitting agency, and any receiver who violates them shall be subject to the same penalty as any officer or employee of such agency would incur for their violation.

**Identity Protection Act** (5 ILCS 179/10, as amended) **COLLECTION AND USE OF SOCIAL SECURITY NUMBERS**

1. Contractor or its employees, agents or assigns are prohibited from engaging in the following activities:
	1. Publicly posting, displaying, communicating, or otherwise making available an individual’s SSN to the general public;
	2. Printing an individual’s SSN on any card required for the individual to access products or services provided by ISAC, another agency, or a private party, including but not limited to Contractor;
	3. Requiring or requesting that an individual transmit a SSN over the internet;
	4. Printing an individual’s SSN on any materials mailed through any public or private mail or courier service unless state or federal law requires SSNs to be included on the document (e.g., on a student’s Free Application for Federal Student Aid (FAFSA)).
2. Contractor shall not collect, use or disclose an individual’s SSN unless it is required to do so by state or federal law or the collection, use, or disclosure is otherwise necessary for ISAC or Contractor to carry out its duties and responsibilities;
3. Only those Contractor employees who are required to use or handle information or documents that contain SSNs shall have access to such information or documents;
4. Any SSN that is requested from individuals should be placed and retained in a manner that makes the information easy to redact if it is required to be released as part of a public records request;
5. Any of Contractor employees who collect a SSN from any individual must explain the purpose for which the information will be used.
6. Prior to receiving Social Security Numbers from ISAC, Contractor shall provide ISAC with its privacy policy that ensures that social security numbers are protected as described herein.

**Family Educational Rights and Privacy Act of 1974, as amended**, (20 U.S.C. 1232g), enacted as section 438 of the General Education Provisions Act. (“FERPA”) ISAC has a duty to maintain confidentiality of student information received from schools.

In furtherance of the above laws and acknowledgements, Contractor agrees to the following:

Use of Data limited to Purpose of Agreement

Contractor shall not disseminate, use or reuse Confidential Data for other than the primary purpose of this Agreement without the express written authority of ISAC.

Publishing Summary Information Only

If Confidential Data received pursuant to this Agreement is distributed or published, such information shall not contain personal identifiers but shall be in summary form.

Disposal/Return of Information:

Confidential Data received pursuant to this Agreement shall be disposed of after the purpose of the Agreement is served. Disposal means the return of the information to ISAC or destruction of the information, as directed by ISAC. The data disclosed shall not be archived or sent to a records center and shall not be retained with personal identifiers for any period longer than the term of the Agreement, (unless, by agreement of the parties, the data is to be retained for a specific period that exceeds the term of the Agreement).

Certification of Communication of Confidentiality Requirements to Personnel:

The undersigned certifies that all personnel having access to Confidential Data under this Agreement have been instructed regarding the confidentiality requirements and sanctions specified for unauthorized disclosure and agrees to fully and promptly report any infraction of the confidentiality provisions to ISAC.

Right of Immediate Cancellation

Notwithstanding any provision to the contrary, this Agreement is subject to immediate cancellation by ISAC for failure of Contractor or its authorized contractor or agent to adhere to any provision set forth in this Confidentiality Agreement. Contractor agrees to indemnify and hold ISAC harmless for Contractor’s breach of these confidentiality provisions.

Securing Data/Right to Inspection:

 Contractor shall secure any and all Confidential Data received pursuant to this Agreement in accordance with standard audit requirements (such as SSAE16, SOC), and retain records of access and use of such Confidential Data received for a period of three (3) years following the expiration or termination of this Agreement.

 **Safeguarding requirements and procedures.**

The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Personally Identifiable Information (PII) before disposal or release for reuse.

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(xvi) ISAC data with personally Identifiable Information (PII) should be encrypted at rest and while in transit.

 Any backup of ISAC’s data should be encrypted.

(xvii) ISAC’s data should not be forwarded to personal emails such as Yahoo or Gmail or stored in cloud services.

(xiii) ISAC’s data should not be accessed using personal devices and public kiosks.

(xix) Apply security patches to the systems in a timely manner.

(xx) Enable whole disk encryption for mobile devices like laptops.

(xxi) External device restrictions and access control should be enabled so that data cannot be leaked by copying to USBs or CDs.

(xxii) Any third-party access to ISAC’s data should be restricted and should strictly be based on what is allowed in this data sharing agreement.

(xxiii) It is recommended that staff with access to ISAC’s data attend periodic Security Awareness Training so that they are aware of various security risks and the steps that can be taken to minimize the risk.

**Without limiting the foregoing, Contractor agrees that:**

1. It is prohibited from disclosing or using any Confidential Data disclosed to it by ISAC by users of the services for which this Agreement relates, except solely to carry out the purposes for which it was disclosed in the ordinary course of business to carry out those purposes; and it has implemented and will maintain an information security program to protect and secure Confidential Data.
2. Contractor shall also be compliant with the best practices established by the National Institute for Standards in Technology (NIST) and Contractor shall periodically participate in a security assessment as requested by ISAC and shall take ISAC recommended corrective action to improve Contractor’s security practices as necessary.

During the term outlined in the Contract between the Illinois Student Assistance Commission (“ISAC”) and Contractor (“the Contract”) and for a period of three (3) years after the termination or expiration of the Contract, its representatives and agents will be entitled to conduct audits of Contractor’s relevant operations, facilities, systems, etc. to confirm that Contractor has complied with the Information Security Program Requirements (the “Security Audits”). Any Security Audit shall be scheduled in advance with Contractor and shall be scheduled and conducted during normal business hours and shall not unreasonably interfere with Contractor’s business activities. In the event that any Security Audit results in the discovery of material security risks to ISAC’s customer information, Contractor shall respond to ISAC in writing with Contractor’s plan to take reasonable measures to promptly take any corrective actions to effectively eliminate the risk, at no cost to ISAC. Contractor shall have five (5) business days to cure such security risk, unless the parties agree to a longer period of time for such cure. In the event of a security risk, ISAC may review any system and transaction logs related thereto which pertain to ISAC’s information or data potentially compromised. ISAC’s right, and the right of its representatives and agents, to conduct Security Audits, and any exercise of such right, shall not in any way diminish or affect Contractor’s duties and liabilities under this agreement.

Contractor shall report to ISAC all known or suspected Security Incidents. “Security Incident” means any unauthorized action by a known or unknown person which, if successfully completed, should reasonably be considered one of the following: an attack, penetration, denial of service, disclosure of confidential customer or other sensitive information, misuse of system access, unauthorized access or intrusion (hacking), virus intrusion, scan of Contractor’s systems or networks, or any other activity that could affect Contractor’s systems or data, or the security, confidentiality or integrity of the ISAC customer information received, stored, processed, or maintained by Contractor. “Security Incident” shall also include any contact by a law enforcement agency with Contractor regarding any ISAC customer information. For purposes hereof, “Contractor” shall include any of Contractor’s employees, agents, contractors or third parties (including, without limitation, any vendors used by Contractor for the provision of services to be provided by Contractor to ISAC) that have access (either authorized or unauthorized) to ISAC customer information. If a Security Incident occurs, Contractor shall immediately notify ISAC at: Telephone number 847-831-8330.

With a follow-up written notification sent immediately via overnight mail to ISAC at the following address:

The Illinois Student Assistance Commission

Attention: Information Security Officer

1755 Lake Cook Road, Deerfield, Illinois 60015

Email: Senoy.Kavalackal@illinois.gov

The package shall also provide the following information: nature and impact of the Security Incident; actions already taken by Contractor; Contractor’s assessment of immediate risk; and corrective measures to be taken, evaluation of alternatives, and next steps. Contractor shall continue providing (i) appropriate status reports to ISAC regarding the resolution of the Security Incident and prevention of future such Security Incidents, and (ii) cooperation, as reasonably requested by ISAC, in order to further investigate and resolve the Security Incident. ISAC may require that the services provided by Contractor to ISAC be suspended, connectivity with Contractor be terminated, or other appropriate action be taken pending such resolution.

**INDEMNIFICATION AND LIABILITY:** Contractor shall indemnify and hold harmless ISAC and the State of Illinois, its agencies, officers, employees, agents and volunteers from any and all costs, demands, expenses, losses, claims, damages, liabilities, settlements and judgments, including in-house and contracted attorneys’ fees and expenses, arising out of: (a) any breach or violation by Contractor of this Agreement (b) any loss or disclosure of ISAC’s Confidential Information and damages or loss claimed to result in whole or in part from Contractor’s negligent performance; or (c) any act, activity or omission of Contractor or any of its employees, representatives, subcontractors or agents arising as a result of the Contractor’s negligence, willful default or fraud.

**WHEREAS, THE UNDERSIGNED AFFIRMS, UNDER PENALTY OF PERJURY, THAT HE OR SHE IS AUTHORIZED TO, AND DOES HEREBY AGREE ON BEHALF OF THE DESIGNATED ORGANIZATION, TO COMPLY WITH THIS DATA CONFIDENTIALITY AND SECURITY AGREEMENT.**

Printed Name of Organization: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name and Title Date: