**Teacher Retirement System of Texas**

**Information Security Terms and Conditions**

These Information Security Terms and Conditions ("InfoSec Terms") are incorporated for all purposes into the contract (“Contract”) between the Teacher Retirement System of Texas ("TRS") and Contractor. To the extent that any provision contained in these InfoSec Terms conflicts with any provision contained elsewhere in the Contract, it is expressly understood and agreed that the provision contained in these InfoSec Terms shall control to the extent necessary to resolve the conflict. If Contractor and TRS have entered into a Business Associate Agreement (“BAA”), the terms of the BAA shall control to the extent necessary to resolve the conflict.

The term “TRS Data” refers to all TRS information, as well as other entity information in the possession of TRS, that is processed, stored, or transmitted by a computer, including data that is generated by Contractor in the performance of services under the Contract.

1. **Data Confidentiality.** Section 16 (TRS Data and Confidentiality) of the TRS General Terms and Conditions shall apply to these InfoSec Terms.
2. **Auditable Information Security Framework.** Contractor agrees to maintain security controls that, at a minimum, conform to an industry-accepted, auditable information security framework, including for example, NIST SP 800-53 or ISO 27001.
3. **Information System Security.** Contractor agrees, at all times, to maintain commercially reasonable information security protection(s) that, at a minimum, include identity and access management, network firewalls, intrusion detection/prevention, and periodic vulnerability and penetration testing conducted by a qualified independent third-party. Contractor further agrees to maintain secure environments by employing vulnerability scanning tools and techniques to identify information systems flaws, improper configurations, and vulnerabilities. Contractor shall remediate and mitigate vulnerabilities in a timely manner.
4. **Data Security.** Contractor agrees to protect and maintain the security of TRS Data and agrees to conform to the following measures to protect and secure data:

4.1. **Data in Transit.** Contractor agrees that any and all transmission or exchange of system application data with TRS shall take place using secure, authenticated, and industry-accepted encryption mechanisms, such as (1) SFTP (FTP over SSH), (2) FTPS (FTP over TLS), (3) HTTPS (HTTP over TLS), and (4) virtual private network.

4.2. **Data Custodianship.** Contractor agrees that all TRS Data in Contractor’s custody will be stored, processed, and maintained solely on Contractor information systems as designated in the Contract. TRS Data in the custody of the Contractor shall not be stored on or transferred to any end-user computing device or any portable storage medium by Contractor or its agents, unless that storage medium is in use as part of the Contractor’s designated backup and recovery processes (e.g., backup tapes or drives). All servers, storage, backups, and network paths utilized in the delivery of the service shall be contained within the states, districts, and territories of the United States unless specifically agreed to in writing by an authorized agent of TRS. An appropriate officer with the necessary authority can be identified by TRS’ Chief Information Security Officer for any general or specific case.

Contractor shall ensure that TRS Data (i.e., primary and backup) remains, at all times, within the continental United States. Contractor shall receive, process, transmit, and store all TRS Data within the continental United States. TRS’s point of access to TRS Data shall be within the continental United States.

4.3. **Data at Rest.** Contractor agrees to encrypt all TRS Data at rest, including its backup and recovery data, in encrypted form, using industry-accepted encryption algorithms commensurate with the classification of the information being protected (e.g., AES 128-bit or higher).

1. **Data Breach.** Contractor agrees to comply with all applicable state and federal laws that require the notification of individuals in the event of unauthorized access to or release of personally identifiable information or other event requiring notification. If an event occurs in which the security of any TRS Data results in the accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction, Contractor shall immediately notify TRS both orally by telephone and in writing, via encrypted email to breachnotifications@trs.texas.gov, but no later than 12 hours after Contractor’s discovery or reasonable belief of an event. Contractor shall reimburse TRS for reasonable out-of-pocket expenses directly resulting from such security incident. In the event a security incident involves a person’s sensitive personal information, Contractor shall comply with the notice requirements under Section 521.053 of the Texas Business and Commerce Code and provide identity theft protection services for one (1) year for each affected person.
2. **End of Agreement Data Handling.** Contractor agrees within 30 days of termination of Contract or receipt of a written request submitted by an authorized agent of TRS, that it must:
	1. Securely return all data, including backup and recovery data, in a timely manner, for no additional compensation, following the termination of the services, to TRS in an agreed file format usable without the outsourced information system or cloud service;
	2. Sanitize (clear, purge, or destroy in a manner consistent with NIST Special Publication 800-88) all TRS Data in its entirety in a manner that prevents its physical reconstruction through the use of commonly available file-restoration utilities; and
	3. Submit to TRS Attachment A (Data Destruction/Return Certification Regarding TRS Data) certifying in writing that these actions have been completed and provide to TRS a record of destruction.

**Attachment A**

**TEACHER RETIREMENT SYSTEM OF TEXAS**

**DATA DESTRUCTION/RETURN CERTIFICATION REGARDING TRS DATA**

**Contract Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

 **Contract Number:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

 **Contract Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

I \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (name/ title) of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (organization), pursuant to Sections 6.1 and 6.2 of the TRS Information Security Terms and Conditions entered into as part of the contract for services identified above, certify the following:

The term “TRS Data” refers to all TRS information, as well as other entity information in the possession of TRS, that is processed, stored, or transmitted by a computer, including data that is generated by Contractor in the performance of services under the Contract.

* The following TRS Data related to the above identified contract has been destroyed in the following manner on the following date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* The following TRS Data related to the above identified contract has been returned to TRS in the following manner and on the following date. : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Return or destruction of the following TRS Data related to the above identified contract is infeasible for the following reasons: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Such information which for which return, or destruction is infeasible will be protected under the terms of the TRS Information Security Terms and Conditions for as long as our organization retains it. The organization estimates that such information will be either returned or destroyed by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Our organization further certifies that we do not possess any Protected Health Information from TRS, whether in hard copy or electronic form, beyond the information that is the subject of this attestation.

Executed on this \_\_\_\_\_\_\_\_\_ day of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 20\_\_\_\_.

By:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(signature)

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

(name)

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(title)