TEXAS STATE UNIVERSITY SYSTEM
INFORMATION SECURITY & ACCESSIBILITY STANDARDS EXHIBIT

To the extent there is a conflict between a term or condition contained in this IT Exhibit and the associated purchase order or executed Agreement (the **Agreement**) between the parties, the terms and conditions contained in this IT Exhibit shall take precedence and its terms and conditions shall govern and control the parties' contractual relationship.

Applicability:

THIS EXHIBIT IS APPLICABLE IF CONTRACTOR IS PROVIDING INFORMATION RESOURCES TO THE REQUESTING INSTITUTION FOR THE REQUESTING INSTITUTION'S USE.

Definitions:

Requesting Institution: The Texas State University System (**System**) Administration or any of the System's seven (7) Component Institutions that elects to enter into an Agreement with Contractor to utilize Contractor's Services.

Information Resources: The term "Information Resources" has the meaning set forth in TAC 202.1. In addition, Information Resources may include the following examples:

1. all physical and logical components of the Requesting Institution's wired and wireless network infrastructure;
2. any device that connects to or communicates electronically via the Requesting Institution's network infrastructure, including computers, printers, and communication devices, both portable and fixed;
3. any fixed or portable storage device or media, regardless of ownership, that contains the Requesting Institution's data;
4. all data created, collected, recorded, processed, stored, retrieved, displayed, or transmitted using devices connected to the Requesting Institution's network;
5. all computer software and services licensed by the Requesting Institution;
6. support staff and services employed or contracted by the Requesting Institution to deploy, administer, or operate the above-described resources or to assist the Requesting Institution community in effectively using these resources;
7. devices, software, or services that support the operations of the Requesting Institution, regardless of physical location (e.g., SAAS, PAAS, IAAS, cloud services); and
8. telephones, audio and video conferencing systems, phone lines, and communication systems provided by the Requesting Institution.

Confidential Information: Data that have been designated as private or confidential by law or by the Requesting Institution. Confidential Information includes, but is not limited to, employment records, medical records, student records, education records, personal financial records (or other personally identifiable information), audit logs, research data, trade secrets, and classified government information. Confidential Information shall not include public records that by law must be made available to the general public. To the extent there is doubt

as to whether any data constitute Confidential Information, the data in question shall be treated as Confidential Information until a determination is made by the Requesting Institution or proper legal authority.

Authorized Agent of Requesting Institution: An officer of the Requesting Institution with designated data, security, or signature authority.

1. Mandatory Compliance

Contractor agrees to comply with all applicable state and federal laws and regulations. Contractor agrees to provide credible evidence, to the sole satisfaction of the Requesting Institution, of the below compliance requirements (i) prior to entering into this Agreement with Requesting Institution, and (ii) the earlier of three (3) years during the term of any agreement entered into or before the contract renewal period, if applicable, thereafter. Contractor understands and acknowledges that Contractor's failure to provide credible evidence satisfactory to the Requesting Institution regarding the same prior to entering into any agreement shall result in no contract being awarded to Contractor. Contractor further understands and acknowledges that Contractor's failure to provide credible evidence satisfactory to the Requesting Institution regarding the same during the term of an already executed agreement shall constitute a breach of the agreement by Contractor and the Requesting Institution may automatically terminate the agreement and pursue whatever remedies available to the Requesting Institution under contract, at law, or in equity.

1.1 **Texas Risk and Authorization Management Program (TX-RAMP).** Pursuant to Sections 2054.0593(d)-(f) of the Texas Government Code relating to cloud computing, state risk and authorization management program, if Contractor's service is a cloud computing service as defined by Texas Government Code Section 2054.0593 (a), Contractor represents and warrants that Contractor's cloud computing service complies with the requirements of the state risk and authorization management program, and Contractor agrees that throughout the term of the Agreement, Contractor shall maintain its certifications and continue to comply with the program requirements.

1.2 **Accessibility.** TAC Section 213 requires the Requesting Institution to verify that Electronic and Information Resource (**EIR**) purchases are compliant with Federal 508 Refresh, TAC 206 and TAC 213 laws. Contractor is required to provide a valid Accessibility Conformance Report (**ACR**) for review.

1.3 **Other Applicable Laws and Regulations.** Applicable laws and regulations may include, but are not limited to, the following:

A. The Family Educational Rights and Privacy Act (**FERPA**)
B. The Health Insurance Portability and Accountability Act (**HIPAA)**
C. The Gramm-Leach-Bliley Act (**GLBA**)
D. Payment Card Industry Data Security Standards (**PCI DSS**)

1.4 **Confidential Information in Internet Websites and Mobile Applications.** Pursuant to Texas Government Code Section 2054.516, if Contractor's service includes an

Internet website or a mobile application that processes confidential information for the Requesting Institution, then prior to processing Requesting Institution data, Contractor agrees to provide the Requesting Institution with:

A. The results or attestation of a vulnerability and penetration test by an independent third party. For clarity, similar testing performed internally by Contractor personnel is not a sufficient substitute for work performed by a qualified, independent third party.

B. Information regarding the following:
   (1) A description of the logical architecture of the websites and/or applications;
   (2) Descriptions of the flow of data between logical components of the websites and/or applications; and
   (3) Technical description of all authentication mechanisms for the websites and/or applications.

1.5 **Security Controls for State Agency Data**. In accordance with Section 2054.138 of the Texas Government Code, Contractor certifies that it will comply with the security controls required under Section 2 of this Exhibit and will maintain records and make them available to Requesting Institution as evidence of Contractor's compliance with the required controls.

2. Security Controls

2.1 **Cybersecurity Framework.** Contractor agrees to maintain security controls that, at a minimum, conform to an industry-accepted cybersecurity framework, including for example, NIST SP 800-53, NIST SP 800-171, ISO 27001, or the CIS Critical Security Controls.

2.2 **Information System Security.** Contractor agrees, at all times, to maintain commercially reasonable information security protection(s) that, at a minimum, include network firewalls, intrusion detection/prevention, and periodic vulnerability and penetration testing conducted by a qualified third party. Contractor further agrees to maintain secure environments that are patched and up to date with all appropriate and/or necessary information security updates.

2.3 **Data Confidentiality.** Contractor shall implement appropriate measures designed to ensure the confidentiality and security of Confidential Information, protect against any anticipated hazards or threats to the integrity or security of such information, protect against unauthorized access or disclosure of information, and prevent any other action that could result in substantial harm to Requesting Institution or an individual identified within the data or information in Contractor's custody.

2.4 **Data Ownership.** Requesting Institution owns all data processed, stored and/or transmitted by Contractor in accordance with the Agreement. Such data must only be used for the purpose of the Agreement.

A. **Data Description**. A description of all Requesting Institution data to which the Contractor has access must be specified in the Agreement, and notifications of any changes must be made in writing by the Contractor within 30 days of the change.

B. **End of Agreement Data Handling**. Contractor agrees within 30 days of termination of the Agreement or receipt of a written request submitted by an Authorized Agent of Requesting Institution, that it must:

(1) return all data, including backup and recovery data, to the Requesting Institution in a useable electronic form;
(2) erase, destroy, and render unreadable all Requesting Institution data in its entirety in a manner that prevents its physical reconstruction through the use of commonly available file-restoration utilities; and
(3) certify in writing that these actions have been completed.

2.5 **Data Security.** Contractor agrees to protect and maintain the security of Requesting Institution's data and agrees to conform to the following measures to protect and secure data:

A. **Data Transmission.** Contractor agrees that any and all transmission or exchange of system application data with the Requesting Institution and/or any other parties shall take place using secure, authenticated, and industry-accepted strong encryption mechanisms.

B. **Data Custodianship.** Contractor agrees that any and all of the Requesting Institution's data in Contractor's custody will be stored, processed, and maintained solely on Contractor information systems as designated in the Agreement. Requesting Institution's 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 Requesting Institution. An appropriate officer with the necessary authority can be identified by the Requesting Institution's Information Security Officer for any general or specific case.

C. **Data at Rest.** Contractor agrees to store all of the Requesting Institution's data, including its backup and recovery data, in encrypted form, using sufficiently strong, industry accepted encryption algorithms commensurate with the classification of the information being protected (e.g., AES 128-bit).

D. **Key Management.** Encryption keys must be stored using industry-accepted methods that include storage on information systems separate from the data they decrypt.

E. **Data Re-use.** Contractor agrees that any and all data exchanged shall be used expressly and solely for the purposes enumerated in the Agreement. Data shall not be distributed, repurposed, or shared across other applications, environments, or business units of Contractor. As required by federal law, Contractor further agrees that none of the Requesting Institution's data (of any kind) shall be revealed, transmitted, exchanged or otherwise passed to other vendors or interested parties except on a case-by-case basis as specifically agreed to in writing by an Authorized Agent of Requesting Institution.

2.6 **Safekeeping and Security.** As part of the Contractor's service, Contractor will be responsible for safekeeping all keys, access codes, combinations, access cards, personal identification numbers and similar security codes, identifiers, passwords, or other authenticators issued to Contractor's employees, agents, contractors, or subcontractors. Contractor agrees to require its employees to report a lost or stolen device or information within 24 hours of such device or information being lost or stolen.

2.7 **Audit Logs.** The Contractor's service shall record audit logs (e.g., application-specific user activities, exceptions, information security events such as successful and rejected events, use of privileges, log-on failed-attempts & successes, log-off, data accessed, data attempted to be accessed, administrative configuration changes, and the use of advanced privileges). All logs pertaining to Requesting Institution's usage of Contractor's service shall be available to Requesting Institution at all times or it shall be promptly made available, without unreasonable delay, to an Authorized Agent of Requesting Institution upon request. These audit logs shall contain sufficient data including but not limited to:

A. User or process identifiers (e.g., the actor or group if applicable);
B. Timestamps including time zone;
C. Source and destination addresses (e.g., IP addresses); and
D. Action or Event descriptions which may include filenames, success or failure indications, and access control or flow control rules invoked.

2.8 **Test / Development Environments.**

A. Requesting Institution data contained within Contractor's test or development environments must be treated as would data in production environments and are subject to the same requirements for safeguards described within this Exhibit.

B. Contractor will make available to the Requesting Institution a development instance separate from the production instance. This environment shall be made available prior to the Requesting Institution's use of the production

instance and this environment shall continue to be made available as long as the Requesting Institution is using Contractor's Service.

C. **Accessibility Testing**. Contractor agrees to provide a link to a demonstration of the EIR that can be tested using automated testing tools and assistive technology.

2.9 **Account Credentials.**

A. Any user accounts provisioned inside the Contractor's service for use by Requesting Institution must be unique and individually assigned.

B. Where applicable, federated authentication services (e.g., SAML, ADFS, or CAS) shall be used.

C. The password management for any non-federated accounts intended for use by the Requesting Institution must comply with institution password policies unless the Contractor formally requests in writing an exception which must first be approved by the Requesting Institution's Information Security Officer.

2.10 **Maintaining Updated Contacts.** The Contractor shall provide Requesting Institution the appropriate contact(s) necessary for Requesting Institution to maintain the requirements set forth in this Exhibit as well as the Agreement. Any updates to the contact information shall be provided in writing to Requesting Institution within ten (10) business days.

3. Data Breach

Contractor agrees to comply with all applicable state and federal laws that require the notification of individuals in the event of unauthorized release of personally identifiable information or other event requiring notification. In the event of a breach of any of Contractor's security obligations or other event requiring notification under applicable law ("Notification Event"), Contractor agrees to:

3.1 Notify the appropriate Requesting Institution's breach notification address (listed below) and any Authorized Agents of Requesting Institution without unreasonable delay and no later than 48 hours after breach discovery.

(1) Texas State University System Administration: breachnotifications@txstate.edu
(2) Texas State University: breachnotifications@txstate.edu
(3) Sam Houston State University: breachnotifications@shsu.edu
(4) Lamar University: breachnotifications@lamar.edu
(5) Sul Ross State University: breachnotifications@sulross.edu
(6) Lamar State College Port Arthur: breachnotifications@lamarpa.edu
(7) Lamar State College Orange: breachnotifications@lsco.edu
(8) Lamar Institute of Technology: breachnotifications@lit.edu

3.2 Include the following information in the notification:

(1) a description of the impacted products or services;
(2) a full description of all breached data fields;
(3) the number of breached records;
(4) date of breach (suspected or known);
(5) date of breach discovery by Contractor;
(6) method of breach (e.g., accidental disclosure, malicious intrusion);
(7) information security program point of contact including name, email and phone details;
(8) and remediation status (complete, in process - with detail).

3.3 Assume responsibility for informing all such individuals in accordance with applicable law.

4. Mandatory Disclosure of Confidential Information

If Contractor becomes compelled by law or regulation (including securities' laws) to disclose any Confidential Information, the Contractor must provide Requesting Institution written notice without unreasonable delay so that Requesting Institution may seek an appropriate protective order or other remedy. If a remedy acceptable to Requesting Institution is not obtained by the date that the Contractor must comply with the request, the Contractor will furnish only that portion of the Confidential Information that it is legally required to furnish, and the Contractor shall require any recipient of the Confidential Information to exercise commercially reasonable efforts to keep the Confidential Information confidential.

5. Remedies for Disclosure of Confidential Information

Contractor and Requesting Institution acknowledge that unauthorized disclosure or use of the Confidential Information may irreparably damage Requesting Institution in such a way that adequate compensation could not be obtained from damages in an action at law. Accordingly, the actual or threatened unauthorized disclosure or use of any Confidential Information shall give Requesting Institution the right to seek injunctive relief restraining such unauthorized disclosure or use, in addition to any other remedy otherwise available (including reasonable attorneys' fees). Contractor further grants Requesting Institution the right, but not the obligation, to enforce these provisions in Contractor's name against any Contractor's employees, officers, board members, owners, representatives, agents, contractors, and subcontractors violating the above provisions.

6. Non-Disclosure

Contractor is permitted to disclose Confidential Information to its employees, authorized contractors and subcontractors, agents, consultants, and auditors on a need-to-know basis only, provided that all such contractors, subcontractors, agents, consultants and auditors have written confidentiality obligation to Contractor.

7. Survival

The confidentiality obligations shall survive termination of any agreement with Contractor and for a period of ten (10) years or for so long as the information remains confidential, whichever is longer and will inure to the benefit of Requesting Institution.