TEXAS STATE UNIVERITY SYSTEM
INFORMATION SECURITY 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 SYSTEM FOR THE SYSTEM'S USE.

Information Resources – as described in UPPS No. 04.01.01, Security of Texas State Information Resources, the term information resources has the meaning ascribed in TAC 202.1. In addition to the term's ascribed definition, information resources may include the following examples:

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

Definitions:

Confidential Information: Data that have been designated as private or confidential by law or by The System. 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 any uncertainty 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 System or proper legal authority.

Authorized Agent of Institution: A Component Institution officer with designated data, security, or signature authority.

1. 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 The System or an individual identified within the data or information in Contractor's custody.

2. Compliance with Laws and Component Institution Policies and Procedures

Contractor shall provide written confirmation within thirty (30) days of contract execution that it has conducted criminal history and credit history background checks on its officers, employees, or other persons it causes to access or handle Component Institution information resources or data. Contractor also agrees to comply with all applicable state and federal laws, regulations, all Component Institution Security and Privacy Policies, the Family Educational Rights and Privacy Act (**FERPA**), Health Insurance Portability and Accountability Act (**HIPAA**), and the Gramm-Leach-Bliley Act (**GLBA**). Contractor shall obtain and maintain all necessary permits, licenses, and certificates required to provide the Services outlined in this Agreement.

3. Information System Security

Contractor agrees, at all times, to maintain commercially reasonable network security that, at a minimum, includes network firewall provisioning, intrusion detection/prevention, and periodic penetration testing conducted by a qualified third party. Likewise, Contractor agrees to maintain network security that, at minimum, conforms to one of the following:

3.1 Current standards set forth and maintained by the National Institute of Standards and Technology, as found at https://nvd.nist.gov/ncp/repository ; or

3.2 Any generally recognized, comparable standard that Contractor then applies to its own network (e.g., ISO 27002) and which has been approved in writing by The System.

3.3 **Confidential Information in Internet Websites and Mobile applications.** If Contractor's service processes confidential information, prior to an Internet website or mobile application being deployed:

A. Results or attestation of a vulnerability and penetration test by an independent third party will be provided by the Contractor to The System; and

B. The following information must be provided to The System:
   (1) Architecture of the website or application
   (2) Authentication mechanism for the website or application
   (3) Administrator level access to data included in the website or application

4. Data Ownership

The System owns all data processed, stored or transmitted by the Contractor's service in accordance with this Agreement. Such data must only be used for the purpose of this Agreement.

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

4.2 A mutually agreed upon data recovery or exit plan must be established at least ninety (90) days prior to the date of future termination of product use (i.e., retrieving stored data from Contractor at the end of this Agreement).

5. Data Security

Contractor agrees to protect and maintain the security of data with measures that include maintaining secure environments that are patched and up-to-date with all appropriate security updates as designated by a relevant authority (e.g., Microsoft notifications). Likewise, Contractor agrees to conform to the following measures to protect and secure data:

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

5.2 Data Custodianship. Contractor agrees that any and all of The System's data in the Contractor's custody will be stored, processed, and maintained solely on Contractor information systems as designated in this Agreement. No such data in the Contractor's custody, at any time, will 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 Services shall be contained within the states, districts, and territories of the United States unless specifically agreed to in writing by a Component Institution officer with designated data, security, or signature authority. An appropriate officer with the necessary authority can be identified by The System's Information Security Officer for any general or specific case.

5.3 Data at Rest. Contractor agrees to store all Component Institution 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).

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

5.5 Data Re-use. Contractor agrees that any and all data exchanged shall be used expressly and solely for the purposes enumerated in the underlying 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 no Institution 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 a Component Institution officer with designated data, security, or signature authority.

6. Compliance

Contractor agrees to provide credible evidence, to the satisfaction of The System, of the following compliance requirements and accepts that failure to do so will prevent The System from purchasing the Services from Contractor.

6.1 **Security Assessment.** Any Security Assessment questionnaires provided by The System will be answered completely and promptly with all supporting documents submitted to The System.

6.2 **Accessibility.** Texas Administrative Code (TAC) 213 requires The System to verify that Electronic and Information Resource (EIR) purchases are compliant with Federal 508 Refresh, TAC 206 and TAC 213 laws. The Contractor is required to provide a valid VPAT and a link to a demo of the EIR that can be tested using automated testing tools and assistive technology.

7. End of Agreement Data Handling

Contractor agrees within thirty (30) days of termination of this Agreement or receipt of a written request submitted by an authorized agent of The System, it must:

A. return all data, including backup and recovery data, to The System in a useable electronic form;

B. erase, destroy, and render unreadable all Component Institution data in its entirety in a manner that prevents its physical reconstruction through the use of commonly available file-restoration utilities; and

C. certify in writing that these actions have been completed.

8. Data Breach

Contractor agrees to comply with all applicable State of Texas 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:

A. notify the information security officer (breachnotifications@txstate.edu) and any authorized agents of The System without unreasonable delay and no later than 48 hours after breach discovery;

B. notifications shall include a full description of all breached data fields and the number of breached records; and

C. assume responsibility for informing all such individuals in accordance with applicable law.

9. 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 The System written notice without unreasonable delay so that The System may seek an appropriate protective order or other remedy. If a remedy acceptable to The System 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.

10. Remedies for Disclosure of Confidential Information

Contractor and The System acknowledge that unauthorized disclosure or use of the Confidential Information may irreparably damage The System 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 The System 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 The System 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.

11. 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 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.

12. 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.

13. Survival

The confidentiality obligations shall survive termination of any agreement with Contractor 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 The System.

14. 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 The System's usage of Contractor's service shall be available to The System at all times or it shall be promptly made available, without unreasonable delay, to an authorized agent of The System 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.

15. Account Credentials

Any user accounts provisioned inside the Contractor's service for use by The System must be unique and individually assigned. Where applicable, federated authentication services (e.g., SAML, ADFS, or CAS) shall be used. The password management for any non-federated accounts intended for use by The System must comply with The System's password policies unless the Contractor formally requests in writing an exception which must first be approved by The System Information Security Officer.

16. Maintaining Updated Contacts

The Contractor shall provide The System the appropriate contact(s) necessary for The System to maintain the requirements set forth in this Exhibit as well as this Agreement. Any updates to the contact information shall be provided in writing to The System within ten (10) business

days.

17. Test / Development Environments

The Contractor will make available to The System a development instance separate from the production instance. This environment shall be made available prior to The System's use of the production instance and this environment shall continue to be made available as long as The System is using the Contractor's service. Component Institution data contained within Contractor 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 Agreement.