

TTU IT ADDENDUM

1. Destruction of Data.

1. In the event of expiration or termination of the Contract and at TTU's discretion, all TTU data will be:
 - a. returned to TTU (and any copies remaining with Bidder will be destroyed and confirmation of the destruction shall be provided to TTU); **OR**
 - b. destroyed and confirmation of the destruction shall be provided to TTU.
2. If such information cannot be returned or destroyed due to statutory requirements, Bidder will continue to protect any TTU data retained after expiration or termination of the Contract, in compliance with NIST Special Publications 800-53, **OR** another comparable cybersecurity standard.
3. TTU data includes all TTU information, TTU databases, TTU confidential information, any backup copies, and copies stored on external/third-party hosted storage.

2. Uptime. In consideration of TTU's payment of the fees under this Contract, Bidder will use commercially reasonable efforts to make its solution available, at least, 99.99% of the time, except for scheduled maintenance (performed outside normal business hours to the extent possible) and unscheduled maintenance required for repairs and events beyond Bidder's reasonable control.

3. Accessibility. Accessibility is a Federal and State of Texas requirement for all electronic and information resources ("EIR(s)") procured by institutions of higher education. Bidder represents and warrants that all EIRs and all associated information, documentation, and support will meet the currently required accessibility standards at a federal and state level (e.g., WCAG 2.1, Level AA, [1 TAC § 206](#), and [1 TAC § 213](#)) ("Standard(s)"), and Bidder shall provide accessibility documentation attesting to any EIR accessible features and capabilities (e.g., for websites and mobile apps.) Bidder shall provide additional documentation as requested by TTU, including but not limited to documentation described in 1 TAC § 213. If Bidder becomes aware that EIRs, including any portion(s) thereof, do not comply with the Standard(s), Bidder represents and warrants that it will, at no cost to TTU, either (1) perform all necessary remediation(s) to make the EIRs satisfy the Standards, or (2) replace the EIRs with new EIRs which satisfy the EIR Standards and do not alter the material purpose of the Contract. In the event Bidder fails or is unable to do so, TTU may terminate this Contract without further duty or obligation hereunder. TTU reserves the right to perform testing on the Bidder's deliverables to ensure the accuracy of their accessibility documentation regarding conformance with the Standards.

4. System Access. Any access to TTU's computer systems must be approved and coordinated through the TTU Chief Information Security Officer. No automated tools may be installed by Bidder without prior written authorization from the TTU Office of the Chief Information Officer ("CIO").

5. Information Security.

- a) Bidder shall abide by and implement the controls specified in NIST Special Publications 800-53 **OR** another generally recognized comparable cybersecurity standard. Examples of controls include, but are not limited to: (1) firewalls, (2) vulnerability scanning, (3) endpoint protection software, (4) regular backups including off-site transfer to facilitate disaster recovery, (5) up-to-date installation of all current patches, (6) encrypting all communications containing personally identifiable or other sensitive or confidential information, and, if required by TTU, (7) encryption in the Bidder's database of all passwords and personally identifiable or other sensitive or confidential information.
- b) Bidder personnel shall regularly monitor server security logs and firewall event logs for potential breaches of security. Bidder will regularly audit the security measures on all servers and network equipment and take appropriate measures to maintain the integrity and security of those systems.
- c) **IF** any systems and/or applications are connected to the TTU network, they will be scanned for vulnerabilities on a weekly basis, per TTU IT's Vulnerability Management Program. Bidder agrees to timely vulnerability assessment and mitigation and to be subject to other applicable TTU IT policies.
- d) In accordance with [Texas Government Code §2054.516](#), deliverables such as a website or mobile app that process sensitive information or personally identifiable information ("PII") or confidential information must have had a recent vulnerability scan and penetration test conducted (i.e., within the last two years.)
- e) Data transfers must be done via an agreed-upon secure method of transmission approved by the TTU Chief Information Security Officer or their designee.

6. **Username and Password Security.** IF the product requires integration with any TTU enterprise system (i.e., SSO), the Bidder must coordinate with the TTU Office of the CIO. When authenticating TTU users, Bidder may be required to integrate with TTU's authentication system using a method approved by TTU. Under certain mutually agreed upon circumstances, Bidder may issue and manage usernames and passwords for TTU users. The passwords must use suitable hashing algorithms with salts applied and be at least as strong as the current standard used by TTU.
7. **Breach of Security.** Bidder and TTU share responsibility for being alert for breaches of security. Bidder shall notify TTU immediately of each instance of an actual or suspected (i) unauthorized access to or use of TTU data or (ii) unauthorized disclosure, misuse, alteration, destruction, or other compromise of TTU data. Bidder shall cooperate with any reasonable request of TTU in enforcing its rights. Both parties shall cooperate in the investigation of such breach, sharing all evidence and findings.
8. **eCommerce.** For eCommerce purchases, a PCI SSC validated P2PE solution must be used unless an exception is granted by the TTU Office of the CIO.
9. **Cybersecurity Training.**
 - a) In accordance with [Texas Government Code §2054.5192](#), any Bidder with access to a state computer system or database (i.e., any person who has been given an account to access any state (or local) information system) must complete an annual cybersecurity training program provided by TTU.
 - b) For the purposes of this section, "Bidder" includes subBidders, affiliates, officers, or employees of the Bidder.
10. **Compliance with Texas Government Code §2054.0593 (TX-RAMP).** Pursuant to [Texas Government Code §2054.0593](#), relating to the Texas Department of Information Resource's State Risk and Authorization Management Program ("Program"), Bidder represents and warrants that it complies with the requirements of the Program and Bidder agrees that throughout the term of the Contract it shall maintain the required certifications and comply with the Program requirements in the performance of the Contract. If the Bidder fails to maintain the requirements of the Program, TTU has the right to terminate the Contract immediately without any further cause.
11. **Use Of Artificial Intelligence ("AI").** Bidder hereby represents and warrants that:
 - a) Artificial Intelligence ("AI") includes machine learning, natural language processing ("NLP"), robotic process automation ("RPA"), computer vision, robotics, expert systems, or any other forms of AI.
 - b) Bidder will promptly provide TTU written disclosure of any current or contemplated use of AI throughout the course of the Contract with the parties.
 - c) Bidder will cooperate with TTU to ensure the provision, use, and storage of TTU data complies with all laws and regulations, including those pertaining to data privacy and security.
 - d) Bidder will not use TTU data and any AI output resulting from TTU data for any other purpose than to fulfill Bidder's obligations under this Contract.
 - e) While any information obtained from and related to TTU, including any derivative data, is in the possession or control of Bidder, Bidder will implement and maintain physical, administrative, and technical safeguards to protect the information from inadvertent or unauthorized access, disclosure, use, or modification, taking into the account the sensitivity and confidentiality of such information. Bidder further warrants and represents that it has and will continue to comply with all applicable data protection laws and regulations with respect to the AI system and any data that is collected or processed.
 - f) Bidder maintains, and shall continue to maintain security safeguards and controls in compliance with NIST Special Publications 800-53, or another comparable cybersecurity standard, including proper access controls for the AI.
 - g) To the best of Bidder's knowledge, there has been no unauthorized use of or access to AI and no AI has been used in violation of any applicable laws and regulations.
 - h) Bidder's current or contemplated use of the AI does not, and will not, infringe upon or violate any intellectual property rights, rights of likeness or publicity, or any other third-party right of any kind.
 - i) Bidder maintains and shall continue to maintain commercially reasonable insurance coverage for claims or losses pertaining to the AI.

- j) Bidder warrants that the AI has not been subject to any claims, suits, demands, rulings, judgements, threats, fines, penalties, or a cease-and-desist letter asserted against, or brought by, Bidder pertaining to intellectual property or any other rights violation or breach of any applicable law, rule, or regulation.