Texas Tech University System
Required IT Terms

When incorporated by reference into an agreement between the Texas Tech University System ("TTUS"), a Texas public system of higher education, and/or any one or more of its component institutions, each Texas public institutions of higher education, the following terms ("IT Terms") form a material and binding part of the agreement between the parties (the "Contract"). As used herein, "University" means the TTUS party or parties to the agreement, and "Contractor" means the non-TTUS party or parties to the agreement, whether or not the relationship of Contractor is that of an independent contractor.

1. **Accessibility**. Contractor will comply with all federal and state accessibility requirements, including without limitation Section 508 of the Rehabilitation Act of 1973 and technical standards contained in 1 Texas Administrative Code §§ 206 and 213. Contractor shall complete, maintain, or provide Voluntary Product Accessibility Templates ("VPATs") attesting to any electronic and information resources' ("EIR") accessible features and capabilities, or provide a similarly formatted document attesting to the EIRs' accessible features and capabilities. University reserves the right to perform testing on Contractor's deliverables to ensure accuracy of their VPAT response regarding conformance with federal or state standards.

2. **Uptime**. Contractor 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), unscheduled maintenance required for repairs, and events beyond Contractor's reasonable control.

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

4. **Vulnerability Management**. If any systems or applications are connected to the University network, they may be scanned for vulnerabilities on a weekly basis per University's vulnerability management program. Contractor consents to timely vulnerability assessment and mitigation and shall be subject to other University IT policies.

5. **Information Security**. Contractor shall abide by and implement the controls specified in NIST Special Publications 800-53 Appendix F safeguards, including but not limited to: (1) firewalls, (2) vulnerability scanning, (3) anti-virus scanning 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 information and, if required by University, (7) encryption in the Contractor's database of all passwords and personally identifiable information such as Social Security Numbers and Driver's License numbers.

6. **Monitoring**. Contractor personnel shall regularly monitor server security logs and firewall event logs for potential breaches of security. Contractor will audit the security measures on all servers and the network equipment no less than monthly and take appropriate measures to maintain the integrity and security of those systems.

7. **Username and Password Security**. If the product(s) provided by Contractor, at University's discretion, require integration with any University enterprise system (i.e., SSO), the Contractor shall coordinate with the University CIO in implementing such integration. When authenticating University users, Contractor may be required to integrate with University's authentication system using a method approved by University. Under certain mutually agreed-upon circumstances, Contractor may issue and manage usernames and passwords for University users. Passwords must use suitable hashing algorithms with salts applied and be at least as strong as the standard used by University.

8. **Breach Notification**. Contractor and University share responsibility for being alert for breaches of security. Contractor shall notify University immediately of each instance of an actual or suspected (i) unauthorized access to or use of University data that could result in substantial harm or inconvenience to University or (ii) unauthorized disclosure, misuse, alteration, destruction, or other compromise of University information. Contractor shall cooperate with reasonable requests by University in enforcing its rights. Both parties shall cooperate in the investigation of such breach, sharing all evidence and findings.

9. **eCommerce**. For eCommerce purchases, if a PCI SSC validated P2PE solution is available, it must be used unless an exception is granted by the University CIO.

10. **Audit of Systems and Data**. With advance notice and coordination, University reserves the right to conduct a security assessment on any of Contractor's systems that stores any University information. If University's assessment finding is that the confidentiality, security, and integrity of University information is insecure, University will notify Contractor in writing of the deficiencies identified in the assessment and Contractor will utilize prevailing industry recognized security controls and best practices to correct such deficiencies within thirty (30) days or within a mutually agreed-upon timeframe following such written notice. Contractor's failure to correct the deficiencies within such timeframe is a material breach of this Contract. University will be responsible for all expenses associated with the aforementioned assessments.

End of IT Terms.