

**Appendix E to DIR Contract No. DIR-TSO-2718**  
**SERVICES AGREEMENT**

This Services Agreement (the “Agreement”) is entered into effective \_\_\_\_\_, 20\_\_\_\_ (the “Effective Date”) by and between [CUSTOMER], with its principal place of business at [ADDRESS], and Adjacent Technologies, a Delaware corporation (“Vendor”), with a principal place of business at 10415 Morado Circle, Building 1, Suite 120, Austin, Texas.

WHEREAS [CUSTOMER] and Vendor have engaged in extensive negotiations, discussions and due diligence that have culminated in the formation of the contractual relationship described in Appendix D, Statement of Work to DIR-TSO-2718 (SOW); and

WHEREAS, [CUSTOMER] desires to procure from Vendor, and Vendor desires to provide to [CUSTOMER] the Services described in this Agreement according to the terms and conditions specified herein.

NOW THEREFORE, in consideration of the mutual promises and covenants contained herein, and of other good and valid consideration, the receipt and sufficiency of which are hereby acknowledged, [CUSTOMER] and Vendor (collectively, the “Parties” and each, a “Party”) hereby agree as follows:

**1. INTRODUCTION AND GENERAL SCOPE**

[CUSTOMER] desires that certain Services be provided, performed and managed by Vendor as described in the SOW. Vendor has reviewed [CUSTOMER]’s requirements, has performed all due diligence it deems necessary, and desires to perform and manage such Services for [CUSTOMER]. Vendor will develop and implement certain solutions for the [CUSTOMER] delivered as Cloud Services in accordance with the mutually approved SOW and incorporated herein for all purposes. The Vendor will provide for, administer and manage third-party professional hosting of the solution, as more thoroughly described herein. Any ambiguity or inconsistency between or among the terms of the SOW and this Agreement shall be resolved by giving priority and precedence to this Agreement and then the Statement of Work. The parties may modify, amend, restate or add additional Statements of Work upon their mutual written agreement and the terms and conditions of this Agreement shall apply to any such amended, restated or additional Statements of Work. Order of Precedent shall be as stated in DIR Contract No. DIR-TSO-2718. In the event of a conflict, the DIR Contract controls.

**2. TERM**

**2.1. Initial Term.** The initial term of this Agreement is for [TERM] from the date of the Agreement. The term may be for a period of 12, 24 or 36 months.

**2.2. Extension.** The Parties may mutually agree to extend the terms of this Agreement.

**3. SERVICES.** The term “Services” as used herein shall include the following:

**3.1. Technical Services.**

(a) **Software Configuration.** Where applicable, vendor will perform software configurations as required by the Statement of Work.

(b) **System Administration.** Vendor will perform system administration services required in the Statement of Work, if applicable.

#### **4. SERVICE LEVELS**

**4.1. Support and Maintenance.** First-call software support and maintenance shall be provided by Vendor to [CUSTOMER] solely pursuant to terms and conditions of a separate Software Support and Maintenance Services Level Agreement between Vendor and [CUSTOMER] (the “Support Agreement”).

**4.2. System Performance.** The Support Agreement shall include response times for support issues. The [CUSTOMER] will be required in the Support Agreement to provide connectivity with sufficient capacity to not impact system response times.

#### **5. CUSTOMER RESPONSIBILITIES**

**5.1. Connectivity.** [CUSTOMER] agrees to coordinate and implement adequate and secure connectivity to the Vendor’s or any approved hosting provider’s data center at [CUSTOMER]’s expense.

**5.2. Security.** [CUSTOMER] agrees to provide and comply with security measures to protect unauthorized access to the hosted solutions. [CUSTOMER] will provide Vendor with required security measures and requirements in advance of solution deployment.

**5.3. User Administration.** [CUSTOMER] agrees to provide services required to administer the user access to any hosted solutions, including user identification and user passwords in accordance with defined security policies, leveraging the Vendor’s authentication methods.

**5.4. Problem Reporting.** [CUSTOMER] agrees to utilize the Vendor’s issue reporting and tracking software to notify Vendor of any and all software system or hosted solution problems.

**6. INVOICING AND PAYMENT.** Vendor shall invoice [CUSTOMER] for Technical Services under the Statement of Work. Payment shall be in accordance with Section 6C of Appendix A, DIR Contract No. DIR-TSO-2718.

#### **7. CONFIDENTIALITY AND SECURITY.**

**7.1. Survival of Provisions; Perpetual Survival and Severability.** [CUSTOMER] rights and privileges applicable to [CUSTOMER] Data, and Vendor obligations regarding Confidentiality, shall survive expiration or any termination of this contract, and shall be perpetual. Vendor obligations (other than its fiduciary duties under this Contract) regarding security shall survive this contract for a period of [SECURITY TERM] after contract termination, or as required by law or conclusion of legal proceedings or audit, whichever is later. As an exception to the foregoing perpetual survival, if certain [CUSTOMER] Data become publicly known and made generally available through no action or inaction of Vendor, then

Vendor may use such publicly known [CUSTOMER] Data to the same extent as any other member of the public. If any term or provision of this contract shall be found to be illegal or unenforceable, it shall be deemed independent and divisible, and notwithstanding such illegality or unenforceability, all other terms or provisions in this contract shall remain in full force and effect and such term or provision shall be deemed to be deleted.

## **7.2. Applicability**

(a) **Inclusion in all Subcontracts.** The requirements of these confidentiality and security provisions shall be included in, and apply to, all subcontracts and any agreements Vendor has with anyone performing Services on Vendor's behalf.

(b) **Third Parties.** This contract is between Vendor and the [CUSTOMER], and is not intended to create any independent cause of action by any third party, individual, or entity against [CUSTOMER] or Vendor.

## **7.3. Disclosure and Confidentiality of Data**

**Protecting Data.** Vendor and Vendor's Agents possess no special right to access, use or disclose [CUSTOMER] Data as a result of Vendor's contractual or fiduciary relationship with the [CUSTOMER]. Tex. Gov't Code Chapter 552 defines the exclusive mechanism for determining whether [CUSTOMER] Data are subject to public disclosure. Vendor stipulates, covenants, and agrees that it will not access, use or disclose [CUSTOMER] Data beyond its limited authorization, or for any purpose not necessary for the performance of its duties under this Agreement. As between the [CUSTOMER] and the Vendor, all [CUSTOMER] Data shall be considered the property of [CUSTOMER] and shall be deemed confidential. Vendor hereby irrevocably assigns, transfers, and conveys, and shall cause Vendor's Agents to irrevocably assign, transfer, and convey to [CUSTOMER] without further consideration all of its and their right title and interest to [CUSTOMER] Data. Upon request by [CUSTOMER], Vendor shall execute and deliver and shall cause Vendor's agents to execute and deliver to [CUSTOMER] any documents that may be necessary or desirable under any law to preserve or enable [CUSTOMER] to enforce its rights with respect to [CUSTOMER] Data.

In the event of any unauthorized disclosure or loss of [CUSTOMER] Data, Vendor shall immediately comply with the Notice subsections of this document. Vendor or Vendor's Agents may, however, disclose [CUSTOMER] Data to the extent required by law or by order of a court or governmental agency; provided that Vendor shall give [CUSTOMER], and shall cause Vendor's Agents to give [CUSTOMER], notice as soon as it or they are aware of the requirement; and use its or their best efforts to cooperate with [CUSTOMER] if [CUSTOMER] wishes to obtain a protective order or otherwise protect the confidentiality of such [CUSTOMER] Data. [CUSTOMER] reserves the right to obtain a protective order or otherwise protect the confidentiality of [CUSTOMER] Data.

Vendor shall comply with any policies, processes, procedures, regulations, rules, or any other [CUSTOMER] requirements that relate to the protection or disclosure of [CUSTOMER] Data or data relating to [CUSTOMER] customers, Vendor's operations, or the Vendor performance of the Agreement.

Vendor and Vendor's Agents shall access [CUSTOMER] systems or disseminate [CUSTOMER] Data only for the purposes for which they are authorized.

Vendor acknowledges and agrees to protect [CUSTOMER] Data.

Vendor shall engage in a continuous cycle of process improvement and vigilance to assess risks, monitor and test security protection, and implement change to protect [CUSTOMER] Data. Vendor agrees to perform such continuous process improvement and to upgrade its security protection during the term of this Agreement.

**Statutory and Regulatory Provisions.** Vendor agrees that it shall comply with all state and federal standards regarding the protection and confidentiality of [CUSTOMER] Data as currently effective, subsequently enacted or as may be amended. The existing requirements that are applicable to Vendor's obligations under this contract are included in this Agreement.

**Data Destruction.** Within [DESTRUCTION TERM] of the effectiveness of this Agreement, Vendor and [CUSTOMER] shall develop, and mutually agree upon, a detailed schedule for the retention and destruction of [CUSTOMER] Data. The schedule will be based upon the Services being performed and the Vendor's limited authorization to access, use, and disclose [CUSTOMER] Data. Subsequent to developing and agreeing upon that schedule, Vendor shall:

- (i) Retain and destroy [CUSTOMER] Data in accordance with the detailed schedule for the retention and destruction;
- (ii) Destroy or purge [CUSTOMER] Data so that they are unusable and irrecoverable; and
- (iii) Within [CONFIRMATION OF DESTRUCTION TERM] of destruction or purging, provide the [CUSTOMER] with a signed statement(s) containing the date of destruction or purging, description of [CUSTOMER] Data destroyed or purged, and the method(s) used.
- (iv) In the event of contract expiration or termination for any reason, Vendor and Vendor's Agents shall completely purge all [CUSTOMER] Data from the information systems of Vendor and Vendor's Agents and no [CUSTOMER] Data will be retained by the Vendor. All hard-copy [CUSTOMER] Data shall be destroyed. If immediate purging of all data storage components is not possible, the Vendor agrees that any [CUSTOMER] Data remaining in any storage component will be protected to prevent unauthorized disclosures.
- (v) Within [DATA DESCRIPTION TERM] of contract expiration or termination, Vendor shall provide [CUSTOMER] with a signed statement detailing the nature of the [CUSTOMER] Data retained, type of storage media, physical location(s), and any planned destruction date.
- (vi) In its discretion, the [CUSTOMER] may waive notification requirements or request reasonable changes to the detailed schedule for the retention and destruction of [CUSTOMER] Data.

**7.4. Requests to Vendor for Confidential or Public Information.** Vendor and Vendor's agents expressly do not have any actual or implied authority to determine whether any [CUSTOMER] Data are public or exempted from disclosure. Vendor is not authorized to respond to public information requests on behalf of the [CUSTOMER]. Vendor agrees to forward to the [CUSTOMER], by facsimile within one (1) [CUSTOMER] Business Day from receipt all request(s) for information associated with the Vendor's services under this contract. Vendor shall forward any information requests to:

[CUSTOMER INFORMATION OFFICER CONTACT INFORMATION]

**7.5. Security**

**General/Administrative Protections.** At all times Vendor shall be fully responsible to [CUSTOMER] for the security of the storage, processing, compilation, or transmission of all [CUSTOMER] Data to which it has access, and of all equipment, storage facilities, and transmission facilities on which or for which such [CUSTOMER] Data are stored, processed, compiled, or transmitted.

The [CUSTOMER] shall have the right to review the Vendor's internal protection systems and access protection lists for all areas of the work site(s). The [CUSTOMER] may, with or without cause, and without cost or liability, revoke or deny any or all authorizations. If any authorization is revoked or denied, then Vendor shall immediately use its best efforts to assist the [CUSTOMER] in preventing access, use or disclosure of [CUSTOMER] Data.

Vendor shall immediately notify the [CUSTOMER] Contract Manager when any person Vendor authorized to access the [CUSTOMER] systems is no longer authorized to have such access. This notice includes re-assigned or terminated individuals.

Vendor will use COBIT 5.0 as our Security Framework where applicable.

At its discretion, the [CUSTOMER] may perform initial and periodic detailed background reviews to include a criminal records check for any person authorized to access, or requesting to access, [CUSTOMER] Data. If requested by the [CUSTOMER], the Vendor shall provide any required consent and authorization to perform any background reviews.

The Vendor's physical access security and systems information access security systems must track all access attempts and failures. The access security systems must produce access logs on request. These logs must identify all access failures and breaches. Notwithstanding anything to the contrary in this Contract, the physical access and systems information access security systems access logs for any particular calendar year must be retained for a period of seven (7) calendar years after the last calendar day of the calendar year in which they were created. Thus a log created on January 1, 2007 may be disposed of, with all other systems access logs created in 2007, on January 1, 2015. All physical access and systems information access security systems access logs must be stored to electronic media. Any stored log must be produced for viewing access and copying upon request of the [CUSTOMER] within five (5) [CUSTOMER] Business Days of the request.

Vendor shall maintain appropriate audit trails to provide accountability for use and updates to [CUSTOMER] Data, changes, procedures, and performances. Audit trails maintained by Vendor will, at a minimum, identify the supporting documentation prepared by Vendor to permit an audit of the system by tracing the activities of individuals through the system. Vendor's automated systems must provide the means whereby authorized personnel have the ability to audit and to verify contractually required performances and to establish individual accountability for any action that can potentially cause access to, generation of, or modification of [CUSTOMER] Data. Vendor agrees that Vendor's failure to maintain adequate audit trails and corresponding documentation shall create a presumption that the services or performances were not performed.

[CUSTOMER] Data are not allowed on mobile/remote/portable storage devices; nor may storage media be removed from the facility used by Vendor. If [CUSTOMER] finds it necessary to allow data on mobile/remote/portable storage devices, or to allow storage media to be removed from a facility used by Vendor, [CUSTOMER] will specify, any encryption standard Vendor shall follow for mobile/remote/portable storage devices and the circumstance(s) under which storage media may be removed.

### **Physical Security**

The computer site and related infrastructures (e.g., information system servers, protected interface equipment, associated peripherals, communications equipment, wire closets, patch panels, etc.) must have physical security that at all times protects [CUSTOMER] Data against any unauthorized access to, or routine viewing of, computer devices, access devices, and printed and stored data.

Data accessed shall always be maintained in a secure environment (with limited access by authorized personnel both during work and non-work hours) using devices and methods such as, but not limited to: alarm systems, locked containers of various types, fireproof safes, restricted areas, locked rooms, locked buildings, identification systems, guards, or other devices reasonably expected to prevent loss or unauthorized removal of manually held data. Vendor shall also protect against unauthorized use of passwords, keys, combinations, access logs, and badges.

Whenever possible, computer operations must be in a secure area with restricted access.

The Vendor agrees that the systems operation room (which houses network equipment, servers and other centralized processing hardware) shall be accessible only by IT personnel or executive management.

In situations such as remote terminals, or office work sites where all of the requirements of a secure area with restricted access cannot be maintained, the equipment shall receive the highest level of protection and shall be consistent with IRS Publication 1075, Section 4.7. Alternate Work Sites.

Data accessed shall be destroyed on a periodic basis in a manner consistent with state policy and Federal regulations for destruction of private or confidential data.

Vendor shall protect information systems against environmental hazards and provide appropriate environmental protection in facilities containing information systems.

### **Personnel**

Adjacent will conduct background checks on customers who require direct access to the platform as warranted. We will not conduct checks on those customers connecting to the SaaS portal.

[CUSTOMER] shall have the right to conduct a criminal background check on Vendor and any of Vendor's Agents that are assigned to provide services to the [CUSTOMER]. Upon request, and to assist [CUSTOMER] in performing a criminal background check, Vendor shall provide identifying data and a signed consent form and authorization form from each person whose background will be checked.

At the sole discretion of the [CUSTOMER], Vendor's Agents assigned to provide services to [CUSTOMER] are subject to removal from providing such services.

Vendor shall ensure that all persons having access to data obtained from [CUSTOMER] Systems are thoroughly briefed on related security procedures, restricted usage, and instructions requiring their awareness and compliance. Vendor shall provide annual reorientation sessions and all of Vendor's Agents that perform or are assigned to perform Services shall re-execute, and/or renew their acceptance of, all applicable security documents and to ensure that they remain alert to all security requirements.

If the [CUSTOMER] determines that an individual or individuals should not have [CUSTOMER] systems access, then such access shall be denied and the Vendor shall be given written notice of the denial.

Vendor shall protect against any key-person dependence or collusion by enforcing policies of separation of duties, restricted job responsibilities, audit logging, and job rotation.

### **Logical/Information System Protections**

The Vendor shall take all reasonable steps to ensure the logical security of all information systems used in the performance of this Agreement, including:

Independent oversight of systems administrators and programmers;

Restriction of user, operator and administrator accounts in accordance with job duties;

Authentication of users to the operating system and application software programs;

Audit trails for user account adds, deletes and changes, as well as, access attempts and updates to individual data records; and

Protection to prevent unauthorized processing in or changes to software, systems, and [CUSTOMER] Data in the production environment.

Vendor shall implement protection for the prevention, detection and correction of processing failure, or deliberate or accidental acts that may threaten the confidentiality, availability or integrity of [CUSTOMER] Data.

Vendor shall implement counter-protection against malicious software on Vendor's internal systems used in contract performance.

Vendor shall ensure that relevant security incidents are identified, monitored, analyzed and addressed.

Vendor shall promote individual accountability and provide data security awareness training to all individuals performing Services.

Vendor shall apply a high-level of protection toward hardening all security and critical server communications platforms and ensure that operating system versions are kept current.

At least once each month, Vendor shall report its data security status, to include current documentation of asset lists, licenses and agreements relating to assets used in the performance of Services.

Vendor shall adhere to mutually agreed upon procedures for authorizing hardware and software changes, and for evaluation of their security impact.

Vendor shall adhere to [CUSTOMER]-approved access methods, and the protection and use of unique identifiers such as user identifications and passwords.

Vendor shall have an authorization process for user access and privileges. Any access not granted is prohibited.

Vendor shall maintain an access protection list that details the rights and privileges with respect to each such user.

Vendor shall institute a process that provides for immediate revocation of a user's access rights and the termination of the connection between systems, if warranted by the nature of any security incident.

Re-use of [CUSTOMER] Data in any form is not permitted.

**Security Audit; Right to Audit, Investigate and Inspect.**

Without notice, the Vendor shall permit, and shall require Vendor's Agents to, permit the [CUSTOMER], the State Auditor of Texas, the United States Internal Revenue Service, the United States Department of Justice and the Comptroller General of the United States to:

Monitor and observe the operations of, and to perform security investigations, audits and reviews of the operations and records of, the Vendor and Vendor's agents;

Inspect its information system in order to access security at the operating system, network, and application levels; provided, however, that such access shall not interfere with the daily operations of managing and running the system; and

Enter, unannounced, into the offices and places of business of the Vendor and Vendor's agents for a security inspection of the facilities and operations used in the performance of Services. Specific remedial measures may be required in cases where the Vendor or Vendor's agents are found to be noncompliant with physical and/or data security protection.

Any audit of documents shall be conducted at the Vendor's principal place of business and/or the location(s) of the Vendor's operations during the Vendor's normal business hours and at the [CUSTOMER]'s expense. Vendor shall provide to [CUSTOMER] and such auditors and inspectors as

[CUSTOMER] may designate in writing, on Vendor's premises, (or if the audit is being performed of a Vendor's agent, the Agent's premises, if necessary) space, office furnishings (including lockable cabinets), telephone and facsimile services, at least one workstation connected to each Vendor system subject to the audit, utilities and office-related equipment and duplicating services as [CUSTOMER] or such auditors and inspectors may reasonably require to perform the audits.

Vendor shall supply to the [CUSTOMER] and the State of Texas any data or reports rendered or available in conjunction with any security audit of Vendor or Vendor's agents if those reports pertain, in whole or in part, to the Services. This obligation shall extend to include any report(s) or other data generated by any security audit conducted up to [TERM OF AUDITABILITY] after the date of termination or expiration of the contract. Records and Audit shall be in accordance with Section 7C of Appendix A, DIR Contract No. DIR-TSO-2718.

### **Security Incidents Response to Security Incidents**

Vendor shall detect and respond to security incidents which might occur. Vendor shall document its relevant procedures and processes into an internal incident response plan and provide such plan for [CUSTOMER] approval no later than thirty (30) days prior to [CUSTOMER] Data being provided to Vendor.

### **Notice**

The term "security incident" means an occurrence or event where the confidentiality of [CUSTOMER] Data may have been compromised and includes, without limitation, a failure by Vendor to perform its obligations under this contract.

Within [FIRST TERM] of discovering or having any reason to believe that there has been, any physical, personnel, system, or [CUSTOMER] Data security incident Vendor shall initiate risk mitigation and notify the [CUSTOMER] Chief Information Security Officer ("[CUSTOMER] CISO") and the [CUSTOMER] Contract Manager, by telephone and by email, of the security incident and the initial risk mitigation steps taken.

Within [SECOND TERM] of the discovery, Vendor shall conduct a preliminary risk analysis of the security incident; commence an investigation into the incident; and provide a written report to the [CUSTOMER] CISO, with a copy to the [CUSTOMER] Contract Manager fully disclosing all information relating to the security incident and the results of the preliminary risk analysis. This initial report shall include, at a minimum: nature of the incident (e.g., data loss/corruption/intrusion); cause(s); mitigation efforts; corrective actions; and estimated recovery time.

Each [FOLLOW-UP PERIOD] thereafter until the investigation is complete, Vendor shall: (i) provide the [CUSTOMER] CISO, or the [CUSTOMER] CISO's designee, with a [REPORTING FREQUENCY TERM] oral or written report regarding the investigation status and current risk analysis; and (ii) confer with the [CUSTOMER] CISO, or the [CUSTOMER] CISO's designee, regarding the proper course of the investigation and risk mitigation.

Whenever oral reports are provided, Vendor shall provide, by close of business [WRITTEN REPORTING DAY], a written report detailing the foregoing daily requirements.

### **Final Report**

Within one (1) [CUSTOMER] Business Day of completing the risk analysis and investigation, Vendor shall submit a written Final Report to the [CUSTOMER] CISO with a copy to the [CUSTOMER] Contract Manager, which shall include:

A detailed explanation of the cause(s) of the security incident;

A detailed description of the nature of the security incident, including, but not limited to, extent of intruder activity (such as files changed, edited or removed; Trojans), and the particular [CUSTOMER] Data affected; and

A specific cure for the security incident and the date by which such cure shall be implemented, or if the cure has been put in place, a certification to the [CUSTOMER] that states: the date that Vendor implemented the cure and a description of how the cure protects against the possibility of a recurrence.

If the cure has not been put in place by the time the report is submitted, Vendor shall within [CERTIFICATION TERM] after submission of the final report, provide a certification to the [CUSTOMER] that states: the date that Vendor implemented the cure and a description of how the cure protects against the possibility of a recurrence.

If Vendor fails to provide a Final Report and Certification within [FINAL REPORT AND CERTIFICATION TERM] of the security incident, Vendor agrees the [CUSTOMER] may exercise any remedy in equity, provided by law, or identified in the contract.

### **Independent Right to Investigate**

The [CUSTOMER] reserves the right to conduct an independent investigation of any security incident, and should [CUSTOMER] choose to do so, Vendor shall cooperate fully, making resources, personnel and systems access available.

### **Remedial Action**

#### **Remedies Not Exclusive and Injunctive Relief**

The remedies provided in this section are in addition to, and not exclusive of, all other remedies available within this contract, or at law or in equity. [CUSTOMER]'s pursuit or non-pursuit of any one remedy for a security incident(s) does not constitute a waiver of any other remedy that [CUSTOMER] may have at law or equity.

If injunctive or other equitable relief is available, then Vendor agrees that the [CUSTOMER] shall not be required to post bond or other security as a condition of such relief.

### **Notice to Third Parties**

Subject to [CUSTOMER] review and approval, Vendor shall provide notice of a security incident affecting a third party by first-class U.S. Mail, with such notice to include: (i) a brief description of what happened; (ii) to the extent possible, a description of the types of personal data that were involved in the security breach (e.g., full name, SSN, date of birth, home address, account number, etc.); (iii) a brief description of what is being done to investigate the breach, mitigate losses, and to protect against any further breaches; (iv) contact procedures for those wishing to ask questions or learn additional data, including a toll-free telephone number, website and postal address; (v) steps individuals should take to protect themselves from the risk of identity theft, including steps to take advantage of any credit monitoring; and (vi) contact information for the Federal Trade Commission website, including specific publications. Notice of the security incident shall comply with Section 504 of the Rehabilitation Act of 1973, with accommodations that may include establishing a Telecommunications Device for the Deaf (TDD) or posting a larger-type notice on the website containing notice. The notice must comply with the notification requirements of Section 521.053, Texas Business and Commerce Code including, but not limited to, that section's consumer reporting agency notification requirements.

The [CUSTOMER] is a government agency subject to the Texas Public Information Act, Chapter 552 of the Government Code ("the Act"). All information submitted to [CUSTOMER] by Vendor is subject to release as public information. All information shall be presumed to be subject to disclosure unless a specific exception to disclosure under the Act applies. If it is necessary for the Vendor to provide the [CUSTOMER] information that Vendor believes is proprietary or otherwise confidential information, that proprietary or confidential information must be clearly identified and reference shall be made to the specific exception to disclosure in the Act. Any information which is not clearly identified as proprietary or confidential shall be deemed to be subject to disclosure pursuant to the Act.

**8. REPRESENTATIONS, WARRANTIES, AND COVENANTS.** Vendor represents, warrants and covenants that:

- (i) the Services shall be rendered with promptness, due care, skill and diligence;
- (ii) the Services shall be executed in a professional and workmanlike manner, in accordance with the requirements of the Statement of Work and accepted industry standards of first tier providers of services that are the same as or similar to the Services;
- (iii) Vendor shall use adequate numbers of qualified individuals with suitable training, education, experience, know-how, competence and skill to perform the Services;
- (iv) Vendor shall provide such individuals with training as to new products and services prior to the implementation of such products and services in [CUSTOMER]s' environments; and
- (v) Vendor shall have the resources, capacity, expertise and ability in terms of equipment, materials, know-how and personnel to provide the Services.

Vendor represents, warrants and covenants that it is either the owner of or is authorized to use, and possesses sufficient rights to grant the rights and licenses contained in this Agreement to, any and all materials, equipment, systems and other resources or items provided by Vendor. As to any such materials, equipment, systems, resources or items that Vendor does not own, Vendor shall advise [CUSTOMER] as

to the ownership and extent of Vendor's rights with regard to such materials, equipment, systems, resources or items to the extent any limitation in such rights would materially impair Vendor's performance of its obligations under this Agreement or the right and licenses granted by Vendor under this Agreement.

**9. WARRANTY.** Except as specifically set forth in Section 8 herein, the Services herein are being delivered to [CUSTOMER] "as-is" without warranty of any kind, expressed or implied, including, but not limited to warranties of merchantability or fitness for a particular purpose. [CUSTOMER] assumes full responsibility for exercising any and all due diligence with regard to determining the applicability and fitness of purpose for any use of the Services and other deliverables and assumes full responsibility for such determination and use.

**10. INSURANCE.** Vendor agrees to carry the insurance coverage required in Section 80 of Appendix A, DIR Contract Number DIR-TSO-2718. Additional insurance beyond required minimums agreed to between the parties is detailed here:

- (i) Comprehensive General Liability Insurance with a minimum limit of [MINIMUM INSURANCE LIMIT] for each occurrence with an aggregate of [AGGREGATE INSURANCE], and
- (ii) Automobile Liability Insurance for all owned, non-owned and hired vehicles with minimum limits of Bodily Injury of [AUTO INSURANCE LIMIT PER PERSON] for each person and [AUTO INSURANCE LIMIT PER OCCURRENCE] for each occurrence and Property Damage Limits of [PROPERTY INSURANCE LIMIT PER OCCURRENCE] for each occurrence.

Proof of, or commitment for, the insurance coverage detailed above, must be presented in the form acceptable to [CUSTOMER] upon the execution of this Agreement. If Vendor submits a commitment for insurance, this Agreement may, in the sole discretion of [CUSTOMER], be terminated if actual proof of insurance is not received by [CUSTOMER] within ten (10) calendar days of [CUSTOMER]'s written demand for such proof of insurance. The insurance coverage must be written by a company licensed to do business in the State of Texas, and Vendor shall not cause said insurance coverage to be canceled nor permit any insurance to lapse. The proof of, or commitment for, the insurance and the insurance policies shall contain a provision that coverage afforded under the policies will not be modified, canceled or allowed to expire until at least thirty (30) calendar days prior written notice has been given to [CUSTOMER].

Vendor shall provide [CUSTOMER] with immediate written notice of cancellation by the insurer of any required coverage or a material change by Vendor or the insurer that affects the coverage. In the event that any of the coverage is canceled by the insurer for any reason, Vendor shall obtain replacement coverage acceptable to [CUSTOMER] no later than fifteen (15) [CUSTOMER] Business Days after the cancellation of coverage. If the Vendor fails to maintain the required coverage, [CUSTOMER] shall have the right (without the obligation to do so) to secure same in the name and for the account of [CUSTOMER], in which event the Vendor shall pay the cost thereof. If any of the insurance coverage detailed above are required to remain in force after the completion of all services, an additional certificate evidencing continuation of such coverage shall be submitted at the same time that Vendor submits its final invoice for payment under this Agreement.

11. **INDEMNITIES.** Indemnification shall be in accordance with Section 8A of Appendix A, DIR Contract No. DIR-TSO-2718.

12. **LIMITATIONS OF LIABILITY.** Limitation of Liability shall be in accordance with Section 8K of Appendix A, DIR Contract No. DIR-TSO-2718.

13. **LIABILITY FOR TAXES.** The Vendor shall pay all taxes resulting from this Agreement including but not limited to any federal, state or local income, sales, excise or property taxes. [CUSTOMER] is exempt from the payment of sales, excise, and use taxes, taxes on property owned by the [CUSTOMER], and taxes on tangible personal property subject to a lease-purchase agreement. [CUSTOMER] shall not be liable to reimburse Vendor for the payment of such taxes incurred by Vendor in acquiring any goods or services as a part of any work called for in this procurement and Vendor's invoice shall not include any amount for such taxes. The [CUSTOMER] shall furnish to Vendor, upon request, suitable documentation of the [CUSTOMER]'s exemption from such taxes on goods and services procured on behalf of the [CUSTOMER].

14. **GOVERNING LAW.** This Agreement is to be construed in accordance with and governed by the laws of the State of Texas, without regard to or application of provisions relating to choice of law. The exclusive venue for any and all legal proceedings that might arise from this Agreement shall be Travis County, Texas.

15. **NOTICES.** Any notice specifically required to be given in writing under this Agreement shall be by a writing placed in the United States mail, certified, postage prepaid, return receipt requested, addressed as follows:

To [CUSTOMER]: [CUSTOMER CONTACT]  
Attention: \_\_\_\_\_

To Vendor: Adjacent Technologies, Inc.:  
10415 Morado Circle  
Building 1, Suite 120  
Austin, TX 78759  
Attention: David Parks

Either party may update this notice information by providing the other party with notice of any changes in accordance with the notice provisions of this paragraph.

16. **DISPUTE RESOLUTION.** Enforcement of Contract and Dispute Resolution shall be in accordance with Section 9A of Appendix A, DIR Contract No. DIR-TSO-2718.

17. **COPYRIGHTS AND INTELLECTUAL PROPERTY.** All software, computer code or other works developed under this Agreement shall be the sole copyrighted intellectual property of Vendor and [CUSTOMER] shall have a royalty-free, nonexclusive license to reproduce, publish or otherwise use for [CUSTOMER]'s purposes the copyright in the works developed under this Agreement; provided,

however, that [CUSTOMER] shall not reproduce, publish or otherwise use or distribute such works for use by any third party.

**18. INDEPENDENT CONTRACTOR.** This Agreement shall not render the Vendor an employee, officer, or agent of the [CUSTOMER] for any purpose. The Vendor is and shall remain an independent contractor in relationship to the [CUSTOMER]. The [CUSTOMER] shall not be responsible for withholding taxes with respect to the Vendor's compensation under this Agreement. The Vendor shall have no claim against the [CUSTOMER] under this Agreement for vacation pay, sick leave, retirement benefits, social security, worker's compensation, health or disability benefits, unemployment insurance benefits, or employee benefits of any kind.

**19. FORCE MAJEURE.**

Force Majeure shall be in accordance with Section 9C of Appendix A, DIR Contract No. DIR-TSO-2718.

**20. FRAUD, WASTE AND ABUSE.** The Vendor shall report any suspected incident of fraud, waste or abuse associated with the performance of this Agreement to any one of the following listed entities:

- (i) [LIST OF CONTACTS]

**The report of suspected misconduct shall include (if known):**

- (i) The specific suspected misconduct;
- (ii) The names of the individual(s)/entity(ties) involved;
- (iii) The date(s)/location(s) of the alleged activity(ties);
- (iv) The names and all available contact information (phone numbers, addresses) of possible witnesses or other individuals who may have relevant information; and
- (v) Any documents which tend to support the allegations.

**The words fraud, waste, or abuse as used in this document have the following meanings:**

- (i) Fraud is the use of one's occupation for obtaining personal benefit (including benefit for family/friends) through the deliberate misuse or misapplication of resources or assets.
- (ii) Waste is the extravagant careless or needless expenditure of funds or consumption of property that results from deficient practices, system controls, or decisions.
- (iii) Abuse, being distinct from fraud, encompasses illegal acts or violations of policy or provisions of contracts or grant agreements. When abuse occurs, no law, regulation or provision of a contract or grant agreement is necessarily violated. Rather, the conduct of an individual falls short of behavior that is expected to be reasonable and necessary business practice by a prudent person. An example of abuse would be misuse of the power or authority of an individual's position.

**Cooperation with the [CUSTOMER]**

The Vendor shall ensure that it cooperates with the [CUSTOMER] and other state or federal administrative agencies, at no charge to the [CUSTOMER], for purposes relating to the administration of

this Agreement. The Vendor agrees to reasonably cooperate with and work with the [CUSTOMER]'s contractors, subcontractors, and third party representatives as requested by the [CUSTOMER].

**21. NO WAIVER OF SOVEREIGN IMMUNITY.** THE PARTIES EXPRESSLY AGREE THAT NO PROVISION OF THIS CONTRACT IS IN ANY WAY INTENDED TO CONSTITUTE A WAIVER BY THE [CUSTOMER] OR THE STATE OF TEXAS OF ANY IMMUNITIES FROM SUIT OR FROM LIABILITY THAT THE [CUSTOMER] OR THE STATE OF TEXAS MAY HAVE BY OPERATION OF LAW.

**22. SEVERABILITY.** If any provision of this Agreement is construed to be illegal or invalid, such construction will not affect the legality or validity of any of its other provisions. The illegal or invalid provision will be deemed severable and stricken from the Agreement as if it had never been incorporated herein, but all other provisions will continue in full force and effect.

**23. ENTIRE AGREEMENT.** DIR Contract No. DIR-TSO-2718 and this Agreement represent the entire agreement between the parties. No prior agreement or understanding, oral or otherwise, of the parties or their agents will be valid or enforceable unless embodied in this Agreement. In the event of a conflict, the DIR Contract controls.

**24. TERMINATION. Convenience of the State of Texas.** Termination for Convenience shall be in accordance with Section 9B(3) of Appendix A, DIR-TSO-2718. Any fees due upon Termination for Convenience shall be specified and mutually agreed upon in the Statement of Work.

(i) **Cause/Default.** Termination for Cause shall be in accordance with Section 9B(4) of Appendix A, DIR Contract No. DIR-TSO-2718.

(ii) **Remedies not Exclusive.** The [CUSTOMER] may exercise any other right, remedy or privilege which may be available to it under applicable law of the State and any other applicable law or proceed by appropriate court action to enforce the provisions of this Agreement, or to recover damages for the breach of any agreement being derived from this Agreement. The exercise of any of the foregoing remedies will not constitute a termination of this Agreement unless the [CUSTOMER] notifies the Vendor in writing prior to the exercise of such remedy. The Vendor will remain liable for all covenants and indemnities under the aforesaid agreement. Except as may be limited herein, the Vendor will be liable for all legal fees, and other costs and expenses, including attorney's fees and court costs, incurred by the [CUSTOMER] with respect to the enforcement of any of the remedies listed herein.

(iii) **Change in Federal or State Requirements.** If Federal or State laws or regulations or other Federal or State requirements are amended or judicially interpreted so that either party cannot reasonably fulfill this Agreement and if the parties cannot agree to an amendment that would enable substantial continuation of the Agreement, the parties shall be discharged from any further obligations under this Agreement.

(iv) **Rights upon Termination of the Agreement.** Except as set forth herein, in the event that the Agreement is terminated for any reason, or upon its expiration, the [CUSTOMER] shall retain ownership of all associated work products and documentation with any order that results from or is associated with this Agreement in whatever form that they exist.

(v) **Survival of Terms.** Termination of this Agreement for any reason shall not release the Vendor from any liability or obligation set forth in this Agreement that is expressly stated to survive any such termination or by its nature would be intended to be applicable following any such termination.

(vi) **Contactor's Termination for Convenience.** Vendor may elect to terminate this Agreement at any time upon thirty (30) days written notice. If Vendor elects to terminate, there will be no additional fees to [CUSTOMER] for Vendor replicating the system software and associated data to an [CUSTOMER]-approved environment. Vendor will be entitled to [MIGRATION TERM] to complete the migration, and [CUSTOMER] agrees to continue paying monthly Hosting Services fees during this time.

[SIGNATURE PAGE FOLLOWS]

The parties have executed this Agreement as of the date first written above.

VENDOR:

Adjacent Technologies, Inc., a Delaware corporation

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

Name: David Parks

Title: Vice President

[CUSTOMER]:

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

Name: \_\_\_\_\_

Title: \_\_\_\_\_