



Texas Department of Public Safety Purchase Order

Purchase Order Number

405-16-P007831

SHOW THIS NUMBER ON ALL
PACKAGES, INVOICES AND
SHIPPING DOCUMENTS.

**V
E
N
D
O
R**
Vendor Number: 00006964
1742748769300 | COMMONWEALTH COMPUTER
COMPANY
24165 IH 10 WEST SUITE 217-616
USA
SAN ANTONIO, TX 78257

**S
H
I
P
T
O**
Texas Department of Public Safety
6100 Guadalupe
Austin, TX 78752
US
Email: eprocurementshipping@dps.texas.gov
Phone: (512) 424-2000

State Sales Tax Exemption Certificate: The undersigned claims an exemption from taxes under Chapter 20, Title 122A, Revised Civil Statutes of Texas, for purchase of tangible personal property described in this numbered order, purchased from contractor and/or shipper listed above, as this property is being secured for the exclusive use of the State of Texas.

**B
I
L
L
T
O**
Texas Department of Public Safety
Finance - Accounts Payable - MSC 0130
PO Box 4087
Austin, TX 78773-0130
US
Email: apinvoices@dps.texas.gov
Phone: (512) 424-2060

Solicitation (Bid) No.:

Payment Terms:
Shipping Terms:
Delivery Calendar Day(s) A.R.O.: 0

Item # 4

This Purchase Order (PO) is in accordance with the Department of Information Resource (DIR) Master Contract, DIR SDD 1951 which expires on 1/9/2017. By acceptance of this PO, vendor agrees to TandCs_PRICING REQUEST DIR ICTs and TXMAS dated 12/10/2014. Notice Under Government Code 2261.252 Pursuant to Government Code 2261.252 the Department may not enter into a contract for the purchase of goods or services with a private vendor if members of the Public Safety Commission or certain positions within the agency including the Executive Director, the General Counsel or the Procurement Director or their covered family members have a financial interest in the vendor. Any contract found to violate Government Code 2261.252 is void. Purchase Order in accordance with Quote # 19129 from Contact: Karla Broadus at 210 698 3825

Please send received notification, of delays, and or back orders of any products to PROCUREMENT
CONTACT William.Myers@dps.texas.gov

Certification Concerning Restricted Employment for Former State Officers or Employees under Texas Government Code 572.069

The Respondent certifies that it has not employed and will not employ a former TXDPS or state officer who participated in a procurement or contract negotiation for TXDPS involving the Respondent within two (2) years after the state officer or employee left state agency employment or service. This certification only applies to former state officers or employees whose state service or employment ceased on or after September 1, 2015. Notice Under Government Code 2252.908

Pursuant to Government Code 2252.908 the Department may not enter into certain contracts with a business entity unless the business entity submits a disclosure of interested parties to the Department at the time the business entity submits the signed contract to the Department. The Texas Ethics Commission has adopted rules and procedures under these provisions:

https://www.ethics.state.tx.us/whatsnew/elf_info_form1295.htm

Any contract found to violate Government Code 2252.908 is void.

Item # 1

Class-Item 204-54

Microsoft Surface Pro 4 - 512GB / Intel Core i7 / 16GB RAM
DIR SDD 1951

Quantity	Unit Price	UOM	Discount %	Total Discount Amt.	Tax Rate	Tax Amount	Freight	Total Cost
16.00	\$ 2,089.05	EA	0.00 %	\$ 0.00		\$ 0.00	\$ 0.00	\$ 33,424.80

<u>LN/FY/Account Code</u>	<u>Dollar Amount</u>
1/16/16-70061-6412-1001- - -0700- - -	\$ 33,424.80

Item # 2

Class-Item 204-68

Surface Pro 4 Type Cover (Black)
DIR SDD 1951

Quantity	Unit Price	UOM	Discount %	Total Discount Amt.	Tax Rate	Tax Amount	Freight	Total Cost
16.00	\$ 110.49	EA	0.00 %	\$ 0.00		\$ 0.00	\$ 0.00	\$ 1,767.84

<u>LN/FY/Account Code</u>	<u>Dollar Amount</u>
2/16/16-70061-6411-1001- - -0700- - -	\$ 1,767.84

Item # 3
 Class-Item 204-68

PerfectFit Surface Pro 4 Antimicrobial CleanShield Premium Film Screen Protection
 DIR SDD 1951

Quantity	Unit Price	UOM	Discount %	Total Discount Amt.	Tax Rate	Tax Amount	Freight	Total Cost
16.00	\$ 43.00	EA	0.00 %	\$ 0.00		\$ 0.00	\$ 0.00	\$ 688.00

<u>LN/FY/Account Code</u>	<u>Dollar Amount</u>
3/16/16-70061-6411-1001- - -0700- - -	\$ 688.00

TAX: \$ 0.00
 FREIGHT: \$ 0.00
 TOTAL: \$ 35,880.64

APPROVED

By: William Myers
 Phone#: (512) 424-6455
 BUYER

**PRICING REQUESTS (PR)
ISSUED BY TXDPS
TO DIR VENDORS**

1. Vendor understands that TXDPS is a "Customer" under Vendor's DIR Contract referenced on page 1 of the TXDPS PO. In submitting information to TXDPS in response to this PR, Vendor affirms its understanding of the General Provisions of Vendor's DIR Contract [generally located in Section 3 of Appendix A, DIR Standard Terms and Conditions for TXMAS Contracts] [generally located in Section 4 of Appendix A, DIR Standard Terms and Conditions for ICT Product and Related Services Contracts]:

A. Entire Agreement

The DIR Contract, Appendices, and Exhibits constitute the entire agreement between DIR and Vendor. No statement, promise, condition, understanding, inducement or representation, oral or written, expressed or implied, which is not contained in the Contract, Appendices, or its Exhibits shall be binding or valid.

B. Modification of Contract Terms and/or Amendments

- 1) The terms and conditions of the DIR Contract shall govern all transactions by Customers under the Contract. The Contract may only be modified or amended upon mutual written agreement of DIR and Vendor.
- 2) Customers will not have the authority to modify the terms of the Contract; however, additional Customer terms and conditions that do not conflict with the Contract and are acceptable to Order Filler may be added in a Purchase Order and given effect. No additional term or condition added in a Purchase Order issued by a Customer can conflict with or diminish a term or condition of the Contract. Pre-printed terms and conditions on any Purchase Order issued by Customer hereunder will have no force and effect. In the event of a conflict between a Customer's Purchase Order and the Contract, the Contract term shall control.
- 3) Customers and Vendor will negotiate and enter into written agreements regarding statements of work, service level agreements, remedies, acceptance criteria, information confidentiality and security requirements, and other terms specific to their Purchase Orders under the Contract with Vendor.

2. TXDPS issues this PR as Customer under Vendor's DIR Contract and requests that Vendor submit a response to TXDPS based on these additional terms and conditions which TXDPS has determined are specific to the TXDPS PO and are allowable under the provisions of Vendor's DIR Contract, reference section 1 of this PR.

3. **BOX CHECKED IF THIS SECTION 3 APPLICABLE TO THIS PR . CONFIDENTIALITY AND SECURITY REQUIREMENTS**

A. General Confidentiality Requirements

1. All information provided by TXDPS or sub-recipients to Vendor or created by Vendor in performing the obligations under this PO is confidential and shall not be used by Vendor or disclosed to any person or entity, unless such use or disclosure is required for Vendor to perform work under this PO.
2. The obligations of this section do not apply to information that Vendor can demonstrate:
 - i. Is publicly available;
 - ii. Vendor received from a third party without restriction on disclosure and without breach of contract or other wrongful act;
 - iii. Vendor independently developed without regard to the TXDPS confidential information; or
 - iv. Is required to be disclosed by law or final order of a court of competent jurisdiction or regulatory authority, provided that Vendor shall furnish prompt written notice of such required disclosure and shall reasonably cooperate with TXDPS at TXDPS' cost and expense, in any effort made by the TXDPS to seek a protection order or other appropriate protection of its confidential information.
3. Vendor shall notify sub-recipient in writing of any unauthorized release of confidential information within two (2) business days of when Vendor knows or should have known of any unauthorized release of confidential information obtained from sub-recipient(s).
4. Vendor shall maintain all confidential information, regardless whether obtained from TXDPS or from sub-recipient(s) in confidence during the term of this PO and after the expiration or earlier termination of this PO.
5. If Vendor has any questions or doubts as to whether particular material or information is confidential information, Vendor shall obtain the prior written approval of TXDPS prior to using, disclosing, or releasing such information.
6. Vendor acknowledges that TXDPS' and sub-recipient(s) confidential information is unique and valuable, and that TXDPS and sub-recipient(s) may have no adequate remedy at law if Vendor does not comply with its confidentiality obligations under this PO. Therefore, TXDPS shall have the right, in addition to any other rights it may have, to seek in any Travis County court of competent jurisdiction temporary, preliminary, and permanent injunctive relief to restrain any breach, threatened breach, or otherwise to specifically enforce any confidentiality obligations of Vendor if Vendor fails to perform any of its confidentiality obligations under this PO.
7. Vendor shall immediately return to TXDPS all confidential information when this PO terminates, at such earlier time as when the confidential information is no longer required for the performance of this PO or when TXDPS requests that such confidential information be returned.
8. Information, documentation and other material in connection with this PO, including Vendor's Offer, may be subject to public disclosure pursuant to the Texas Government Code, Chapter 552.
9. The FBI and TXDPS have computer security requirements. Vendor's and subcontractor's employees working on this assignment shall sign and submit appropriate agreements and abide by these security requirements, within five (5) calendar days of TXDPS' request.

B. Sensitive Personal Information

To the extent this subsection does not conflict with the subsection herein entitled "General Confidentiality Requirements," Vendor shall comply with both subsections. To the extent this subsection conflicts with the subsection herein entitled "General Confidentiality Requirements," this subsection entitled "Sensitive Personal Information" controls.

"Sensitive personal information" is defined as follows:

1. An individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:
 - a. Social security number;
 - b. Driver's license number or government-issued identification number; or
 - c. Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
2. Information that identifies an individual and relates to:
 - a. The physical or mental health or condition of the individual;
 - b. The provision of health care to the individual; or
 - c. Payment for the provision of health care to the individual.
3. Sensitive personal information does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government.
4. "Breach of system security" is defined as follows: Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information Vendor maintains under this PO, including data that is encrypted if Vendor's employee or agent accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of Vendor for the purposes of performing under this PO is not a breach of system security unless the employee or agent of Vendor uses or discloses the sensitive personal information in an unauthorized manner.
5. Vendor shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by Vendor under this PO.
6. Vendor shall notify TXDPS, any affected sub-recipient and the affected people of any breach of system security immediately after discovering the breach or receiving notification of the breach, if sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. However, Vendor shall delay providing notice to the affected people and sub-recipients at TXDPS' request, if TXDPS determines that the notification shall impede a criminal investigation. The notification to the affected people shall be made as soon as TXDPS determines that it will not compromise any criminal investigation.
7. Vendor shall give notice as follows, at Vendor's expense:
 - a. Written notice;
 - b. Electronic notice, if the notice is provided in accordance with 15 U.S.C. Section 7001;
 - c. Notice as follows:
 - i. If Vendor demonstrates that the cost of providing notice would exceed \$250,000, the number of affected people exceeds 500,000, or Vendor does not have sufficient contact information for the affected people, Vendor may give notice as follows:
 - Electronic mail, if Vendor has an electronic mail address for the affected people;
 - Conspicuous posting of the notice on Vendor's website;
 - Notice published in or broadcast on major statewide media; or
 - ii. If Vendor maintains its own notification procedures (as part of an information security policy for the treatment of sensitive personal information) that comply with the timing requirements for notice under this subsection entitled "Sensitive Personal Information," Vendor may provide notice in accordance with that policy.
8. If this subsection requires Vendor to notify at one time more than 10,000 people of a breach of system security, Vendor shall also notify, without unreasonable delay, each consumer reporting agency (as defined by 15 U.S.C. Section 1681a) that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices.
9. In the event of a breach of system security, if sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person, TXDPS is authorized to assess liquidated damages in the amount of \$ [REDACTED] against Vendor for the following damages; however, TXDPS reserves the right to claim actual damages for any damages other than the following: limited to the initial assessment and review of lost or compromised data. This amount is a reasonable estimate of the damages TXDPS shall suffer as a result of such breach and is enforceable. Vendor will not be responsible and liquidated damages may not be assessed due to a breach of system security caused entirely by someone other than Vendor, Vendor's subcontractor, or Vendor's agent. Any liquidated damages assessed under this Contract may, at TXDPS' option, be deducted from any payments due Vendor. TXDPS has the right to offset any liquidated damages payable to TXDPS, as specified above, against any payments due to Vendor. If insufficient payments are available to offset such liquidated damages, then Vendor shall pay to TXDPS any remaining liquidated damages within fifteen (15) calendar days following receipt of written notice of the amount due.

4. BOX CHECKED IF THIS SECTION 4 APPLICABLE TO THIS PR. CRIMINAL HISTORY BACKGROUND CHECK:

- A. Vendor shall have its project personnel – as specifically identified by TXDPS -- submit to TXDPS a fingerprint-based Criminal History Background Investigation, if required by TXDPS, at Vendor's expense. To facilitate this Criminal History Background Investigation, each person shall complete TXDPS' Vendor Background Information form (HR-22), which shall be provided by TXDPS.
- B. If TXDPS requires a fingerprint-based Criminal History Background Investigation, Vendor will not allow personnel to work on the project who have not successfully completed TXDPS's fingerprint-based Criminal History Background Investigation and who do not otherwise maintain TXDPS's security clearance. TXDPS has the right to prevent Vendor's personnel from gaining access to TXDPS' building(s) and computer systems if TXDPS determines that such personnel do not pass the background check or fail to otherwise maintain TXDPS security clearance.
- C. When required, Vendor's Project Manager shall provide the following to TXDPS' Project Manager within 21 calendar days of receiving this PO: a) the completed Vendor Background Information form (HR-22) for all proposed personnel; and b) acceptable fingerprints for all proposed personnel.
- D. Throughout the term of this PO, TXDPS may require Vendor personnel to submit an annual TXDPS fingerprinted-based Criminal History Background Investigation to TXDPS.
- E. Throughout the term of this PO, Vendor shall promptly notify TXDPS of any activity or action by Vendor's personnel that may affect that individual's ability to continue to work under this PO.

5. NOTICE:

Any written notices required under this PO will be by hand delivery to Vendor's office address specified on Page 1 of this PO or by U.S. Mail, certified, return receipt requested, to TXDPS, 5805 N. Lamar Blvd., Austin, Texas 78752. Notice will be effective on receipt by the affected party. Either party may change the designated notice address in this Section by written notification to the other party.

6. OWNERSHIP OF HARDWARE AND TANGIBLE PERSONAL PROPERTY; PURCHASES ONLY:

Except as otherwise indicated on this PO by specific reference to this Section, TXDPS shall own all hardware and tangible personal property provided by Vendor under this PO. This PO is structured as a separate contract under which the costs for hardware and tangible personal property are separately stated from the charge for services. Under this PO, title in all hardware and tangible personal property shall pass directly from Vendor to the State of Texas upon delivery, and upon delivery all property shall be labeled as the property of the State of Texas. Vendor shall make no use of the hardware or tangible personal property prior to passage of title to the State of Texas. TXDPS makes no representation or warranty to Vendor that Vendor's purchase of such hardware and tangible personal property shall be exempt from any state, local or other applicable taxes; however, Vendor shall make reasonable efforts to obtain such exemptions prior to purchasing such hardware and tangible personal property and shall notify TXDPS of the status of such exemptions. Vendor's pricing shall be reduced by the amount of taxes resulting from such exemptions.

7. REPRESENTATIONS AND WARRANTIES RELATED TO SOFTWARE:

Vendor represents and warrants each of the following for all Software to which TXDPS has access under this PO:

- A. Vendor has sufficient right, title, and interest in the Software to grant the license required.
- B. Contract terms and conditions included in any "clickwrap", "browsewrap", "shrinkwrap", or other license agreement that accompanies any Software, including but not limited to Software Updates, Software Patch/Fix, or Software Upgrades, provided under this Contract are void and have no effect unless the Department specifically agrees to each licensure term in this Contract.
- C. The Software provided under this PO does not infringe upon or constitute a misuse or misappropriation of any patent, trademark, copyright, trade secret or other proprietary right;
- D. Software and any Software Updates, Software Maintenance, Software Patch/Fix, and Software Upgrades provided under this PO will not contain viruses, malware, spyware, key logger, back door or other covert communications, or any computer code intentionally designed to disrupt, disable, harm, or otherwise impede in any manner, including aesthetical disruptions or distortions, the operation of the computer program, or any other associated software, firmware, hardware, or computer system, (including local area or wide-area networks), in a manner not intended by its creator(s); and
- E. Software provided under this PO does not and will not contain any computer code that would disable the Software or impair in any way its operation based on the elapsing of a period of time, exceeding an authorized number of copies, advancement to a particular date or other numeral, or other similar self-destruct mechanism (sometimes referred to as "time bombs", "time locks", or "drop dead" devices) or that would permit Vendor to access the Software to cause such disablement or impairment (sometimes referred to as "trap door" devices").

8. INFORMATION TECHNOLOGY REQUIREMENTS AND STANDARDS:

Vendor represents and warrants that it shall comply with all technology, security, accessibility, warranty, maintenance, confidentiality, testing and other standards, policies and procedures of TXDPS and the State of Texas that are applicable to Vendor in its performance of this PO as such standards, policies, and procedures are amended by TXDPS or the State throughout the term of this PO, including any renewal or optional periods. The Information Resource Manager designated by TXDPS shall assist Vendor in reviewing these standards, policies and procedures and identifying those that are applicable to Vendor in its performance of this PO. Vendor shall comply with TXDPS standards and requirements wherever they are applicable to this PO. TXDPS shall have the sole right to waive specific requirements if, in its sole judgment doing so would mitigate costs or risks or significantly improve the installed and configured solution. **If required, additional requirements are included as Appendices A and B to this PR.**

- A. **System Security and Access**, if required, this information is provided as Appendix A
- B. **System Architecture and TXDPS IT Requirements**, if required, this information is provided as Appendix B

9. TEXAS PUBLIC INFORMATION ACT:

The Confidentiality Clause included in Vendor's DIR Contract [generally located in Section 8 of Appendix A, DIR Standard Terms and Conditions for TXMAS Contracts] [generally located in Section 9) of Appendix A, DIR Standard Terms and Conditions for ICT Product and Related Services Contracts], is modified to include the following sentence: Vendor shall make any information created or exchanged with the state pursuant to this PO, and not otherwise exempted from disclosure under the Texas Public Information Act, available in a format that is accessible by the public at no additional charge to the state. **TXDPS requires such information to be available in _____ format.**

10. U.S. DEPARTMENT OF HOMELAND SECURITY'S E-VERIFY SYSTEM

By entering into this Contract, the Contractor certifies and ensures that it utilizes and will continue to utilize, for the term of this Contract, the U.S. Department of Homeland Security's E-Verify system to determine the eligibility of:

- All persons employed to perform duties within Texas, during the term of the Contract; and
- All persons (including subcontractors) assigned by the Contractor to perform work pursuant to the Contract, within the United States of America.

The Contractor shall provide, upon request of (agency name), an electronic or hardcopy screenshot of the confirmation or tentative non-confirmation screen containing the E-Verify case verification number for attachment to the Form I-9 for the three most recent hires that match the criteria above, by the Contractor, and Contractor's subcontractors, as proof that this provision is being followed.

If this certification is falsely made, the Contract may be immediately terminated, at the discretion of the state and at no fault to the state, with no prior notification. The Contractor shall also be responsible for the costs of any re-solicitation that the state must undertake to replace the terminated Contract.

11. VENDOR AFFIRMATIONS TO TXDPS:

Signing a response to this PR with a false statement or otherwise providing TXDPS with a false statement is a material breach of contract and shall void this PO, and Vendor shall be removed from all bid lists. During the term of this PO, Vendor shall, for itself and on behalf of its subcontractors, promptly disclose to TXDPS all changes that occur to the foregoing certifications, representations and warranties. Vendor covenants to fully cooperate in the development and execution of resulting documentation necessary to maintain an accurate record of the certifications, representations and warranties. By signature hereon affixed, Vendor hereby certifies that:

- A. Vendor has not given, offered to give, nor intends to give at any time hereafter any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor, or service to a public servant in connection with this PO.
- B. Vendor certifies that it is not currently delinquent in the payment of any franchise tax owed the State of Texas and are not ineligible to receive payment under §231.006(d), Texas Family Code, regarding child support, and that the individual or business entity named in this PO is not ineligible to receive the specified payment and acknowledges that this PO may be terminated and payment may be withheld if this certification is inaccurate. Furthermore, any Vendor subject to §231.006, Gov't Code, shall include names and Social Security numbers of each person with at least 25% ownership of the business entity submitting this PO. This information must be provided prior to award. Enter the Name & Social Security Numbers for each person below:

Name:	Social Security Number:
Name:	Social Security Number:
Name:	Social Security Number:

- C. Under §2155.004, Gov't Code, Vendor certifies that the individual or business entity named in this Offer is not ineligible to receive a PO and acknowledges that this PO may be terminated and payment withheld if this certification is inaccurate. §2155.004 prohibits a person or entity from receiving a state contract if they received compensation for participating in preparing the solicitation or specifications for this PO.
- D. As required by §2252.903, Gov't Code, Vendor agrees that any payments due under this PO shall be directly applied towards eliminating any debt or delinquency including, but not limited to, delinquent taxes, delinquent student loan payments, and delinquent child support, until the debt is paid in full. Vendor shall comply with rules adopted by TXDPS under §§403.055, 403.0551, 2252.903, Gov't Code and other applicable laws and regulations regarding satisfaction of debts or delinquencies to the State of Texas.
- E. Pursuant to §669.003, Gov't Code, TXDPS may not issue a PO to a person who employs a current or former executive head of any state agency until four years has passed since that person was the executive head of the state agency. Vendor certifies that it does not employ any person who was the executive head of any state agency in the past four years. If Vendor does employ a person who was the executive head of a state agency, provide the following information:

Name of Former Executive:

Name of State Agency:

Date of Separation from State Agency:

Position with Vendor:

Date of Employment with Vendor:

- F. In accordance with §2155.4441, Gov't Code, Vendor agrees that during the performance of this PO it shall purchase products and materials produced in Texas when they are available at a price and time comparable to products and materials produced outside this state.
- G. Vendor certifies that the entity and its principals are eligible to participate in this transaction and have not been subjected to suspension, debarment, or similar ineligibility determined by any federal, state or local governmental entity and that Vendor is in compliance with the State of Texas statutes and rules relating to procurement and that Vendor is not listed on the federal government's terrorism watch list as described in Executive Order 13224. Entities ineligible for federal procurement are listed at <http://www.epls.gov>.
- H. Sections 2155.006 and 2261.053, Gov't Code, prohibit state agencies from awarding contracts to any person who, in the past five years, has been convicted of violating a federal law or assessed a penalty in connection with a contract involving relief for Hurricane Rita, Hurricane Katrina, or any other disaster, as defined by §418.004, Gov't Code, occurring after September 24, 2005. Under §2155.006, Gov't Code, Vendor certifies that the individual or business entity named in this PO is not ineligible to receive a PO and acknowledges that this PO may be terminated and payment withheld if this certification is inaccurate.
- I. Vendor represents and warrants that payment to Vendor and Vendor's receipt of appropriated or other funds under this PO are not prohibited by §556.005 or §556.008, Gov't Code, relating to the prohibition of using state funds for lobbying activities.
- J. Vendor represents and warrants that it has no actual or potential conflicts of interest in providing the requested items to TXDPS under this PO, if any, and that Vendor's provision of the requested items under this PO, if any, would not reasonably create an appearance of impropriety.
- K. Vendor certifies that it, nor anyone acting for it, has violated the antitrust laws of the United States or the State of Texas, nor communicated directly or indirectly to any competitor or any other person engaged in such line of business for the purpose of obtaining an unfair price advantage.
- L. Vendor certifies that to the best of its knowledge and belief, there are no suits or proceedings pending or threatened against or affecting it, which if determined adversely to it will have a material adverse effect on its ability to fulfill its obligations under this PO.

- M. To the extent applicable to the scope of this PO, Vendor hereby certifies that it is in compliance with Subchapter Y, Chapter 361, Health and Safety Code related to the Computer Equipment Recycling Program and its rules, 30 TAC Chapter 328.
- N. Vendor certifies for itself and its subcontractors that it has identified all current or former, within the last five (5) years, employees of the State of Texas assigned to work on the TXDPS PO 20% or more of their time and has disclosed them to TXDPS and has disclosed or does not employ any relative of a current or former state employee within two (2) degrees of consanguinity, and, if these facts change during the course of this PO, Vendor certifies it shall disclose for itself and on behalf of subcontractors the name and other pertinent information about the employment of current and former employees and their relatives within two (2) degrees of consanguinity.

**APPENDIX A
SYSTEM SECURITY AND ACCESS**

**PRICING REQUEST (PR)
ISSUED BY TXDPS
TO DIR VENDORS**

1. SYSTEM SECURITY AND ACCESS

1.1 Information Technology Standards

Vendor represents and warrants that it shall comply with all technology, security, accessibility, warranty, maintenance, confidentiality, testing and other standards, policies and procedures of TXDPS and the State of Texas that are applicable to Vendor in its performance of this Contract as such standards, policies, and procedures are amended by TXDPS or the State throughout the term of this Contract, including any renewal or optional periods. The Information Resource Manager designated by TXDPS shall assist Vendor in reviewing these standards, policies and procedures and identifying those that are applicable to Vendor in its performance of this Contract.

1.2 Cloud Security

Vendor shall comply with the current Cloud Security Alliance's (CSA) Cloud Control Matrix (CCM) security requirements for Vendor hosted services or applications that are included as part of Vendor's solution. Information pertaining to CSA <https://cloudsecurityalliance.org/> and CCM information may be found at <https://cloudsecurityalliance.org/research/ccm/>.

1.3 User Security

- A. Account Management: Establish and administer user accounts in accordance with role-based scheme and shall track and monitor role assignment.
- B. Account Management: Automatically audit account creations, modifications, disabling and termination actions with notification to TXDPS' personnel.
- C. Prevent multiple concurrent active sessions for one user identification.
- D. Enforce a limit of no more than five (5) consecutive invalid access attempts by a user.
- E. Automatically lock the account/node for a ten (10) minute time period unless released by the TXDPS Administrator.
- F. Prevent further access to the system by initiating a session lock after a maximum of thirty (30) minutes of inactivity, and the session lock shall remain in effect until the user reestablishes access using appropriate identification and authentication procedures.
- G. Ensure all users shall be uniquely identified.
- H. Force users to follow the secure password attributes, below, to authenticate a user's unique ID. The secure password attributes shall:
 - 1) Be a minimum length of eight characters;
 - 2) Not be a dictionary word or proper name;
 - 3) Not be the same as the User ID;
 - 4) Expire within a maximum of ninety (90) calendar days;
 - 5) Not be identical to the previous ten (10) passwords;
 - 6) Not be transmitted in the clear text outside the secure location;
 - 7) Not be displayed in clear text when entered; and
 - 8) Never be displayed in clear text on the screen.

1.4 System Security

- A. Provide audit logs that enable tracking of activities taking place on the system.
- B. Audit logs must track successful and unsuccessful system log-on attempts.
- C. Audit logs must track successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.

- D. Audit logs must track successful and unsuccessful attempts to change account passwords.
- E. Audit logs must track successful and unsuccessful actions by privileged accounts.
- F. Audit logs must track successful and unsuccessful attempts for users to access, modify, or destroy the audit log.
- G. Provide the following content to be included with every audited event:
 - 1) Date and time of the event;
 - 2) The component of the information system (e.g. software component, hardware component) where the event occurred;
 - 3) IP address;
 - 4) Type of event;
 - 5) User/subject identity; and
 - 6) Outcome (success or failure) of the event.
- H. Provide real-time alerts to appropriate TXDPS officials in the event of an audit processing failure. Alert recipients and delivery methods must be configurable and manageable by the TXDPS System Administrators.
- I. Undergo vulnerability scan/penetration testing conducted by TXDPS or the Texas Department of Information Resources. Vendor shall remediate legitimate vulnerabilities and system/application will not be accepted until all vulnerability issues are resolved at no cost to TXDPS.
- J. Notifications shall display an approved system use notification message or banner before granting access to the system. The notification shall state:
 - 1) Users are accessing a TXDPS system;
 - 2) System usage shall be monitored, recorded and subject to audit;
 - 3) Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
 - 4) A description of the authorized use of the system.
- K. Vendor shall implement and use management and maintenance applications and tools, appropriate fraud prevention and detection, and data confidentiality/protection/encryption technologies for endpoints, servers and mobile devices. This must include mechanisms to identify vulnerabilities and apply security patches.
- L. Vendor shall establish and maintain a continuous security program as part of the Services. The security program must enable TXDPS (or its selected third party) to:
 - 1) Define the scope and boundaries, policies, and organizational structure of an information security management system;
 - 2) Conduct periodic risk assessments to identify the specific threats to and vulnerabilities of TXDPS due to the Services, subject to the terms, conditions and procedures;
 - 3) Implement appropriate mitigating controls and training programs, and manage resources; and
 - 4) Monitor and test the security program to ensure its effectiveness. Vendor shall review and adjust the security program in light of any assessed risks.

1.5 Physical Access Controls

- A. Vendor shall restrict physical access to the system(s) containing TXDPS data to authorized personnel with appropriate clearances and access authorizations.
- B. Vendor shall enforce physical access authorizations for all physical access points to the facility where information system resides;
- C. Vendor shall verify individual access authorizations before granting access to the facility containing the information system;
- D. Vendor shall control entry to the facility containing the information system using physical access devices and guards; and
- E. Vendor shall change combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.

- F. TXDPS and Vendor shall collaborate on security monitoring and incident response, define points of contact on both sides, establish monitoring and response procedures, set escalation thresholds, and conduct training. Vendor shall, at the request of TXDPS or, in the absence of any request from TXDPS, at least quarterly, provide TXDPS with a report of the incidents that it has identified and taken measures to resolve.

1.6 Data Security

- A. If Vendor or any subcontractors require access to the TXDPS network; TXDPS data; or the network processing, transporting, or storing of TXDPS' data (may at TXDPS discretion), Vendor shall be required to sign the CJIS Security Addendum, and all of Vendor's employees requiring access to the TXDPS network shall sign the FBI Certification to the CJIS Security Addendum and complete a fingerprint based background check.
- B. Vendor's solution shall protect against an employee falsely denying having performed a particular action (non-repudiation).
- C. Require Vendor, subcontractor, and their staff to obtain and provide proof of PII certifications for its employees accessing TXDPS' data at the request of TXDPS.
- D. Comply with relevant federal and state statutes and rules, and TXDPS' policies, and standards, including but not limited to CJIS requirements.
- E. Data will not be exported to an external location without the permission of TXDPS.
- F. In the event of any impermissible disclosure, loss or destruction of Confidential Information, the receiving Party must immediately notify the disclosing Party and take all reasonable steps to mitigate any potential harm or further disclosure, loss or destruction of such Confidential Information.

1.7 Encryption

The system shall protect the confidentiality of TXDPS' information. All data transmitted outside or stored outside the secure network shall be encrypted. When cryptography (encryption) is employed within information systems, the system shall perform all cryptographic operations using Federal Information Processing Standard (FIPS) PUB140-2 validated cryptographic modules with approved modes of operation. The system shall produce, control, and distributes symmetric cryptographic keys using NIST-approved key management technology and processes. The key management process is subject to audit by TXDPS.

- A. Wireless: The following requirements specifies the minimum set of security measures required on WLAN-enabled portable electronic devices (PEDs) that transmit, receive, process, or store PII or confidential information:
 - 1) Personal Firewall: WLAN-enabled PED shall use personal firewalls or run a Mobile Device Management system that facilitates the ability to provide firewall services.
 - 2) Anti-Virus Software: Anti-virus software shall be used on wireless ECMs-capable PEDs or run a Mobile Device Management System that facilitates the ability to provide anti-virus services.
 - 3) Encryption of PII or confidential data-in-transit via WLAN-enabled PEDs, systems and technologies will be implemented in a manner that protects the data end-to-end. All systems components within a WLAN that wirelessly transmit PII or confidential information shall have cryptographic functionality that is validated under the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program as meeting requirements per Federal Information Processing Standards (FIPS) Publication 140-2. Encryption shall be a minimum of 128 bit.
 - 4) Data-at-Rest: Data at rest encryption shall be implemented in a manner that protects PII and confidential information stored on WLAN enabled PEDs by requiring that the PED must be powered on and credentials successfully authenticated in order for the data to be deciphered. Data-at-rest encryption shall include the encryption of individual files, portions of the file system (e.g., directories or partitions), or the entire drive (e.g. hard disks, on-board memory cards, memory expansion cards). In recognition of the increased risk of unauthorized access to PII or confidential information in the event that a PED is lost or stolen and the inherently mobile nature of these devices, encryption shall be provided for data-at-rest on all WLAN enabled PEDs that is validated as meeting FIPS 140-2.
 - 5) WLAN Infrastructure: WLAN infrastructure systems may be composed of either stand-alone (autonomous) access points (AP) or thin APS that are centrally controlled by a WLAN controller.
 - 6) Validated Physical Security: APs used in the WLANS should not be installed in unprotected environments due to an increased risk of tampering and/or theft.
- B. Mobile Device Management Requirement. Mobile Device Management (MDM) facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery. MDM shall include the following core features:
 - 1) The ability to push security policies to managed devices;
 - 2) The ability to query the device for its configuration information;

- 3) The ability to modify device configuration as required;
- 4) Security functionality that ensures the authenticity and integrity of the transaction in the three categories above;
- 5) Asset management (track/enable/disable) mobile devices being managed via the MDM server;
- 6) The ability to manage proxy access to network resources via the connection of the mobile device to the MDM server;
- 7) The ability to query devices being managed on the status of security policy compliance and to implement a specified mediation function based on compliance status;
- 8) The ability to download and store mobile device audit records;
- 9) The ability to receive alerts and other notifications from managed mobile devices;
- 10) The ability to receive alerts and other notifications from managed mobile devices;
- 11) The ability to generate audit record reports from mobile device audit records; and
- 12) Application management (application white list) for applications installed on managed mobile devices.

1.8 Secure Erasure Of Hard Disk Capability

All equipment provided to TXDPS by Vendor that is equipped with hard disk drives (i.e. computers, telephones, printers, fax machines, scanners, multifunction devices, etc.) shall have the capability to securely erase data written to the hard drive prior to final disposition of such equipment, either at the end of the equipment's useful life or the end of the related services agreement for such equipment, in accordance with 1 TAC §202.

1.9 Data Center Location Requirements

The data center must be located in the continental United States of America.

1.10 Access to Internal TXDPS Network and Systems

As a condition of gaining remote access to any internal TXDPS network and systems, Vendor shall comply with TXDPS policies and procedures. TXDPS' remote access request procedures shall require Vendor to submit a Remote Access Request form for TXDPS' review and approval.

- A. Remote access technologies provided by Vendor shall be approved by TXDPS' CISO.
- B. Individuals who are provided with access to the TXDPS network may be required to attend or review the TXDPS' Security Awareness Training on an annual basis.
- C. Vendor shall secure its own connected systems in a manner consistent with TXDPS requirements.
- D. TXDPS reserves the right to audit the security measures in effect on Vendor's connected systems without prior warning.
- E. TXDPS also reserves the right to immediately terminate network and system connections not meeting such requirements.

1.11 FBI CJIS Security Addendum

Vendor shall execute an originally signed CJIS Security Addendum which can be downloaded from <http://www.txdps.state.tx.us/securityreview>. Additionally, a CJIS Security Addendum Certification shall be signed by each employee performing duties related to this project prior to final Contract award. Each original Certification shall include an original signature of the employee and Vendor's representative. Non-compliance by Respondent will be cause for termination of contract negotiations and TXDPS may elect to enter into negotiations with the next highest evaluated Offer.

1.12 TXDPS Information Protection Policies, Standards & Guidelines

- A. Vendor, its employees, and any subcontractors shall comply with all applicable TXDPS Information Protection Policies, Standards & Guidelines and any other TXDPS requirements that relate to the protection or disclosure of TXDPS Information. TXDPS Information includes all data and information
 - 1) submitted to Vendor by or on behalf of TXDPS,
 - 2) obtained, developed, produced by Vendor in connection with this Contract,
 - 3) communicated verbally whether intentionally or unintentionally, or
 - 4) to which Vendor has access in connection with the services provided under this Contract.
- B. Such TXDPS Information may include taxpayer, Vendor, and other state agency data held by TXDPS.
- C. As used herein, the terms "Sensitive" and "Confidential" information shall have the meanings set forth in TXDPS' Information Protection Policies, Standards & Guidelines.

- D. All waiver requests shall be processed in accordance with TXDPS' Information Protection Policies, Standards & Guidelines Waiver Policy.
- E. TXDPS reserves the right to audit Vendor's compliance with TXDPS' Information Protection Policies, Standards & Guidelines
- F. TXDPS reserves the right to take appropriate action to protect TXDPS' network and information including the immediate termination of system access.
- G. Vendor shall ensure that any confidential TXDPS Information in the custody of Vendor is properly sanitized or destroyed when the information is no longer required to be retained by TXDPS or Vendor in accordance with this Contract.
- H. Electronic media used for storing any confidential TXDPS Information shall be sanitized by clearing, purging or destroying in accordance with NIST Special Publication 800-88 Guidelines for Media Sanitization. Vendor shall maintain a record documenting the removal and completion of all sanitization procedures with the following information:
 - 1) Date and time of sanitization/destruction,
 - 2) Description of the item(s) and serial number(s) if applicable,
 - 3) Inventory number(s), and
 - 4) Procedures and tools used for sanitization/destruction.
- I. No later than sixty (60) days from contract expiration or termination or as otherwise specified in this Contract, Vendor shall complete the sanitization and destruction of the data and provide to TXDPS all sanitization documentation.

1.13 Disclosure of Security Breach

Without limitation on any other provision of this Contract regarding information security or security breaches, Vendor shall provide notice to TXDPS' Project Manager and the CISO as soon as possible following TXDPS' discovery or reasonable belief that there has been unauthorized exposure, access, disclosure, compromise, or loss of sensitive or confidential TXDPS information ("Security Incident").

- A. Within twenty-four (24) hours of the discovery or reasonable belief of a Security Incident, Vendor shall provide a written report to the CISO detailing the circumstances of the incident, which includes at a minimum:
 - 1) A description of the nature of the Security Incident;
 - 2) The type of TXDPS information involved;
 - 3) Who may have obtained TXDPS information;
 - 4) What steps Vendor has taken or shall take to investigate the Security Incident;
 - 5) What steps Vendor has taken or shall take to mitigate any negative effect of the Security Incident; and
 - 6) A point of contact for additional information.
- B. Each day thereafter until the investigation is complete, Vendor shall provide the CISO with a written report regarding the status of the investigation and the following additional information as it becomes available:
 - 1) Who is known or suspected to have gained unauthorized access to TXDPS' information;
 - 2) Whether there is any knowledge if TXDPS information has been abused or compromised;
 - 3) What additional steps Vendor has taken or shall take to investigate the Security Incident;
 - 4) What steps Vendor has taken or shall take to mitigate any negative effect of the Security Incident; and
 - 5) What corrective action Vendor has taken or shall take to prevent future similar unauthorized use or disclosure.
- C. Vendor shall confer with the CISO regarding the proper course of the investigation and risk mitigation. TXDPS reserves the right to conduct an independent investigation of any Security Incident, and should TXDPS choose to do so, Vendor shall cooperate fully by making resources, personnel, and systems access available to TXDPS and TXDPS' authorized representative(s).
- D. Subject to review and approval of the CISO, Vendor shall, at its own cost, provide notice that satisfies the requirements of applicable law to individuals whose personal, confidential, or privileged data were compromised or likely compromised as a result of the Security Incident. If TXDPS, in its sole discretion, elects to send its own separate notice, then all costs associated with preparing and providing notice shall be reimbursed to TXDPS by Vendor. If Vendor does not reimburse such costs within thirty (30) calendar days of TXDPS' written request, TXDPS shall have the right to collect such costs.

1.14 Cyber Insurance Requirement

Vendor will maintain sufficient cyber insurance to cover any and all losses, security breaches, privacy breaches, unauthorized distributions, or releases or uses of any data transferred to or accessed by Vendor under or as a result of this Contract.

- A. This insurance shall provide sufficient coverage(s) for Vendor, TXDPS, and affected third parties for the review, repair, notification, remediation and other response to such events, including but not limited to, breaches or similar incidents under Chapter 521, Texas Business and Commerce Code.
- B. TXDPS may, in its sole discretion, confer with the Texas Department of Insurance to review such coverage(s) prior to approving them as acceptable under this Contract.
- C. Vendor shall obtain modified coverage(s) as reasonably requested by TXDPS within ten (10) calendar days of Vendor's receipt of such request from TXDPS.

1.15 Rights to Data, Documents and Computer Software (State Ownership)

- A. Any biographic data, demographic data, image data inclusive of fingerprints, photograph and signatures or any other data or metadata in any form acquired or accessed by Vendor in the performance of its obligations under this Contract shall be the exclusive property of the State of Texas and all such data shall be delivered to TXDPS by Vendor upon completion, termination, or cancellation of this Contract.
- B. Vendor will not use, willingly allow, or cause to have such data used for any purpose other than the performance of Vendor's obligations under this Contract without the prior written consent of TXDPS.
- C. The ownership rights described herein shall include, but not be limited to, the right to copy, publish, display, transfer, prepare derivative works, or otherwise use the works.
- D. Vendor shall provide, at no additional charge, appropriate licenses for TXDPS to use and access, as necessary for TXDPS to use and access the turnkey solution during the term of the lease, Vendor's pre-existing software or other intellectual or proprietary property that Vendor determines is necessary to facilitate the performance of Vendor's obligations under this Contract.

APPENDIX B
SYSTEM ARCHITECTURE AND IT REQUIREMENTS

PRICING REQUEST (PR)
ISSUED BY TXDPS
TO DIR VENDORS

1. SYSTEM ARCHITECTURE AND TXDPS IT REQUIREMENTS

1.1 System Architecture

- A. Vendor shall provide communication schema and network diagrams, and detailed narrative description of all network areas.
- B. The following information will assist Vendor in providing the requested detailed system architecture requirements:
- 1) Vendor's services shall provide secure connectivity to TXDPS. TXDPS connections are Ti and Internet Service Provider (ISP) connections and are considered to be quite reliable in general, but with available variable bandwidth for application needs.
 - 2) Network Topology — TXDPS utilizes a combination of public and private TCP/IP network resources. All internal communications between client resources, other systems, and system services will be through this network.
- C. Vendor shall address each of the following:
- 1) System Access Control: Vendor shall support external authentication and authorization services, auditing, and role definitions as defined in Exhibit A to this PR.
 - 2) Scalability/Bandwidth Formula: Vendor shall provide a scalability/bandwidth formula identifying the minimum and maximum bandwidth needs of the application based upon utilization required to support the number of unexpected users and volume of work.
 - 3) Solution Architecture:
 - a. Vendor shall provide the solution architecture with workflow and detailed specifications.
 - b. Vendor shall provide the recommended ideal platform.
 - c. Vendor shall provide a list of platforms supported other than the recommended platform.
 - d. Vendor shall provide all specific hardware/software that shall be utilized or integrated with application (e.g. specialized hosted tools, platforms, server software, operating systems, application servers, databases, existing hosting environments, etc.)
 - e. Vendor shall provide typical installed architecture and network topology.
 - f. Vendor shall provide the architecture of the application.
 - g. Vendor shall provide the communication standards and protocols utilized by the application.
 - 4) Vendor shall provide a complete hardware and software inventory including any servers required, an architectural diagram of the complete overall system, and the recommended workstation configuration if any and that itemizes all assumed capabilities and minimum hardware and software requirements of any TXDPS IT related systems required to access Vendor's services.
 - a. Any applicable server hardware shall identify:
 1. The processor requirements;
 2. The memory requirements;
 3. Operating System details and dependencies; and
 4. Data storage requirements.
 - b. All testing consoles and mobile device recommendations shall identify:
 1. The processor requirements;
 2. The memory requirements;
 3. Operating System details and dependencies;
 4. Data storage requirements; and
 5. Any support applications required such as Internet Explorer Adobe PDF Reader etc.
 - c. Peripherals required:
 1. Printers;
 2. Scanners; and
 3. Fax.
 - 5) Network Topography

Vendor shall be capable of supporting the number of expected users and volume of work.

1.2 Information Technology (IT) Requirements

- A. Vendor shall comply with the following standards and requirements wherever they are applicable to this Contract. TXDPS shall have the sole right to waive specific requirements if, in its sole judgment, doing so would mitigate costs or risks or significantly improve the installed and configured solution.
- 1) Vendor Hosted COTS Software – Vendor shall provide a complete hardware and software inventory including any servers required, an architectural diagram, security diagram, network diagram, network usage assessment, and communications port diagram of the complete overall system and narrative describing requested diagrams and any API and Web service components, and the recommended workstation configuration, if any. Vendor shall also itemize all assumed capabilities and minimum hardware and software requirements of any TXDPS IT related systems required to access or support product or system.
 - a. Any applicable server hardware shall identify:
 - i. Processor requirements
 - ii. Memory requirements
 - iii. Operating system details and dependencies; and
 - iv. Data storage requirements.
 - b. All workstation recommendations shall identify:
 - i. Processor requirements;
 - ii. Display requirements;
 - iii. Memory requirements;
 - iv. Operating system details and dependencies;
 - v. Data storage requirements; and
 - v. Any support applications required such as Internet Explorer, Adobe PDF Reader, etc..
 - c. Peripherals required:
 - i. Printers;
 - ii. Scanners; and
 - iii. Fax.
 - 2) TXDPS Hosted COTS Software – Vendor shall follow TXDPS’ hosting standards for any software and hardware that are hosted with the TXDPS Data Centers. The existing TXDPS infrastructure framework supports several industry standard products and platforms. Vendor shall identify the products required to properly support the contracted solution.
 - a. Vendor shall identify:
 - i. Required hardware platforms and operating system to support the proposed solution.
 - a) Processor requirements;
 - b) Memory requirements;
 - c) Operating system details and dependencies;
 - d) Data storage requirements; and
 - ii. Required application server platforms:
 - a) Processor requirements;
 - b) Memory requirements;
 - c) Operating system details and dependencies;
 - d) Data storage requirements; and
 - iii. Required web server platforms
 - a) Processor requirements;
 - b) Memory requirements;
 - c) Operating system details and dependencies;
 - d) Data storage requirements; and
 - iv. Required support services such as email servers, etc.
 - a) Processor requirements;
 - b) Memory requirements;
 - c) Operating system details and dependencies;
 - e) Data storage requirements; and
 - 3) TXDPS’ IT infrastructure only allows the following database platforms:
 - a) Vendor SQL Server 2008 R2; and
 - b) DB2 9.7.2 on Distributed (AIX and LINUX).
 - 4) TXDPS’ IT infrastructure report services are supported with Crystal Reports.

B. TXDPS Communication Standards

COTS software shall support integration with other TXDPS systems utilizing standard web services or provide API tools that can be incorporated into TXDPS' applications or secure file transfer protocol with data encryption.

C. Network Topography

- 1) TXDPS utilizes a combination of public and private TCP/IP network resources. All internal communications between client resources, other systems, and system services shall be through this network.
- 2) Vendor shall include in its Offer, an estimate on the amount of bandwidth or formulas to calculate usage required to support the number of expected users and volume of work.

D. Workstation installed software – If the software solution is client based and needs to be installed on each computer, Vendor shall provide the client software in an MSI format so the install can be packaged.