# SYSTEM AND SERVICES AGREEMENT BETWEEN BROWARD COUNTY AND TIBA PARKING SYSTEMS, LLC

This System and Services Agreement (the "Agreement") is made and entered into by and between Broward County, a political subdivision of the State of Florida ("County"), and TIBA Parking Systems, LLC, a Georgia limited liability corporation with headquarters in the State of Ohio, authorized to transact business in the State of Florida ("Provider") (collectively, Provider and County are referred to as the "Parties" and each a "Party").

## RECITALS

A. In 2018, Broward County conducted a solicitation for a Parking Access Revenue Control System (PARCS) Replacement for Port Everglades, Request for Proposals (RFP) No. PNC2117468P1. Provider was the first-ranked vendor for the referenced RFP.

B. Pursuant to this Agreement, Provider will provide County with all necessary equipment, software, and services, including ongoing support and maintenance, for a comprehensive PARCS solution to be implemented at Port Everglades.

Now, therefore, for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties hereto agree as follows:

## ARTICLE 1. DEFINITIONS

1.1 Board. The Board of County Commissioners of Broward County, Florida.

1.2 Business hours or business day. 7 a.m. to 7 p.m. Eastern Time during weekdays that are not County holidays and on which County has not otherwise declared its offices closed.

1.3 Contract Administrator. The Director of Port Everglades, or such person's designee as designated by same in writing.

1.4 Documentation. All manuals, user documentation, specifications, and other related materials pertaining to the System and other hardware and software that Provider customarily furnishes to purchasers of the System.

1.5 Equipment. The hardware and other property identified in Exhibit A being provided to County pursuant to this Agreement, including any embedded software and firmware incorporated therein or customarily provided by Provider to purchasers of the Equipment.

1.6 Purchasing Director. The Broward County Purchasing Director as appointed by the Broward County Administrator.

1.7 Services. All required installation, integration, programming, configuration, customization, and enhancements of the System, together with necessary and appropriate consulting, training, and project management services, to meet County's ongoing needs in connection with the System, as further specified in Exhibit A.

1.8 Software. All proprietary or third-party software or other intellectual property, including the Documentation for same, provided or licensed to County or third-party users pursuant to this Agreement, including the computer programs (in machine readable object code form) listed in Exhibit A and any subsequent updates, upgrades, releases, or enhancements thereto developed by Provider during the term of this Agreement.

1.9 Support and Maintenance Services. The maintenance and support required to maintain optimal performance of the System as described in the Documentation and Exhibit C, as well as the support and maintenance services required for County to achieve and maintain optimal performance of the System.

1.10 System. The Software, Equipment, and other property identified in Exhibit A being provided to County pursuant to this Agreement.

## ARTICLE 2. EXHIBITS

The following exhibits are attached hereto and incorporated into this Agreement:

| | |
|---|---|
| **Exhibit A** | **Statement of Work** |
| **Exhibit B** | **Payment Schedule** |
| **Exhibit C** | **Support and Maintenance Services** |
| **Exhibit D** | **Minimum Insurance Requirements** |
| **Exhibit E** | **Work Authorization Form** |
| **Exhibit F** | **CBE Subcontractor Schedule and Letters of Intent** |
| **Exhibit G** | **Port Everglades Security Requirements** |
| **Exhibit H** | **PCI Responsibility Matrix** |
| **Exhibit I** | **Security Requirements** |

If there is a conflict or inconsistency between any provision contained in Articles 1 - 14 and any provision contained in any of the Exhibits, the provision of Articles 1 - 14 shall prevail and be given effect unless expressly stated to the contrary.

## ARTICLE 3. SCOPE OF WORK & SOFTWARE LICENSE

3.1 Scope of Work. Provider shall complete all Services required in this Agreement inclusive of the Exhibits. Unless stated otherwise in this Agreement, the work required of Provider includes all labor, materials, and tasks, whether or not enumerated in the Agreement, that are such an inseparable part of the work expressly stated in the Agreement that exclusion thereof would render Provider's performance impractical, illogical, or unconscionable. Provider and the System must always comply with the requirements set forth in Exhibit I.

3.2 Support and Maintenance Services. For so long as requested by County, Provider shall provide Support and Maintenance Services to ensure the proper functioning and optimal performance of the System as set forth in the Documentation pursuant to the terms of Exhibit C. For the first year following Final Acceptance, all Support and Maintenance Services for the

Software and System are included at no additional cost. For subsequent years, Support and Maintenance Services shall be invoiced and paid in accordance with the Payment Schedule set forth in Exhibit B.

3.2.1 Updates, Upgrades, and Releases. During the Software warranty period, Provider shall promptly provide to County, with advance notice and at no additional cost, any and all updates (including error corrections, bug fixes, security updates, and patches), upgrades, or new releases to the Software (as well as any firmware included with the Equipment), including all that Provider has made available to other licensees of all or part of the Software licensed pursuant to this Agreement. All such updates, upgrades, and new releases shall remain the sole property of Provider and shall be deemed to be included within the scope of the license granted under this Agreement.

3.2.2 Compatibility. For the full term of this Agreement, Provider will use commercially reasonable efforts to ensure the continued compatibility of the Software and System with all major releases, updates, or upgrades of any third-party software used by County for access or operation of the System. In the event Provider is not be able to support any third-party software update, upgrade, or new release that is not backwards compatible with the Software or System, Provider shall use all reasonable efforts to resolve such issues and to provide optimal functionality of the Software and System in accordance with this Agreement. If Provider is unable to provide continued optimal functionality of the Software and System in accordance with this Agreement due to any third-party software release, update, or upgrade, County shall be entitled to terminate the Agreement upon written notice with no further obligation to Provider except for the payment of any undisputed fees owed to Provider through the date of termination.

3.2.3 Software Enhancements or Modifications. Upon mutual agreement of the Parties, Provider will incorporate certain features and enhancements into the licensed Software, County will be granted the same license rights to the features and enhancements granted by this Agreement, and the source code for those features and enhancements shall be the property of Provider. Any such agreement must be formalized into a Statement of Work that shall define in detail the services to be performed, the financial terms, and the proposed project staffing and schedule. Any such Statement of Work shall be incorporated into a Work Authorization, to the extent permitted by Section 3.4 below, or an amendment to this Agreement.

3.3 License. For the full term of the Agreement, inclusive of any renewals, Provider grants to County a perpetual, royalty-free, nonexclusive license to the Software and System, including to any software embedded in or provided with the Equipment, with no geographical limitations, for an unlimited number of users, as specified in Exhibit A. This license grant is for use solely for County governmental and business purposes, including on- and off-site access and use of the Software and System by third-party users (identified by County in writing in Exhibit A), including those persons or entities with which County may contract to operate the System or components thereof, and for the benefit of and use by all governmental entities within County, including the offices of the County constitutional officers.

Exhibit 2

3.3.1 Authorized Users and Additional Licenses. Unless otherwise stated in Exhibit A (Statement of Work), County and any of its employees, agents, suppliers of services, or other authorized third-party users shall have the right to concurrently operate and use the System for County governmental or business purpose. If anything less than unlimited, concurrent use is expressly provided under this Agreement and additional licenses may be required, County's Purchasing Director is authorized to execute a Work Authorization (Exhibit E).

3.3.2 Additional Uses. County may, if required by reason of an emergency, disaster, or operational need, or for testing of recovery resources, temporarily use the Software on recovery resources at no additional cost, including recovery resources that may not be owned by County. County may, at no additional cost, copy the Software for backup and archiving purposes for the purposes of support or maintenance by County or others hired by County to provide such support or maintenance. County may, at no additional cost, utilize a hosted environment, including without limitation through a third-party hosting provider, for all otherwise permitted uses of the Software.

3.3.3 Prohibited Uses. Except as otherwise provided in this Agreement or required under Florida law, County shall not reproduce, publish, or license the Software to others. County shall not modify, reverse engineer, disassemble, or decompile the Software or any portion thereof, except (a) to the extent expressly authorized in Exhibit A, in which event such authorized actions shall be deemed within the license grant of Section 3.3, or (b) to the extent permitted under any applicable open source license.

3.4 Change of Scope Procedures. Provider acknowledges that Contract Administrator has no authority to make changes that would increase, decrease, or otherwise modify the scope of work to be provided under this Agreement except as expressly provided herein. To the extent any goods or services under this Agreement, or the quantity thereof, are optional ("Optional Services"), County may select the type, amount, and timing of such goods or services pursuant to a Work Authorization (Exhibit E) executed by Provider and County pursuant to this section, and provided that no such selection, when combined with those goods or services required under the Agreement, would result in a payment obligation exceeding the applicable maximum amount stated in Section 5.1. Notwithstanding anything to the contrary in the Agreement, Work Authorizations for Optional Services pursuant to this section shall be executed on behalf of County as follows: the Contract Administrator may execute Work Authorizations for which the total cost to County in the aggregate is less than $50,000.00; the Purchasing Director may execute Work Authorizations for which the total cost to County in the aggregate is within the Purchasing Director's delegated authority; any Work Authorizations above the Purchasing Director's delegated authority shall require Board approval. Subsequent to the full execution of any Work Authorization, the Contract Administrator will issue a Notice to Proceed for those authorized Optional Services. Provider shall not commence work on any Work Authorization until after receipt of the applicable Notice to Proceed.

3.5 Contract Administrator Authority. The Contract Administrator is authorized to coordinate and communicate with Provider to manage and supervise the performance of this

Agreement. Unless expressly stated otherwise in this Agreement or otherwise set forth in an applicable provision of the Broward County Procurement Code, Broward County Code of Ordinances, or Broward County Administrative Code, the Contract Administrator may exercise any ministerial authority under this Agreement in connection with the day-to-day management of this Agreement. The Contract Administrator may approve in writing minor modifications to the scope of work provided that such modifications that do not increase the total cost to County or waive any rights of County.

## ARTICLE 4. TERM AND TIME OF PERFORMANCE

4.1 Term. The Agreement shall become effective on the date it is fully executed by the Parties (the "Effective Date"). The initial term of the Agreement shall be for a period of five (5) years from the date of Final Acceptance (the "Initial Term").

4.2 Extensions. County shall have the option to renew this Agreement for up to five (5) additional one (1) year terms by sending notice of renewal to Provider at least thirty (30) days prior to the expiration of the then-current term. The Purchasing Director is authorized to exercise this renewal option. In the event that unusual or exceptional circumstances, as determined in the sole discretion of the Purchasing Director, render the exercise of an extension not practicable or if no extension is available and expiration of this Agreement would result in a gap in the provision of services necessary for the ongoing operations of County, then this Agreement may be extended on the same terms and conditions by the Purchasing Director for period(s) not to exceed three (3) months in the aggregate.

4.3 Fiscal Year. The continuation of this Agreement beyond the end of any County fiscal year shall be subject to both the appropriation and the availability of funds, in accordance with Chapter 129, Florida Statutes.

4.4 Delivery. Provider shall deliver the Equipment and Documentation via inside delivery to County in accordance with Exhibit A at the address provided by County. Transportation cost and risk, and the cost of delivery (including lift gate services and depalletization), assembly and installation, including any applicable taxes and all actions necessary to integrate the Equipment into County's existing system, shall be the responsibility of Provider, except to the extent (if any) expressly provided in Exhibit A.

4.5 Timetable. If the System fails to achieve Final Acceptance by October 1, 2020, County shall have the option to terminate the Agreement by written notice from its Contract Administrator, in which event Provider shall, within fifteen (15) days, pick up the System at Provider's expense and reimburse all sums paid by County under this Agreement, if any, except for such sums paid for or to be paid for the Services provided within two (2) months after the Effective Date. For purposes of this paragraph, any delays caused by County prior to Final Acceptance shall extend the Final Acceptance deadline by the same number of days as the delay caused by County.

4.6 Time is of the essence for all performance required under this Agreement.

## ARTICLE 5. COMPENSATION

5.1 For the duration of the Agreement, County will pay Provider in accordance with Exhibit B up to the following maximum amount(s):

| Services/Goods | Term | Not-To-Exceed Amount |
|---|---|---|
| Equipment, Software, System, and Services per Exhibit A | Initial Term | $1,836,120.00 |
| Support and Maintenance Services per Exhibit C | Initial Term | $433,935.00 |
| Optional renewal terms for Support and Maintenance Services per Exhibit C | Total for all renewal terms | $650,000.00 |
| Optional Services | Duration of the Agreement (inclusive of any renewals) | $600,000.00 |
| **TOTAL NOT TO EXCEED** | | $3,520,055.00 |

Payment shall be made only for work actually performed and completed pursuant to this Agreement or as otherwise set forth in Exhibit B (Payment Schedule), which amount shall be accepted by Provider as full compensation for all such work. Provider acknowledges that the amounts set forth herein are the maximum amounts payable for the respective terms and constitute a limitation upon County's obligation to compensate Provider for its work under this Agreement. These maximum amounts, however, do not constitute a limitation of any sort upon Provider's obligation to perform all items of work required under this Agreement. Unless otherwise expressly stated in this Agreement, Provider shall not be reimbursed for any expenses it incurs under this Agreement.

5.2 Method of Billing and Payment

5.2.1 Invoices. Provider may submit invoices only for goods provided and services completed in accordance with the Payment Schedule set forth in Exhibit B. Unless otherwise indicated in Exhibit B, an original plus one copy of each invoice must be submitted within fifteen (15) days after the end of the month for which payment is sought, except that the final invoice must be submitted no later than sixty (60) days after all services are completed. Provider shall submit with each invoice a Certification of Payments to Subcontractors and Suppliers on the form provided by County, as may be modified in County's reasonable discretion. If applicable, the certification shall be accompanied by a copy of the notification sent to each subcontractor and supplier listed in item 2 of the certification form, explaining the good cause why payment has not been made. Unless otherwise stated in Exhibit B or the applicable Work Authorization, any Optional Services shall be invoiced in accordance with the existing invoicing schedule for any like goods or services provided under this Agreement, including (if applicable) invoiced pro rata for the initial invoice period.

Exhibit 2

5.2.2 Payments. County shall pay Provider within thirty (30) days of receipt of Provider's proper invoice, as required by the "Broward County Prompt Payment Ordinance" (Broward County Ordinance No. 89-49). Payment shall be made to Provider at the most recent address designated under the "Notices" provision of this Agreement. To be deemed proper, an invoice must comply with all requirements set forth in this Agreement and must be submitted pursuant to any instructions prescribed by the Contract Administrator. County shall have the right to withhold payment of the invoice based on Provider's failure to comply with any term, condition, or requirement of this Agreement. The Parties hereto agree that any amounts so withheld shall not be subject to payment of any interest by County.

5.2.3 Unless a shorter period is required under applicable law or under the applicable contract, Provider shall pay its Certified Business Entity ("CBE") subcontractors and suppliers within fifteen (15) days following receipt of payment from County and shall pay all other subcontractors and suppliers within thirty (30) days following receipt of payment from County.

5.3 Travel. With respect to travel costs and travel-related expenses, Provider agrees to adhere to Section 112.061, Florida Statutes, except to the extent, if any, that Exhibit B expressly provides to the contrary. County shall not be liable for any such expenses that have not been approved in advance, in writing, by County.

5.4 Fixed Pricing. Except for Milestone 4, prices set forth in Exhibit B shall remain firm and fixed for the term of the Agreement, including any optional terms. However, Provider may offer incentive or volume discounts to County at any time.

## ARTICLE 6. WARRANTIES

6.1 Ownership and License Rights. Provider represents and warrants that it is the owner of all right, title, and interest in and to the Equipment and other property being sold to County under this Agreement, that it has the right to sell such Equipment and other property to County, and that such sale is free and clear of any lien or interest of any other person or entity. Provider further represents and warrants that it has the right to grant to County the rights and the licenses granted under this Agreement as to the Software and System. Provider warrants that it has not knowingly granted rights or licenses to any other person or entity that would restrict rights and licenses granted hereunder, except as may be expressly stated herein.

6.2 System Warranty. For one (1) year following the date of Final Acceptance (as defined in Exhibit A), Provider represents and warrants to County that the System will perform substantially as described in the Documentation and in the Statement of Work (Exhibit A). This warranty does not cover any failure of the System resulting from (a) use of the System in a manner other than that for which it was intended; (b) any modification of the System by County that is not intended or authorized by Provider; or (c) County's provision of improperly formatted data to be processed through the System.

6.3 Software Warranty. For the duration of the Agreement, inclusive of all renewal terms, Provider represents and warrants to County that the Software will perform substantially as described in the Documentation and in the Statement of Work (Exhibit A). This warranty does not cover any failure of the Software resulting from (a) use of the Software in a manner other than that for which it was intended; (b) any modification of the Software by County that is not intended or authorized by Provider; or (c) County's provision of improperly formatted data to be processed through the Software.

6.4 Equipment Warranty. Provider represents and warrants to County that for a period of one (1) year after the date of Final Acceptance, the Equipment will perform substantially as described in the Documentation and the Statement of Work (Exhibit A), will be free from defects in workmanship and material, and will have all of the qualities and features and be capable of performing all of the functions described in the Documentation and Statement of Work. This warranty shall not cover any failure of the Equipment resulting from (a) use of the Equipment in a manner other than that for which it was intended; or (b) modification of the Equipment by County not authorized by Provider.

6.5 Warranty Regarding Viruses and PCI Compliance. Provider further represents, warrants, and agrees that the System and any software or firmware provided under this Agreement are free from currently-known viruses or malicious software (at the time the System and any subsequent version thereof is provided to County), and that Provider has and will continue, for the full term of this Agreement, to use commercially reasonable security measures to ensure the integrity of such software and firmware from data leaks, hackers, denial of service attacks, and other unauthorized intrusions. If the System will accept, transmit, or store any credit cardholder data, Provider represents and warrants that the System complies with the most recent of the Security Standards Council's Payment Card Industry ("PCI") Payment Application Data Security Standard. The Parties agree to adhere to the PCI Responsibility Matrix set forth in Exhibit H.

6.6 Intellectual Property Warranty. Provider represents and warrants that at the time of entering into this Agreement, no claims have been asserted against Provider (whether or not any action or proceeding has been brought) that allege that any part of the System or other property provided to County under this Agreement infringes or misappropriates any patent, copyright, mask copyright, or any trade secret or other intellectual or proprietary right of a third party, and that Provider is unaware of any such potential claim. Provider also agrees, represents, and warrants that the System (or any portion thereof) and services to be provided pursuant to this Agreement will not infringe or misappropriate any patent, copyright, mask copyright, or any trade secret or other intellectual or proprietary right of a third party.

6.7 Quality of Performance and Materials. Provider represents and warrants that all services provided under this Agreement will be performed by a person duly qualified and sufficiently experienced to perform such services and, where required, licensed by all appropriate governmental authorities in the applicable area(s). Provider agrees that all services under this Agreement shall be performed in a skillful and respectful manner, and that the quality of all such services shall meet or exceed prevailing industry and professional standards for such services.

Exhibit 2

Provider represents and warrants that all materials, Equipment, and products furnished pursuant to this Agreement shall be of good quality and free from defective or inferior workmanship; any items found not to be in conformance with the foregoing and with the Documentation or applicable specifications (if any) in Exhibit A shall be replaced by Provider at no additional cost to County. If requested by County's Contract Administrator, Provider shall develop and utilize a quality assurance plan approved by County to ensure the appropriate quality of the work and materials provided under this Agreement.

6.8 Remedy for Breach of Warranty. In the event of written notice from County of a breach of warranty during the applicable warranty period, Provider shall, at no charge to County, promptly correct the warranty breach including, when required, by (a) correcting or updating the Software, (b) correcting or replacing the affected Equipment, or (c) providing to County other measures that correct the breach. In addition, upon notice from County of any warranty breach or other error or defect in the System, Provider will immediately provide to County any known reasonable methods of operating the System in a manner that eliminates the adverse effects of the error or defect. If Provider is unable to correct a material breach of this article during the applicable warranty period and within a reasonable period of time not to exceed ten (10) business days, County shall be entitled to cancel the Agreement and receive a full refund of all amounts paid to Provider, Provider shall arrange for the return of the Equipment at Provider's expense, and neither Party shall have any further obligation under the Agreement except as to any provision that expressly survives the Agreement's termination or expiration. In the event of replacement of any of the Software or Equipment, the Software or Equipment as replaced will be warranted as provided above from the date of installation. The remedies in this section are in addition to any other rights and remedies County may have under this Agreement or applicable law.

## ARTICLE 7. DELIVERY, TESTING AND ACCEPTANCE

7.1 Software. Unless otherwise stated in Exhibit A, within a mutually agreed upon time period based on the approved installation and deployment schedule, Provider shall make the Software available to County and deliver to County a master copy of the Software licensed hereunder in object code form, suitable for reproduction in accordance with this Agreement, in electronic files unless otherwise requested by County. All County license keys, usernames, and passwords shall be authenticated by Provider and perform according to Exhibit A (Statement of Work).

7.2 Documentation. Provider shall deliver copies of the Documentation to County concurrently with delivery of the applicable Equipment and Software, and thereafter shall promptly provide any updated Documentation as it becomes available during the term of this Agreement. Provider represents and warrants that the Documentation is sufficiently comprehensive and of sufficient quality to enable a competent user to operate the applicable portions of the System efficiently and in accordance with Exhibit A. County has the right to copy and modify the Documentation as it deems necessary for its own internal use.

7.3 Final Acceptance Testing. Broward County Administrative Code Section 22.148 requires that all applicable software purchases be inspected and tested by County, including verification by its Enterprise Technology Services ("ETS"), prior to final written acceptance of the software and software-related services. Within thirty (30) days following completion of installation and integration of the System, County shall test the System to determine whether the System: (i) properly functions with any applicable operating software; (ii) provides the capabilities stated in this Agreement and the Documentation; and (iii) if applicable, meets the acceptance criteria stated in the Statement of Work (the criteria referenced in (i), (ii), and (iii) are collectively referred to as the "Final Acceptance Criteria"). In the event of a conflict between the Documentation and the acceptance criteria stated in the Statement of Work, the Statement of Work shall prevail. Final payment shall not be made to Provider prior to the written confirmation by County's Chief Information Officer or his or her designee that the System has successfully passed the Final Acceptance Criteria, and such written confirmation shall constitute "Final Acceptance."

7.3.1 The testing period shall commence on the first business day after Provider informs County in writing that it has completed the Services required to be performed prior to testing and that the System is ready for testing, and shall continue for a period of up to thirty (30) days.

7.3.2 During the testing period, County may notify Provider in writing of any error or defect in the System so that Provider may make any needed modifications or repairs. If Provider so elects in writing, testing will cease until Provider resubmits for Final Acceptance testing, at which time the testing period shall be reset to that of a first submission for testing.

7.3.3 County shall notify Provider in writing of its Final Acceptance or rejection of the System, or any part thereof, within fifteen (15) days after the end of the testing period, as same may be extended or reset. If County rejects the System, or any part thereof, County shall provide notice identifying the criteria for Final Acceptance that the System failed to meet. Following such notice, Provider shall have thirty (30) days to (a) modify, repair, or replace the System or any portion thereof, or (b) otherwise respond to County's notice. If Provider modifies, repairs, or replaces the System or portion thereof, the testing period shall re-commence consistent with the procedures set forth above in this Section 7.3.

7.3.4 In the event Provider fails to remedy the reason(s) for County's rejection of the System, or any part thereof, within ninety (90) days after County's initial notice of rejection, County may elect, in writing, to either accept the System as it then exists or to reject the System and terminate the Agreement or applicable Work Authorization. If County elects to reject the System and terminate the Agreement or applicable Work Authorization, all sums paid by County under the Agreement or applicable Work Authorization shall be reimbursed to County by Provider within 15 days after such election is made. If County elects to accept the System as it then exists (partial acceptance), Provider shall continue to use its best efforts to remedy the items identified in the applicable notice of rejection. If, despite such continuing best efforts, Provider fails to remedy the issue(s) identified by County within a reasonable time as determined by County, then County shall be entitled to deduct from future sums due under the Agreement the value of the rejected portion of the System as mutually determined by the Parties. If the Parties cannot agree upon such value, County shall have the right to reject the System and terminate the Agreement or applicable Work Authorization on the terms stated above in this paragraph.

## ARTICLE 8. PROTECTION OF SOFTWARE AND PROPRIETARY RIGHTS

8.1 County Proprietary Rights. Provider acknowledges and agrees that County retains all rights, title and interest in and to all materials, data, documentation and copies thereof furnished by County to Provider under this Agreement, including all copyright and other proprietary rights therein, which Provider as well as its employees, agents, subconsultants, and suppliers may use only in connection with the performance of Services or Support and Maintenance Services under this Agreement. All rights, title, and interest in and to certain ideas, designs and methods, specifications, and other documentation related thereto developed by Provider and its subconsultants specifically for County (collectively, "Developed Works") shall be and remain the property of Provider. Accordingly, neither County nor its employees, agents, subconsultants, or suppliers shall have any proprietary interest in such Developed Works. The Developed Works may not be utilized, reproduced, or distributed by or on behalf of County, or any employee, agent, subconsultants, or supplier thereof, without the prior written consent of Provider, except as required for Provider's performance hereunder. Provider shall grant to County a nonexclusive perpetual license to use such Developed Works per the terms set forth in this Agreement.

8.2 Ownership. Except for custom work products, if any, County acknowledges that all copies of the Software (in any form) provided by Provider are the sole property of Provider. County shall not have any right, title, or interest to any such Software or copies thereof except as expressly provided in this Agreement, and shall take all reasonable steps to secure and protect all Software consistent with maintenance of Provider's proprietary rights therein.

8.3 Product Technology. Notwithstanding anything stated in this Agreement, County does not acquire any property or proprietary rights in software, technical data, know-how, concepts, processes, algorithms, code, users manuals, documentation, or applications incorporated, embedded, included or otherwise provided in or with the System including any inventions, discoveries and improvements related thereto (referred to herein as "Product Technology"), other than the right to use the Product Technology for its intended use with the System and the perpetual license to the Developed Works as stated in Section 8.1. Provider remains the exclusive owner of any intellectual or industrial property rights relating to the Product Technology and any and all trademarks represented by the Provider's company name, logos, and product names. The Product Technology is protected by patent, copyright, and trade secret laws. Except as provided in Section 7.2 or otherwise permitted under this Agreement, County shall not copy or duplicate, remanufacture, translate, reverse engineer, decompile, or disassemble, nor shall County permit any other person, including customers or end users, to copy or duplicate, remanufacture, translate, reverse engineer, decompile, or disassemble, all or any part of the System or other Product Technology, in any manner.

## ARTICLE 9. CONFIDENTIAL INFORMATION, SECURITY AND ACCESS

9.1 Public Records Law. As a political subdivision of the State of Florida, County is subject to Florida's Public Records Law, Chapter 119 of the Florida Statutes. Notwithstanding anything else in this Agreement, any action taken by County in compliance with, or in a good faith attempt to comply with, the requirements of Chapter 119 shall not constitute a breach of this Agreement.

9.2 Provider Confidential Information. Provider represents that the Software contains proprietary products and trade secrets of Provider. Accordingly, to the full extent permissible under applicable law, County agrees to treat the Software as confidential in accordance with this article. Any other material submitted to County that Provider contends constitutes or contains trade secrets or is otherwise exempt from production under Florida public records laws (including Florida Statutes Chapter 119) ("Trade Secret Materials") must be separately submitted and conspicuously labeled "EXEMPT FROM PUBLIC RECORD PRODUCTION – TRADE SECRET." In addition, Provider must, simultaneous with the submission of any Trade Secret Materials, provide a sworn affidavit from a person with personal knowledge attesting that the Trade Secret Materials constitute trade secrets under Florida Statutes Section 812.081 and stating the factual basis for same. In the event that a third party submits a request to County for records designated by Provider as Trade Secret Materials, County shall refrain from disclosing the Trade Secret Materials, unless otherwise ordered by a court of competent jurisdiction or authorized in writing by Provider. Provider shall indemnify and defend County and its employees and agents from any and all claims, causes of action, losses, fines, penalties, damages, judgments and liabilities of any kind, including attorneys' fees, litigation expenses, and court costs, relating to the nondisclosure of the Software or any Trade Secret Materials in response to a records request by a third party.

9.3 County Confidential Information.

9.3.1 All Developed Works, materials, data, transactions of all forms, financial information, documentation, inventions, designs, and methods that Provider obtains from County in connection with this Agreement, that are made or developed by Provider in the course of the performance of the Agreement, or in which County holds proprietary rights, constitute "County Confidential Information."

9.3.2 All County-provided employee information, financial information, and personally identifiable information for individuals or entities interacting with County (including, without limitation, social security numbers, birth dates, banking and financial information, and other information deemed exempt or confidential under state or federal law) also constitute County Confidential Information.

9.3.3 County Confidential Information may not, without the prior written consent of County, or as otherwise required by law, be used by Provider or its employees, agents, subconsultants or suppliers for any purpose other than for the benefit of County pursuant to this Agreement. Neither Provider nor its employees, agents, subconsultants or suppliers may sell,

Exhibit 2

transfer, publish, disclose, display, license, or otherwise make available to any other person or entity any County Confidential Information without the prior written consent of County.

9.3.4 Provider expressly agrees to be bound by and to defend, indemnify and hold harmless County and its officers and employees from the breach of any federal, state or local law by Provider or its employees, agents, subconsultants, or suppliers regarding the unlawful use or disclosure of County Confidential Information.

9.3.5 Upon expiration or termination of this Agreement, or as otherwise demanded by County, Provider shall immediately turn over to County all County Confidential Information, in any form, tangible or intangible, possessed by Provider or its employees, agents, subconsultants, or suppliers.

9.4 Maintenance of Confidential Information. Each Party shall advise its employees, agents, subconsultants, and suppliers who receive or otherwise have access to the other Party's Confidential Information of their obligation to keep such information confidential, and shall promptly advise the other party in writing if it learns of any unauthorized use or disclosure of the other Party's Confidential Information. In addition, the Parties agree to cooperate fully and provide reasonable assistance to ensure the confidentiality of the other party's Confidential Information.

9.5 Security and Access. Any access by Provider to any aspect of County's network must comply at all times with all applicable County access and security standards, as well as any other or additional restrictions or standards for which County provides written notice to Provider. Provider will provide any and all information that County may reasonably request in order to determine appropriate security and network access restrictions and verify Provider's compliance with County security standards. If at any point in time County, in the sole discretion of its Chief Information Officer, determines that Provider's access to any aspect of County's network presents an unacceptable security risk, County may immediately suspend or terminate Provider's access and, if the risk is not promptly resolved to the reasonable satisfaction of County's Chief Information Officer, may terminate this Agreement or any applicable Work Authorization upon ten (10) business days' notice (including, without limitation, without restoring any access to County's network to Provider).

9.6 Data and Privacy. Provider shall comply with all applicable data and privacy laws and regulations, including without limitation the Florida Information Protection Act of 2014, Florida Statutes Section 501.171, and shall ensure that County data transmitted or stored in the System is not transmitted or stored outside the continental United States. Provider may not sell, market, publicize, distribute, or otherwise make available to any third party any personal identification information (as defined by Florida Statutes Section 817.568 or Section 817.5685) that Provider may receive or otherwise have access to in connection with this Agreement, unless expressly authorized in advance by County. If and to the extent requested by County, Provider shall ensure that all hard drives or other storage devices and media that contained County data have been wiped in accordance with the then-current best industry practices, including without limitation

Exhibit 2

DOD 5220.22-M, and that an appropriate data wipe certification is provided to the satisfaction of the Contract Administrator.

9.7 Injunctive Relief. The Parties represent and agree that neither damages nor any other legal remedy is adequate to remedy any breach of this article, and that the injured party shall therefore be entitled to injunctive relief to restrain or remedy any breach or threatened breach.

9.8 Survival. The obligations under this Article 9 shall survive the termination of this Agreement or of any license granted under this Agreement.

## ARTICLE 10. INDEMNIFICATION AND LIMITATION OF LIABILITY

10.1 Indemnification. Provider shall be fully liable for the actions of its current, former, and future officers, employees, subcontractors, and other agents under this Agreement. Provider shall at all times hereafter indemnify, hold harmless and defend County and all of County's current and former officers, employees, and other agents (collectively, "Indemnified Party") from and against any and all lawsuits, causes of action, demands, claims, losses, fines, penalties, damages, judgments, liabilities, and expenditures of any kind, including attorneys' fees, litigation expenses, and court costs (collectively, "Claim"), raised or asserted by any person or entity that is not a party to this Agreement, which Claim is caused or alleged to be caused, in whole or in part, by any intentional, reckless, or negligent act or omission of Provider or any current or former officer, employee, subcontractor, or other agent of Provider, arising from, relating to, or in connection with any obligation or performance under this Agreement. In the event any Claim is brought against an Indemnified Party, Provider shall, upon written notice from County, defend each Indemnified Party against each such Claim through counsel satisfactory to County. The provisions and obligations of this section shall survive the expiration or earlier termination of this Agreement. The right to be indemnified shall be conditioned upon County: (i) promptly notifying Provider of the Claim; (ii) granting Provider exclusive control over the defense and/or settlement of the Claim, provided Provider does not reach a settlement on any Claim that would impose any liability and/or monetary obligation on County or infringe on County's rights without County's written consent, and reasonably assisting Provider in such defense; and (iii) making no compromise or settlement of any such Claim without the prior written approval of the Provider. To the extent considered necessary by the County Attorney, in his or her reasonable discretion, any sums due Provider under this Agreement may be retained by County until all Claims subject to this indemnification obligation have been resolved. Any sums so withheld shall not be subject to the payment of interest by County.

10.2 Limitation of Liability. Neither Provider nor County shall be liable to the other Party for any damages under this Agreement that exceed the largest of the following amounts: (a) $100,000; (b) twice the maximum compensation amount specified in Section 5.1; or (c) the amount of $1,900,000 Dollars insurance Provider is required to provide under Article 11. Neither Party shall be liable for the other Party's special, indirect, punitive, or consequential damages (including damages resulting from lost data or records other than costs incurred in the recovery thereof), even if the Party has been advised that such damages are possible, or for the other party's lost profits, lost revenue, or lost institutional operating savings. These limitations of liability shall not apply to (i) any Claim resulting from a Party's actual or alleged disclosure of the other Party's Confidential Information or resulting from an actual or alleged data breach in violation of applicable law, (ii) any Claim resulting from an actual or alleged infringement of any interest in any intellectual property, or (iii) any indemnification obligation under this Agreement.

10.3 Infringement Remedy. If any Equipment, Software, or portion of the System is finally adjudged to infringe, or in Provider's opinion is likely to become the subject of such a Claim, Provider shall, at Provider's option, either: (i) procure for County the right to continue using the applicable portion of the System; (ii) modify or replace the System (in part or in whole) to make it noninfringing; or (iii) if neither of the above sections (i) and (ii) is commercially feasible, Provider shall have the right to terminate this Agreement and refund to County all fees paid under this Agreement. Provider shall have no liability regarding any infringement claim caused by any County modification of the System not authorized by Provider.

10.4 Third-Party Pass Thru Rights. Provider shall extend to County all rights and benefits Provider has from any third party as to the Equipment or Software relating to warranty or third-party claims, including any and all indemnification and hold harmless rights, to the extent permitted under any applicable agreement with the third-party equipment or software supplier or otherwise available to Provider. Provider shall at all times use all reasonable efforts to cooperate with County in the event of an infringement claim involving System.

## ARTICLE 11. INSURANCE

11.1 For purposes of this article, the term "County" shall include Broward County and its members, officials, officers, and employees.

11.2 Provider shall maintain, at its sole expense and at all times during the term of this Agreement (unless a different time period is otherwise stated herein), at least the minimum limits of insurance coverage designated in Exhibit D (inclusive of any amount provided by an umbrella or excess policy) in accordance with the terms and conditions stated in this article. All required insurance shall apply on a primary basis, and shall not require contribution from, any other insurance or self-insurance maintained by County. Any insurance, or self-insurance, maintained by County shall be in excess of, and shall not contribute with, the insurance provided by Provider.

11.3 Insurers providing the insurance required by this Agreement must either be: (1) authorized by a current certificate of authority issued by the State of Florida to transact insurance in the State of Florida, or (2) except with respect to coverage for the liability imposed by the Florida Workers' Compensation Act, an eligible surplus lines insurer under Florida law. In addition, each such insurer shall have and maintain throughout the period for which coverage is required, a minimum A. M. Best Company Rating of "A-" and a minimum Financial Size Category of "VII." To the extent insurance requirements are designated in Exhibit D, the applicable policies shall comply with the following:

Exhibit 2

11.3.1 Commercial General Liability Insurance. Policy shall be no more restrictive than that provided by the latest edition of the standard Commercial General Liability Form (Form CG 00 01) as filed for use in the State of Florida by the Insurance Services Office (ISO), with the exception of endorsements specifically required by ISO or the State of Florida, and liability arising out of:

Mold, fungus, or bacteria
Terrorism
Silica, asbestos or lead
Sexual molestation
Architects and engineers professional liability, unless coverage for professional liability is specifically required by this Agreement.

County shall be included on the policy (and any excess or umbrella policy) as an "Additional Insured" on a form no more restrictive than ISO form CG 20 10 (Additional Insured – Owners, Lessees, or Contractor). The policy (and any excess or umbrella policy) must be endorsed to waive the insurer's right to subrogate against County.

11.3.2 Business Automobile Liability Insurance. Policy shall be no more restrictive than that provided by Section II (Liability Coverage) of the most recent version of the standard Business Auto Policy (ISO Form CA 00 01) without any restrictive endorsements, including coverage for liability contractually assumed, and shall cover all owned, non-owned, and hired autos used in connection with the performance of work under this Agreement. County shall be included on the policy (and any excess or umbrella policy) as an "Additional Insured." The policy (and any excess or umbrella policy) must be endorsed to waive the insurer's right to subrogate against County.

11.3.3 Workers' Compensation/Employer's Liability Insurance. Such insurance shall be no more restrictive than that provided by the latest edition of the standard Workers' Compensation Policy, as filed for use in Florida by the National Council on Compensation Insurance (NCCI), with the exception of endorsements required by NCCI or the State of Florida. The policy must be endorsed to waive the insurer's right to subrogate against County in the manner which would result from the attachment of the NCCI form "Waiver of our Right to Recover from Others Endorsement" (Advisory Form WC 00 03 13) with County scheduled thereon. Where appropriate, coverage shall be included for any applicable Federal or State employer's liability laws including, but not limited to, the Federal Employer's Liability Act, the Jones Act, and the Longshoreman and Harbor Workers' Compensation Act.

11.3.4 Professional Liability Insurance. Such insurance shall cover Provider for those sources of liability arising out of the rendering or failure to render professional services in the performance of the services required in this Agreement. If policy provides coverage on a claims-made basis, such coverage must respond to all claims reported within at least three (3) years following the period for which coverage is required, unless a longer period is indicated in Exhibit D.

11.3.5 Cyber Liability, or Technology Errors and Omissions Insurance. Coverage is required for any system connected to, and, or accessible from the internet. Coverage may be included as part of the required Professional Liability Insurance. If policy provides coverage on a claims-made basis, such coverage must respond to all claims reported within at least three (3) years following the period for which coverage is required, unless a longer period is indicated in Exhibit D. Such policy shall cover, at a minimum, the following:

Data Loss and System Damage Liability
Security Liability
Privacy Liability
Privacy/Security Breach Response coverage, including Notification Expenses

County shall be included on the policy as an "Additional Insured" unless such endorsement is not available by the insurer.

11.4 Within fifteen (15) days after the Effective Date of this Agreement or notification of award, whichever is earlier, Provider shall provide to County satisfactory evidence of the insurance required in this Agreement. With respect to the Workers' Compensation/Employer's Liability Insurance, Professional Liability, and Business Automobile Liability Insurance, an appropriate Certificate of Insurance identifying the project and signed by an authorized representative of the insurer shall be satisfactory evidence of insurance. With respect to the Commercial General Liability, an appropriate Certificate of Insurance identifying the project, signed by an authorized representative of the insurer, and copies of the actual additional insured endorsements as issued on the policy(ies) shall be satisfactory evidence of such insurance.

11.5 Coverage is not to cease and is to remain in force until County determines all performance required of Provider is completed. If any of the insurance coverage will expire prior to the completion of the Services, proof of insurance renewal shall be provided to County prior to the policy's expiration.

11.6 Provider shall provide County thirty (30) days' advance notice of any cancellation of the policy except in cases of cancellation for non-payment for which County shall be given ten (10) days' advance notice.

11.7 Provider shall provide, within thirty (30) days after receipt of a written request from County, a copy of the policies providing the coverage required by this Agreement. Provider may redact portions of the policies that are not relevant to the insurance required by this Agreement.

11.8 County and Provider, each for itself and on behalf of its insurers, to the fullest extent permitted by law without voiding the insurance required hereunder, waive all rights against the other Party and any of the other Party's contractors, subcontractors, agents, and employees for damages or loss to the extent covered and paid for by any insurance maintained by the other Party.

11.9 If Provider uses a subcontractor, Provider shall require each subcontractor to endorse County as an "Additional Insured" on the subcontractor's Commercial General Liability policy.

## ARTICLE 12. EQUAL EMPLOYMENT OPPORTUNITY AND CBE COMPLIANCE

12.1 No Party may discriminate on the basis of race, color, sex, religion, national origin, disability, age, marital status, political affiliation, sexual orientation, pregnancy, or gender identity and expression in the performance of this Agreement. Provider shall include the foregoing or similar language in its contracts with any Subcontractors, except that any project assisted by the U.S. Department of Transportation funds shall comply with the nondiscrimination requirements in 49 C.F.R. Parts 23 and 26.

12.2 Provider shall comply with all applicable requirements of Section 1-81, Broward County Code of Ordinances, in the award and administration of this Agreement. Failure by Provider to carry out any of the requirements of this article shall constitute a material breach of this Agreement, which shall permit County to terminate this Agreement or exercise any other remedy provided under this Agreement, the Broward County Code of Ordinances, the Broward County Administrative Code, or under other applicable law, all such remedies being cumulative.

12.3 Provider will meet the required CBE goal by utilizing the CBE firms listed in Exhibit F (or a CBE firm substituted for a listed firm, if permitted) for twenty-one percent (21%) of total Services under this Agreement (the "Commitment").

12.4 In performing the Services, Provider shall utilize the CBE firms listed in Exhibit F for the scope of work and the percentage of work amounts identified on each Letter of Intent. Promptly upon execution of this Agreement by County, Provider shall enter into formal contracts with the CBE firms listed in Exhibit F and, upon request, shall provide copies of the contracts to the Contract Administrator and OESBD.

12.5 Each CBE firm utilized by Provider to meet the CBE goal must be certified by OESBD. Provider shall inform County immediately when a CBE firm is not able to perform or if Provider believes the CBE firm should be replaced for any other reason, so that OESBD may review and verify the good faith efforts of Provider to substitute the CBE firm with another CBE firm. Whenever a CBE firm is terminated for any reason, Provider shall provide written notice to OESBD and, upon written approval of the Director of OESBD, shall substitute another CBE firm in order to meet the CBE goal, unless otherwise provided in this Agreement or agreed in writing by the Parties. Such substitution shall not be required in the event the termination results from modification of the scope of work and no CBE firm is available to perform the modified scope of work; in which event, Provider shall notify County, and OESBD may adjust the CBE goal by written notice to Provider. Provider shall not terminate a CBE firm for convenience without County's prior written consent, which consent shall not be unreasonably withheld.

12.6 The Parties stipulate that if Provider fails to meet the Commitment, the damages to County arising from such failure are not readily ascertainable at the time of contracting. If Provider fails to meet the Commitment and County determines, in the sole discretion of the OESBD Program Director, that Provider failed to make Good Faith Efforts (as defined in Section 1-81, Broward County Code of Ordinances) to meet the Commitment, Provider shall pay County liquidated damages in an amount equal to fifty percent (50%) of the actual dollar amount by which Provider failed to achieve the Commitment, up to a maximum amount of ten percent (10%) of the total contract amount excluding costs and reimbursable expenses. An example of this calculation is stated in Section 1-81.7, Broward County Code of Ordinances. As elected by County, such liquidated damages amount shall be either credited against any amounts due from County, or must be paid to County within thirty (30) days after written demand. These liquidated damages shall be County's sole contractual remedy for Provider's breach of the Commitment, but shall not affect the availability of administrative remedies under Section 1-81. Any failure to meet the Commitment attributable solely to force majeure, changes to the scope of work by County, or inability to substitute a CBE Subcontractor where the OESBD Program Director has determined that such inability is due to no fault of Contractor, shall not be deemed a failure by Provider to meet the Commitment.

12.7 Provider acknowledges that the Board, acting through OESBD, may make minor administrative modifications to Section 1-81, Broward County Code of Ordinances, which shall become applicable to this Agreement if the administrative modifications are not unreasonable. Written notice of any such modification shall be provided to Provider and shall include a deadline for Provider to notify County in writing if Provider concludes that the modification exceeds the authority under this section. Failure of Provider to timely notify County of its conclusion that the modification exceeds such authority shall be deemed acceptance of the modification by Provider.

12.8 County may modify the required participation of CBE firms under this Agreement in connection with any amendment, extension, modification, change order, or Work Authorization to this Agreement that, by itself or aggregated with previous amendments, extensions, modifications, change orders, or Work Authorizations, increases the initial Agreement price by ten percent (10%) or more. Provider shall make a good faith effort to include CBE firms in work resulting from any such amendment, extension, modification, change order, or Work Authorization, and shall report such efforts, along with evidence thereof, to OESBD.

12.9 Provider shall provide written monthly reports to the Contract Administrator attesting to Provider's compliance with the CBE goal stated in this article. In addition, Provider shall allow County to engage in onsite reviews to monitor Provider's progress in achieving and maintaining Provider's contractual and CBE obligations. The Contract Administrator in conjunction with OESBD shall perform such review and monitoring, unless otherwise determined by the County Administrator.

12.10 The Contract Administrator may increase allowable retainage or withhold progress payments if Provider fails to demonstrate timely payments of sums due to all Subcontractors and suppliers. The presence of a "pay when paid" provision in a Provider's contract with a CBE firm shall not preclude County or its representatives from inquiring into allegations of nonpayment.

Exhibit 2

## ARTICLE 13. TERMINATION

13.1 This Agreement may be terminated for cause based on any breach that is not cured within ten (10) days after written notice from the aggrieved Party identifying the breach. This Agreement may also be terminated for convenience by the Board upon providing written notice to Provider of the termination date, which shall be not less than thirty (30) days after the date such written notice is provided. If County erroneously, improperly, or unjustifiably terminates for cause, such termination shall, to the full extent permissible under applicable law, be deemed a termination for convenience, which shall be effective thirty (30) days after such notice of termination for cause is provided.

13.2 County may terminate this Agreement if Provider is found to have submitted a false certification pursuant to Section 287.135, Florida Statutes, if Provider has been placed on the Scrutinized Companies with Activities in Sudan List or the Scrutinized Companies with Activities in the Iran Petroleum Energy Sector List, or if Provider has failed to promptly implement corrective action for audit deficiencies upon reasonable notice by County. Notwithstanding anything contained in this Agreement to the contrary, the rights and obligations of the Parties under this paragraph shall be governed by Section 287.135, Florida Statutes, to the full extent applicable.

13.3 Provider represents that neither it nor any of its affiliates has been placed on the discriminatory vendor list, as defined by Section 287.134, Florida Statutes. County may terminate this Agreement effective immediately, without any further obligation to Provider, upon learning that such representation is false or if Provider or any of its affiliates is placed on the discriminatory vendor list.

13.4 Additionally, and notwithstanding anything to the contrary in this Agreement, County may terminate this Agreement without any further liability to Provider upon the decertification of Provider as a Certified Business Entity ("CBE") by County's Office of Economic and Small Business Development ("OESBD"), if Provider's status as a CBE was a factor in the award of the Agreement and such status was misrepresented by Provider. However, such termination shall not be effective until expiration of any timely-filed review or appeal of the decertification decision.

13.5 Notice of termination shall be provided in accordance with the "Notices" section of this Agreement.

13.6 In the event this Agreement is terminated for convenience, Provider shall be paid for any goods and services properly provided through the termination date specified in the written notice of termination. Provider acknowledges that it has received good, valuable and sufficient consideration from County, the receipt and adequacy of which are hereby acknowledged by Provider, for County's right to terminate this Agreement for convenience, and Provider hereby waives, to the full extent permissible under applicable law, any and all rights to challenge the adequacy of such consideration or the validity of County's right to terminate for convenience.

Exhibit 2

## ARTICLE 14. MISCELLANEOUS

14.1 Rights in Documents and Work. Subject to the terms of this section, any and all reports, photographs, surveys, and other data and documents provided or created in connection with this Agreement shall be and remain the property of County and, if a copyright is claimed, Provider hereby grants to County a nonexclusive perpetual license to use the copyrighted item(s), to prepare derivative works, and to make and distribute copies to the public. In the event of termination or expiration of this Agreement, any reports, photographs, surveys, and other data and documents prepared by Provider, whether finished or unfinished, shall become the property of County and shall be delivered by Provider to the Contract Administrator within seven (7) days of termination or expiration of this Agreement by either Party. Notwithstanding anything to the contrary, any work product and other materials (i) existing prior to commencement of the work, (ii) developed outside the scope of the work, or (iii) developed as part of the work and within the scope of the Provider's business practice (including without limitation, business methods, tools, methodologies, processes, techniques, system architecture and the like), shall be and remain the sole and exclusive property of Provider and Provider retains intellectual property rights in Provider's products and technology.

14.2 Audit Right and Retention of Records. County shall have the right to audit the books, records, and accounts of Provider and its subcontractors that are related to this Agreement. Provider and its subcontractors shall keep such books, records, and accounts as may be necessary in order to record complete and correct entries related to the Agreement and performance thereunder. All books, records, and accounts of Provider and its subcontractors shall be kept in written form, or in a form capable of conversion into written form within a reasonable time, and upon request to do so, Provider or its subcontractor, as applicable, shall make same available at no cost to County in written form.

Provider and its subcontractors shall preserve and make available, at reasonable times within Broward County for examination and audit by County, all financial records, supporting documents, statistical records, and any other documents pertinent to this Agreement for a minimum period of three (3) years after expiration or termination of this Agreement or until resolution of any audit findings, whichever is longer. County audits and inspections pursuant to this section may be performed by any County representative (including any outside representative engaged by County). County reserves the right to conduct such audit or review at Provider's place of business, if deemed appropriate by County, with seventy-two (72) hours' advance notice.

Any incomplete or incorrect entry in such books, records, and accounts shall be a basis for County's disallowance and recovery of any payment upon such entry. If an audit or inspection in accordance with this section discloses overpricing or overcharges to County of any nature by Provider in excess of five percent (5%) of the total contract billings reviewed by County, the reasonable actual cost of County's audit shall be reimbursed to County by Provider in addition to making adjustments for the overcharges. Any adjustments and/or payments due as a result of

Exhibit 2

such audit or inspection shall be made within thirty (30) days from presentation of County's findings to Provider.

Provider shall ensure that the requirements of this section are included in all agreements with its subcontractor(s).

14.3 Public Records. To the extent Provider is acting on behalf of County as stated in Section 119.0701, Florida Statutes, Provider shall:

a. Keep and maintain public records required by County to perform the services under this Agreement;

b. Upon request from County, provide County with a copy of the requested records or allow the records to be inspected or copied within a reasonable time and at a cost that does not exceed that provided in Chapter 119, Florida Statutes, or as otherwise provided by law;

c. Ensure that public records that are exempt or confidential and exempt from public record requirements are not disclosed except as authorized by law for the duration of this Agreement and following completion or termination of this Agreement if the records are not transferred to County; and

d. Upon completion or termination of this Agreement, transfer to County, at no cost, all public records in possession of Provider or keep and maintain public records required by County to perform the services. If Provider transfers the records to County, Provider shall destroy any duplicate public records that are exempt or confidential and exempt. If Provider keeps and maintains public records, Provider shall meet all applicable requirements for retaining public records. All records stored electronically must be provided to County upon request in a format that is compatible with the information technology systems of County.

The failure of Provider to comply with the provisions of this section shall constitute a material breach of this Agreement entitling County to exercise any remedy provided in this Agreement or under applicable law.

A request for public records regarding this Agreement must be made directly to County, who will be responsible for responding to any such public records requests. Provider will provide any requested records to County to enable County to respond to the public records request.

**IF PROVIDER HAS QUESTIONS REGARDING THE APPLICATION OF FLORIDA STATUTES CHAPTER 119 TO PROVIDER'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS AGREEMENT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT (954) 468-0108, BIALEXANDER@BROWARG.ORG, 1850 ELLER DR., SUITE 603, FORT LAUDERDALE, FLORIDA 33316.**

14.4 Truth-In-Negotiation Representation. Provider's compensation under this Agreement is based upon representations supplied to County by Provider, and Provider certifies that the wage rates, factual unit costs, and other factual information supplied to substantiate Provider's compensation are accurate, complete, and current at the time of contracting. County shall be entitled to recover any damages it incurs to the extent any such representation is untrue.

14.5 Public Entity Crime Act. Provider represents that it is familiar with the requirements and prohibitions under the Public Entity Crime Act, Section 287.133, Florida Statutes, and represents that its entry into this Agreement will not violate that Act. In addition to the foregoing, Provider further represents that there has been no determination that it committed a "public entity crime" as defined by Section 287.133, Florida Statutes, and that it has not been formally charged with committing an act defined as a "public entity crime" regardless of the amount of money involved or whether Provider has been placed on the convicted vendor list. Notwithstanding any provision in this Agreement to the contrary, if any representation stated in this paragraph is false, County shall have the right to immediately terminate this Agreement and recover all sums paid to Provider under this Agreement.

14.6 Independent Contractor. Provider is an independent contractor under this Agreement. Provider shall not have the right to bind County to any obligation not expressly undertaken by County under this Agreement.

14.7 Third-Party Beneficiaries. The Parties acknowledge that there are no third-party beneficiaries under this Agreement.

14.8 Notices. In order for a notice to a Party to be effective under this Agreement, notice must be sent via U.S. first-class mail with a contemporaneous copy via email to the addresses listed below and shall be effective upon mailing. The addresses for notice shall remain as set forth herein unless and until changed by providing notice of such change.

NOTICE TO COUNTY:
Broward County Port Everglades
Attn: Director
1850 Eller Drive
Fort Lauderdale, Florida 33316
Email address: gwiltshire@broward.org

NOTICE TO PROVIDER:
TIBA Parking Systems, LLC
Attn: Jon Bowsher
President, North and South America
2228 Citygate Drive
Columbus, Ohio 43219
Email address: Jon.Bowsher@tibaparking.com

14.9 Assignment. Except for subcontracting approved by County at the time of the execution of this Agreement or any written amendment hereto, neither this Agreement nor any right or interest herein may be assigned, transferred, subcontracted, or encumbered by Provider without

Exhibit 2

the prior written consent of County. If Provider violates this provision, County shall have the right to immediately terminate this Agreement.

14.10 Conflicts. Provider agrees that neither it nor its employees will have or hold any continuing or frequently recurring employment or contractual relationship that is substantially antagonistic or incompatible with Provider's loyal and conscientious exercise of the judgment and care required to perform under this Agreement. Provider further agrees that none of its officers or employees shall, during the term of this Agreement, serve as an expert witness against County in any legal or administrative proceeding in which he, she, or Provider is not a party, unless compelled by court process. Further, such persons shall not give sworn testimony or issue a report or writing, as an expression of his or her expert opinion, which is adverse or prejudicial to the interests of County in connection with any such pending or threatened legal or administrative proceeding unless compelled by court process. The limitations of this section shall not preclude Provider or any person from in any way representing themselves, including giving expert testimony in support thereof, in any administrative or legal proceeding. Provider agrees that each of its contracts with subcontractors performing under this Agreement shall contain substantively identical language to ensure that each subcontractor and its officers and employees meet the obligations contained in this paragraph.

14.11 Waiver of Breach. The failure of either Party to enforce any provision of this Agreement shall not be deemed a waiver of such provision or modification of this Agreement. A waiver of any breach under this Agreement shall not be deemed a waiver of any subsequent breach.

14.12 Compliance with Laws. Provider shall comply with all applicable federal, state, and local laws, codes, ordinances, rules, and regulations in performing under this Agreement.

14.13 Severability. In the event any part of this Agreement is found to be unenforceable by any court of competent jurisdiction, that part shall be deemed severed from this Agreement and the balance of this Agreement shall remain in full force and effect.

14.14 Joint Preparation. This Agreement has been jointly prepared by the Parties hereto, and shall not be construed more strictly against either Party.

14.15 Headings and Interpretation. The headings contained in this Agreement are for reference purposes only and shall not in any way affect the meaning or interpretation of this Agreement. All personal pronouns used in this Agreement shall include the other gender, and the singular shall include the plural, and vice versa, unless the context otherwise requires. Terms such as "herein," "hereof," "hereunder," and "hereinafter," refer to this Agreement as a whole and not to any particular sentence, paragraph, or section where they appear, unless the context otherwise requires.

14.16 Governing Law, Venue and Waiver of Jury Trial. This Agreement shall be interpreted and construed in accordance with, and governed by, the laws of the state of Florida. The Parties agree that the exclusive venue for any lawsuit arising from, related to, or in connection with this

Exhibit 2

Agreement shall be in the state courts of the Seventeenth Judicial Circuit in and for Broward County, Florida. If any claim arising from, related to, or in connection with this Agreement must be litigated in federal court, the Parties agree that the exclusive venue for any such lawsuit shall be in the United States District Court or United States Bankruptcy Court for the Southern District of Florida. **BY ENTERING INTO THIS AGREEMENT, PROVIDER AND COUNTY HEREBY EXPRESSLY WAIVE ANY AND ALL RIGHTS EITHER PARTY MAY HAVE TO A TRIAL BY JURY OF ANY CAUSE OF ACTION OR CLAIM ARISING FROM, RELATED TO, OR IN CONNECTION WITH THIS AGREEMENT.**

14.17 Amendments. No modification or amendment to this Agreement shall be effective unless it is in writing and executed by authorized representatives of each Party. Without limiting the foregoing, the terms of this Agreement shall prevail over and against any additional or contrary terms and conditions in any format or medium whatsoever including, without limitation, shrinkwrap, click-through, or terms and conditions associated with any upgrade, update, release, patch, or other modification of the System or Software, unless expressly agreed to in writing by an amendment hereto executed by authorized representatives of each Party.

14.18 Prior Agreements. This Agreement represents the final and complete understanding of the Parties regarding the subject matter hereof and supersedes all prior and contemporaneous negotiations and discussions regarding that subject matter. There is no commitment, agreement, or understanding concerning the subject matter of this Agreement that is not contained in this written document.

14.19 HIPAA Compliance. It is understood by the Parties that County personnel or their agents have access to protected health information (hereinafter known as "PHI") that is subject to the requirements of 45 C.F.R. § 160, 162, and 164 and related statutory and regulatory provisions. In the event Provider is considered by County to be a covered entity or business associate or otherwise required to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") or the Health Information Technology for Economic and Clinical Health Act ("HITECH"), Provider shall fully protect individually identifiable health information as required by HIPAA and HITECH. If requested by County, Provider shall execute a Business Associate Agreement in the form set forth at www.broward.org/Purchasing/Pages/StandardTerms.aspx. Where required, Provider shall handle and secure such PHI in compliance with HIPAA, HITECH and its related regulations and, if required by HIPAA, HITECH, or other laws, shall include in its "Notice of Privacy Practices" notice of Provider's and County's uses of a client's PHI. The requirement to comply with this provision, HIPAA and HITECH shall survive the expiration or termination of this Agreement. County hereby authorizes the County Administrator to sign Business Associate Agreements if required under this Agreement.

14.20 Payable Interest

14.20.1 Payment of Interest. County shall not be liable to pay any interest to Provider for any reason, whether as prejudgment interest or for any other purpose, and in furtherance thereof Provider waives, rejects, disclaims and surrenders any and all entitlement it has or may have to receive interest in connection with a dispute or claim arising from, related to, or in connection with this Agreement. This subsection shall not apply to any claim interest, including for post-judgment interest, if such application would be contrary to applicable law.

14.20.2 Rate of Interest. If the preceding subsection is inapplicable or is determined to be invalid or unenforceable by a court of competent jurisdiction, the annual rate of interest payable by County under this Agreement, whether as prejudgment interest or for any other purpose, shall be, to the full extent permissible under applicable law, 0.25% (one quarter of one percent) simple interest (uncompounded).

14.21 Incorporation by Reference. Any and all Recital clauses stated above are true and correct and are incorporated herein by reference.

14.22 Representation of Authority. Each individual executing this Agreement on behalf of a Party hereto represents and warrants that he or she is, on the date of execution, duly authorized by all necessary and appropriate action to execute this Agreement on behalf of such Party and does so with full legal authority. Provider represents that it is an entity authorized to transact business in the State of Florida.

14.23 Domestic Partnership Requirement. Unless this Agreement is exempt from the provisions of Section 16½-157 of the Broward County Code of Ordinances, which requires County contractors to provide benefits to domestic partners of their employees, Provider agrees to fully comply with Section 16½-157 during the entire term of the Agreement. If Provider fails to fully comply with that section, such failure shall constitute a material breach which shall allow County to exercise any remedy available under this Agreement, under applicable law, or under section 16½-157. For that purpose, the contract language referenced in Section 16½-157 is incorporated herein as though fully set forth in this paragraph.

14.24 Drug-Free Workplace. It is a requirement of County that it enter into contracts only with firms that certify the establishment of a drug-free workplace in accordance with Chapter 21.31(a)(2) of the Broward County Procurement Code. Execution of this Agreement by Provider shall serve as Provider’s required certification that it has or will establish a drug-free workplace in accordance with Section 287.087, Florida Statutes, and Chapter 21.31(a)(2) of the Broward County Procurement Code, and that it will maintain such drug-free workplace for the full term of this Agreement.

14.25 Contingency Fee. Provider represents that it has not paid or agreed to pay any person or entity, other than a bona fide employee working solely for Provider, any fee, commission, percentage, gift, or other consideration contingent upon or resulting from the award or making of this Agreement. If County learns that this representation is false, County shall have the right to terminate this Agreement without any further liability to Provider. Alternatively, if such representation is false, County, at its sole discretion, may deduct from the compensation due Provider under this Agreement the full amount of such fee, commission, percentage, gift, or consideration.

14.26 Living Wage Requirement. If Provider is a "covered employer" within the meaning of the Broward County Living Wage Ordinance, Broward County Code sections 26-100 – 26-105, Provider agrees to and shall pay to all of its employees providing "covered services," as defined therein, a living wage as required by such ordinance, and Provider shall fully comply with the requirements of such ordinance. Provider shall be responsible for and shall ensure that all of its subcontractors that qualify as "covered employers" fully comply with the requirements of such ordinance.

14.27 Force Majeure. If the performance of this Agreement, or any obligation hereunder, is prevented by reason of hurricane, earthquake, or other casualty caused by nature, or by labor strike, war, or by a law, order, proclamation, regulation, or ordinance of any governmental agency, the Party so affected, upon giving prompt notice to the other Party, shall be excused from such performance to the extent of such prevention, provided that the Party so affected shall first have taken reasonable steps to avoid and remove such cause of nonperformance and shall continue to take reasonable steps to avoid and remove such cause, and shall promptly notify the other Party in writing and resume performance hereunder whenever and to the full extent such causes are removed. However, if such nonperformance exceeds sixty (60) days, the Party that is not prevented from performance by the force majeure event shall have the right to immediately terminate this Agreement upon written notice to the Party so affected. This section shall not supersede or prevent the exercise of any right the Parties may otherwise have to terminate this Agreement.

14.28 County Logo. Provider shall not use County's name, logo, or otherwise refer to this Agreement in any marketing or publicity materials without the prior written consent of County.

14.29 Additional Security Requirements. Consultant certifies and represents that it will comply with the Port Everglades Security Requirements attached hereto and incorporated herein as Exhibit G.

14.30 Counterparts. This Agreement may be executed in multiple originals, and may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement.

(The remainder of this page is intentionally left blank.)

IN WITNESS WHEREOF, the Parties hereto have made and executed this Agreement: BROWARD COUNTY through its BOARD OF COUNTY COMMISSIONERS, signing by and through its Mayor or Vice-Mayor, authorized to execute same by Board action on the _____ day of _________________, 2020, and TIBA PARKING SYSTEMS, LLC, signing by and through its ___________________________, duly authorized to execute same.

COUNTY

ATTEST:

___________________________________
Broward County Administrator, as
ex officio Clerk of the Broward County
Board of County Commissioners

BROWARD COUNTY, by and through
its Board of County Commissioners

By: ___________________________________

______ day of ______________, 2020

Approved as to form by
Andrew J. Meyers
Broward County Attorney
Governmental Center, Suite 423
115 South Andrews Avenue
Fort Lauderdale, Florida 33301
Telephone: (954) 357-7600
Telecopier: (954) 357-7641

By: 1-28-2020
Neil Sharma (Date)
Assistant County Attorney

By: 1/28/2020
Rene D. Harrod (Date)
Deputy County Attorney

NS/RDH
TIBA Parking LLC System and Services Agreement
455805.18
01_22_2020

PROVIDER

WITNESSES:

Signature

Joe Mollish

Print Name of Witness above

Signature

ADAM ROHRER

Print Name of Witness above

TIBA PARKING SYSTEMS, LLC

By: Jon Bowsher

Authorized Signor

Jon Bowsher, President of North and South America

Print Name and Title

22 day of JANUARY, 2020

ATTEST:

Marilyn J Stone

Corporate Secretary or other person authorized to attest

(CORPORATE SEAL OR NOTARY)

NOTARIAL SEAL
STATE OF OHIO

MARILYN J JOHNSON-STONE
NOTARY PUBLIC
STATE OF OHIO
Comm. Expires
03/15/2022

## Exhibit A – Statement of Work

Provider and County agree that Provider shall provide the following work under this Agreement:

### 1. Project Request

Provider will install the System, inclusive of the Software and Equipment listed below, at the parking sites specified herein to provide County with a real time computerized parking access and revenue control system at Port Everglades. This System will allow County to control access and collect parking revenues while increasing efficiency and reducing transaction times for customers and employees. Provider will perform all Services required for full implementation of the System. Provider may utilize two (2) approved subcontractors to perform Services under this Agreement: Pinnacle Parking Systems; and Arbor Electrical Services d/b/a Mr. Wireman. Provider is responsible for its subcontractors' performance under this Agreement.

Provider represents that the Software, Equipment, and related Services provided under this Agreement will provide this functionality and solution.

### 2. Services Description

A. Software. Provider will provide the following Software under the terms of this Agreement:

| **Software Suite, Version & Module** | **Quantity & Type of License** ***(e.g., Enterprise, User, Third-Party)*** | **Describe Purpose, Functionality & Expected Operation of Software** |
|---|---|---|
| TIBA SmartPark Facility Management System – version SP 5.2.0, or most current version at time of implementation | Enterprise license for an unlimited number of users | Provides a real time computerized parking access and revenue control system to allow County to control access and collect parking revenues from customers, employees, and parking facility staff |

| **Third-Party Software provided by Provider** | **Quantity & Type of License** | **Describe Purpose, Functionality & Expected Operation of Software** |
|---|---|---|
| Commend VoIP Intercom Software | Third-Party Enterprise Perpetual License | Intercoms that integrates with the System for on-site management (requires an additional module for full remote management while off-site) |

B. Equipment. Provider will provide the Equipment listed in Attachment 1 to this Statement of Work.

### 3. Technical Approach

A. Site Locations

Provider will perform Services at the following sites. The sites may be referenced by site name or site number throughout this Statement of Work.

Exhibit 2

- Site 1 – Back office (temporary server installation only – address to be provided by County prior to commencement of the project)
- Site 2 – Terminal 19 surface lot
- Site 3 – Terminal 18 surface lot
- Site 4 – Midport garage
- Site 5 – T2/T4 garage

B. <u>Onsite Analysis and Critical Design Review</u>

Provider will be responsible for performing a complete analysis of County's current operations. The results of this analysis will be used during the critical design review meeting to develop the installation and deployment schedule and for County to choose the best methods for Provider's software and hardware replacement and deployment activities. The analysis will include each of the five (5) County sites listed above.

Provider shall provide County with an installation and deployment schedule after the onsite analysis and critical design review meeting. This installation and deployment schedule will contain a transition plan/project schedule, which will be agreed to by the Parties and based on the priority of County's parking needs and operation. The project schedule must include the timeline for the complete project, including, but not limited to start date, site construction, electrical, training, and testing. The installation and deployment schedule must be submitted for review and approval by County, any edits or changes requested by County incorporated, and the revised installation and deployment schedule approved in writing by County.

The installation and deployment schedule will include, at a minimum:

- Results of the onsite analysis of current operations, including Provider's proposed configuration of the System based on the onsite analysis.
- A final configuration and programming design based on County feedback to the proposed configuration in the bullet above.
- Test scripts created by Provider to use for the applicable testing procedures, inclusive of the test criteria outlined in this Statement of Work; the test scripts may be amended by written agreement of the Parties.
- Detail regarding implementation of the license place inventory system.
- Detail regarding training sessions (as further specified in Section 5 below).
- Process and procedures for installation and lane acceptance testing.
- Creation of the transition plan/project schedule (see below).
- Details and process for Equipment delivery (including staging at Provider's corporate office in Columbus). Equipment will be shipped directly to County and stored by County until installation.

The transition plan/project schedule will include, at a minimum:

- Timeframe for installation of any new network infrastructure and testing
- Timeframe for installation of new data servers and testing
- Timeframe for installation of new credit card processing and connection to clearinghouse

with testing

- Timeframe for coordination for the removal of existing parking and revenue control system (i.e., Federal APS)
- Timeframe for installation of Equipment
- Timeframe for integration and development of other Services required per this Statement of Work
- Traffic Coordination Plan (see Section 4)

C. Server Installation and Relocation

As the permanent location of the server (Site 5 - T2/T4 garage) is still undergoing construction, Provider will temporarily install a fully functioning server solution at Site 1 (back office). In addition to the server installation, Provider will build a System network utilizing the current fiber infrastructure available at Site 1. At a time mutually agreed to by the Parties, Provider will relocate the server solution to its final location at the management office at Site 5, as determined by County. The server will be on a separate network segment from the County network and County staff will not have access to the server. Provider is solely responsible for the security of the server, including applying patches and updates to the server.

D. Equipment Removal and Disposal

As part of Provider's implementation services, Provider will remove all existing parking equipment. The removal and disposal of all equipment will follow a process to be approved by County.

Equipment will be removed at Sites 2-4, one (1) site location at a time and one (1) lane at a time, unless otherwise requested by County. Provider will minimize lane closures during the removal of old equipment to ensure minimal impact on County operations. During equipment removal, Provider will ensure two (2) systems run simultaneously (County's existing Federal APS system and the new System) following the process reflected below to minimize lane closures during removal of old equipment.

E. Project Phases

After Provider performs the tasks set forth in Sections B, C, and D above, Provider's implementation services shall be performed onsite at each of the five (5) County sites in accordance with the phases set forth below. The order of these sites may be re-ordered or sites may be modified or removed, as agreed to by the Parties. Two (2) of the Provider's subcontractors will be onsite to perform equipment replacement: Pinnacle Parking Systems, and Mr. Wireman.

During Equipment installation, Provider will ensure that County's existing Federal APS system runs concurrently with the System until Final Acceptance to minimize lane closures during

Equipment replacement.

After completion of all Phases for each project site, County will perform preliminary acceptance testing in accordance with Section 7 at the applicable site.

Phase 1 (To be performed at each Site 1-5, unless stated otherwise)

Provider will:

- Ensure Phase 1 activities do not affect any existing equipment
- Install license plate recognition cameras in advance in all available/accessible areas
- Install free exit gates at short term and reserved exits
- Pull all communication wires in all available/accessible areas
- Ensure sign controllers are installed and tested as on each lane as the lane is installed
- Ensure the arming vehicle detection loop is saw-cut at all terminal lots and garages. Due to the depth of the re-enforcement bars, Provider will install above ground loops or sensors at Site 5 (T2/T4 garage).
- Ensure the reset/protection vehicle detection loop is saw-cut at all terminal lots and garages, except the T2/T4 Garages.
- Ensure the arming vehicle detection (for Site 5 only)
- Ensure the reset/protection vehicle detection (for Site 5 only)
- Ensure the double stroke red X/green arrow sign are installed in the entry/exit lanes
- Ensure barrier gate arms are installed in the entry/exit lanes

Phase 2 Cabling and Electrical (To be performed at each Site 1-5, unless stated otherwise):

Provider will:

- Install electrical to enable the powering of all devices
- Proceed with the installation of all non-electrical components once electrical has been completed and is functioning successfully, including cabling
- Follow County approved installation and deployment schedule at County’s five (5) site locations
- Pull cabling – Entry lane (Possible removal of old device if no room in the conduit)
- Pull cabling – Exit lanes (Possible removal of old device if no room in the conduit)
- Pull cabling – Wrap up cabling
- Perform installation of all required Equipment in the entrance lane, one (1) lane at a time, using the applicable Equipment listed in Attachment 1 – Equipment List By Location.
- Install entry of each lane
- Perform installation of all required Equipment in the exit lane, one (1) lane at a time, using the applicable Equipment listed in Attachment 1 – Equipment List by Location.
- Install exit of each lane (replace, test, and open)

Phase 3 (To be performed at Site 4 only)

Provider will:

- Ensure the gate is tied to the sliding door gate controllers and addressed when the lane is scheduled in the installation and deployment schedule
- Pull cabling – Entry lane (Possible removal of old device if no room in the conduit)
- Pull cabling – Exit lanes (Possible removal of old device if no room in the conduit)
- Pull cabling – Wrap up cabling
- Install entry of each lane

Phase 4 (To be performed at each Site 2-4)

Provider will:

- Replace, test, and open each entry lane
- Replace, test, and open each exit lane

Phase 5 (To be performed at Site 5 only)

Provider will:

- Test and open each entry lane
- Test and open each exit lane
- Testing of all lanes and addressing punch list items; punch list items are all items identified by County that require further testing or correction.

Phase 6 (To be performed at each Site 2-5)

Provider will perform installation of all automatic pay-on-foot stations (cash, coins, credit card payments) and central pay-on-foot stations (credit card payments only), one (1) pay station at a time, using the applicable equipment listed in Attachment 1 – Equipment List by Location. Each automatic and central pay station will provide the following functionality, as applicable:

- Each automatic pay station will have standard graphic panels, thin-film-transistor ("TFT") display, Commend VoIP intercom, and a voice annunciator to assist customers with their transaction.
- Each automatic pay station will include bank storage and dispensing of up to three (3) denominations of cash bills (U.S. dollars: $1, $5, $10).
- Each automatic pay station machine will allow a customer to insert their barcode ticket, and then insert their credit card, coins, or cash bills as form of payment. Any change needed will be in the form of cash bills. Once payment is accepted, the customer's validated barcode ticket will be returned to them to use at the exit lane station. An allotted grace period, to be identified by County during implementation, will allow customer to exit the facility from the automatic pay station without incurring additional hourly charges.
- Each central pay station will have graphic panels, TFT display, and Commend intercom to assist customers with their transaction.

- Each central pay station will only accept credit cards as a form of payment. A customer will need to insert their barcode ticket and then insert their credit card. Once payment is accepted, the customer's validated barcode ticket will be returned to them to use at the exit lane station. An allotted grace period, to be identified by County during implementation, will allow customer to exit the facility from the pay station without incurring additional hourly charges. The Parties will mutually agree on a Go-Live Date for each site after all Phases are complete at the applicable site(s). Final Acceptance must be achieved on or before October 1, 2020.

F. System Functionality

**Entry Device Functionality Description**
Provider will configure each entry lane to provide the following functionality:

- Customers will be granted entry by either pulling a barcode ticket in the entry lane using an hourly rate to park or by presenting a valid pre-printed barcode or Smartphone QR code to the scanner for entry (or other approved format agreed to by the Parties).
- Proximity card holders will be granted entry by presenting a valid credential to the proximity reader.
- The Commend VoIP digital intercom will provide customers the ability to communicate with parking facility staff and for parking facility staff to respond to the customer via the intercom and initiate opening of the barrier gate arm. The Commend VoIP digital intercom must be able to forward calls to any phone number.
- The vehicle detectors/loop detectors will provide detection of vehicle presence essential to Equipment operation and facility entry/exit count totals. The vehicle detector will be fully self-tuning, and self-scanning vehicle detector sensors (arming and closing) installed at all entry/exit lane equipment shall provide complete facility entry/exit count totals, regardless of the status of the component Equipment (e.g., gate arm raised). The vehicle detector will be integrated into the overall vehicle count control as part of the System and will have sufficient speed and reliability to transmit accurate live data for the System.
- The barrier gate arm will raise after a customer takes a ticket for entry to the parking site and will lower once the vehicle has completed entering.
- The double stroke red X/green arrow sign will display the open lanes for entry by displaying a green arrow and a closed lane by displaying a red X.

**Exit Lane Functionality Description**
Provider will configure each exit lane to provide the following functionality:

- Customers will be permitted to exit by performing one (1) of these actions:
  - Inserting a validated ticket and making payment at the applicable pay station with credit card or smartphone QR code;
  - If parking fees were paid at an automatic pay station, the pre-paid barcode ticket will be inserted and any additional fees due will be paid by credit card only at the exit lane station;

   - Inserting an un-validated ticket to the applicable pay station and inserting credit card or using smartphone QR code for payment; or
   - Presenting a valid pre-printed barcode or Smartphone QR code to the scanner (or other approved format agreed to by the Parties). Any additional fees due will require a credit card payment.
- Proximity card holders will be granted exit by presenting a valid credential to the proximity reader.
- The Commend VoIP digital intercom will provide a customer the ability to communicate with parking facility staff and for parking facility staff to respond to the customer via the intercom and initiate opening of the barrier gate arm. The Commend VoIP digital intercom must be able to forward calls to any phone number.
- The vehicle detectors/loop detectors and will provide detection of vehicle presence essential to Equipment operation and facility entry/exit count totals. Vehicle detector will be fully self-tuning and self-scanning vehicle detector sensors (arming and closing) installed at all entry/exit lane equipment shall provide complete facility entry/exit count totals, regardless of the status of the component Equipment (e.g., gate arm raised). The vehicle detector will be integrated into the overall vehicle count control as part of the System. The detector will have sufficient speed and reliability transmit accurate live data for the System.
- The barrier gate arm will raise after a customer insert their ticket for exit at the exit station and completes the payment. The barrier gate arm will lower once the vehicle has completed exiting.
- The double stroke red X/green arrow sign will display the open lanes for exiting by displaying a green arrow and a closed lane by displaying a red X.

G. <u>License Plate Recognition Cameras and License Plate Inventory System</u>

At Sites 2, 3, 4, and 5, Provider will install and configure a license plate inventory system to integrate with each of its license plate recognition ("LPR") cameras. Provider will install and configure a license plate recognition camera at each entry lane and exit lane, at sites 2-5. The System will provide the following abilities:

- Maintain a license plate inventory for every car that enters the facility
- Enables facility counts
- Tie a license plate to a ticket transaction to eliminate issues with lost tickets

H. <u>Merchant Validation Feature</u>

Provider will configure the System to provide a merchant validation feature to provide County the ability to perform the following tasks:

- Print pre-paid parking barcode validation label sheets on a color laser printer which can be distributed and applied to a customer's entry ticket.
- Process the pre-paid parking barcode validation at the System's exit station according to County's programming preferences.

- Allow customers with a pre-paid parking barcode validation to pay the additional parking fee with a credit card at the exit station if the customer has remained longer than the allotted time which was pre-paid.

I. Data Conversions

Provider will be responsible for performing data conversions from County's current parking access and revenue control system (Federal APS) to the System from the beginning of the installation through Final Acceptance. This action will be performed at each County site and using a closed loop single server housed at a designated County location. The format for data conversions will be determined after Provider has conducted the onsite analysis of County's current operations and during the critical design review process. Provider must test all data conversions prior to County conducting Final Acceptance Testing. County will test the data conversions for accuracy during Final Acceptance Testing.

J. System Reporting

Provider will ensure the System provides real time reporting and a variety of canned reports that can be exported to Excel, including, but not limited to:

- Revenue reports - Comprehensive financial and statistical data about the parking facility's revenue streams
- System event reports - Event log data on gate openings, garage station counters and device alerts
- Ticket reports - Tracks and details parking ticket usage to help protect a garage's revenue
- Occupancy and traffic reports - Statistical traffic and occupancy data including parking time counts, overflow area analysis and demand level assessments
- Vehicle ID reports - Provides access to transaction logs and usage statistics
- Validation reports - Provides information into the operations of the validation programs that are in use
- Company reports - Financial and revenue data about how companies and their employees use the parking facility
- Customer reports - Traffic usage data specific to customers plus financial and revenue information
- Analytical charts - Graphically summarizes statistical traffic and occupancy data by customer type and cruise ship
- Revenue and transactions - Refined by facility, type of transaction, number of transactions, payment type and cruise ship, or event.
- Entry and exit lane – Reporting for all functional and non-functional entry lanes and exit lanes and number of vehicles entering and exiting all lanes.

K. Security/Access

Provider will cooperate with County and provide any and all information that County may request in order to determine appropriate security and network access restrictions and verify Provider compliance with County security standards. Provider will provide County with a System access list for the individuals that will need access. County will review and approve this list to ensure the list is accurate.

## 4. Managerial Approach & Communication

Provider will ensure that the persons responsible for Provider's performance of the Services under this Agreement and, to the extent applicable, identified below (collectively "Key Personnel") are appropriately trained and experienced and have adequate time and resources to perform in accordance with the terms of this Agreement. To the extent Provider seeks or is required to make any change to the composition of the Key Personnel, Provider will provide County with thirty (30) days' advance notice (or as much advance notice as is possible if thirty (30) days' notice is not possible) regarding such changes and the management plan associated with such changes. County shall not be responsible for any additional costs associated with a change in Key Personnel.

Key Personnel

Each of the on-site Key Personnel will work with County and Provider to coordinate dates and times for project tasks, which may include after-hours and weekends.

**Key Personnel**

| Provider Participants: | Role | Email | Address/Phone |
|---|---|---|---|
| Tom Foster | EVP Projects & Delivery | tom.foster@tibaparking.com | TIBA LLC<br>2228 Citygate Drive<br>Columbus, OH 43219<br>(614) 755-0242 |
| Adam Rohrer | Director, Sales Support | adam.rohrer@tibaparking.com | TIBA LLC<br>2228 Citygate Drive<br>Columbus, OH 43219<br>(614) 328-2040 |
| Joe Mollish | Vice President, Strategic Accounts | joe.mollish@tibaparking.com | TIBA LLC<br>2228 Citygate Drive<br>Columbus, OH 43219<br>(314) 280-4750 |
| Gregory Dann | Project Manager | gregory.dann@tibaparking.com | TIBA LLC<br>2228 Citygate Drive<br>Columbus, OH 43219<br>(614) 449-2317 |
| Doug Tinklepaugh | Managing Member | doug@pinnacleparkingsystems.com | Pinnacle Parking Systems, LLC<br>516 NE 13 Street<br>Ft. Lauderdale, FL 33304<br>(954)-654-8934 |

| Provider Participants: | Role | Email | Address/Phone |
|---|---|---|---|
| Lambert Anglin | Electrical | service@mrwireman.com | Arbor Electrical (CBE)<br>3501 SW 47 Avenue<br>Davie, FL 33314<br>(954) 812-1442 |

Project Manager (Day-to-day point of contact)

Gregory Dann is the project manager and will direct the installation and technical team. The project manager will be responsible for the entire project from contract signature to beginning of warranty. Gregory Dann will report directly to Joe Mollish.

Executive Level (Executive level single point of contact)

Joe Mollish is the senior executive level and single point of contact for higher-level communications for Provider.

Reporting Schedule

Provider and County will adhere to the following communication and reporting schedule unless otherwise agreed in writing by the Parties:

*Project Kickoff Meeting*

Provider and County will participate in an initial onsite kickoff meeting at the commencement of the project to review the project plan and details of the work to be performed. The kickoff meeting will be attended by the Provider's Project Manager and County's Project Manager and other individuals requested by the respective Project Managers.

*Status Meetings*

After the project kickoff meeting, Provider will coordinate and conduct remote status meetings on a bi-weekly basis. These bi-weekly meetings will continue up until one (1) week before System installation.

After System installation, Provider will coordinate and conduct status meetings on a weekly basis. These weekly meetings will continue until County issues written notice of Final Acceptance to Provider.

*Monthly Installation Reports*

A monthly installation update report will be prepared by Provider and sent out to all parties to provide an update of what has been installed and what phases are next.

*Traffic Coordination Plan*

Provider will develop and deliver a traffic coordination plan to County for written approval. The traffic coordination plan will address implementation procedures to ensure operational disruptions during Equipment replacement are kept to a minimum. The traffic coordination plan will be used to:

- Minimize lane closures during installation of new Equipment

- Prepare a work plan to schedule and minimize installation work around peak season hours of operation, holidays, and weekends from October through April and to schedule around cruise schedules
- Focus equipment installation activities occur during non-business hours when possible
- Ensure the implementation of all electrical and communication infrastructure before work in entry or exit lanes occurs, where possible
- Phase equipment implementation so that one (1) entry is installed with one (1) exit

### 5. Onsite Training

Provider will provide onsite training sessions for County staff and/or third-party personnel identified by County, consisting of a minimum of twenty-four (24) training hours. Each class will run a minimum of four (4) hours. Training hours shall be allocated as desired by County and will adhere to County approved training plan format. Each training session will be conducted at a designated County location between Monday and Friday from 8:30 a.m. to 5:00 p.m., and will be conducted after the established Go-Live for each parking site, as agreed to by both Parties. Each training session will be tailored to specific shift tasks to provide onsite training using functioning parking lanes as well as the utilization of data and reports to train staff on the back-office functions of the System.

Provider will be responsible for creating a training plan for County's review and approval. The training schedule will be provided to County a minimum of thirty (30) days before the commencement of training sessions.

Provider will provide training attendees with a hard copy of all training materials. County will be provided with an electronic and hard copy version of all training materials. After the initial training, County may request additional training sessions for basic training topics at no cost to County.

Cashiers

Provider will deliver three (3) sessions: training session 1 for morning shift, training session 2 for afternoon shift, training session 3 for evening shift.

For the cashiers training sessions, basic training topics shall include, at a minimum:

- Logging on/off the computer and printing a shift summary (if applicable)
- Detailed operation of the point-of-sale equipment
- Basic operation of ticket dispenser and credit card exit machines
- Changing out receipt paper

Managers/Supervisors

Provider will deliver two (2) sessions: training session 1, training session 2.

For the managers/supervisors training sessions, basic training topics shall include, at a minimum:

- Detailed operation and troubling shooting of all devices
- Replacement of receipt paper and ticket rolls

- Processing of credit cards at the point-of-sale unit
- Replacing/Loading currency bills in the pay-on foot equipment
- Basic report run off and review
- Review of System software
- Equipment programming macros

Administrative/Back office
Provider will deliver two (2) sessions: training session 1, training session 2.

For the administrative/back office training sessions, basic training topics shall include, at a minimum:

- Logging into the System
- Counts
- Software operation
- Understanding reports
- Credit card reports and processing
- Macros for reports

## 6. Deliverable Products and Services

**DELIVERABLES:**

| No. | Description | Requirements or Preliminary Acceptance Criteria |
|---|---|---|
| 1. | Installation and deployment schedule (including transition plan/project schedule) | County to confirm in writing the installation and deployment schedule, including the transition plan/project schedule, are provided and approve same, as described in section 3 – Technical Approach |
| 2. | Monthly installation reports | County to confirm monthly installation reports are provided and approve same, as described in section 4 – Managerial Approach and Communication |
| 3. | Traffic coordination plan | County to confirm the traffic coordination plan is provided and approve same, as described in section 4 – Managerial Approach and Communication |
| 4. | System access list | County to confirm the System access list is provided and approve same, as described in section 3 – Technical Approach |
| 5. | Training plan | County to confirm the Training plan is provided and approve same, as described in section 5 – Onsite Training |
| 6. | Training agenda and materials | County to confirm the Training agenda and materials are provided and approve same, as described in section 5 – Onsite Training |
| 7. | Test scripts for system testing & acceptance plan | County to confirm the test scripts and acceptance plan are provided and approve same, as described in section 7 – Final Acceptance Test Plan |

## 7. Final Acceptance Test Plan:

Provider will provide County with complete System performance testing scripts.

Exhibit 2

Preliminary Acceptance Testing

Preliminary acceptance testing will occur at each site after the Go-Live for each site. Provider will provide County with a set of testing scripts to perform testing of the System at each site. The testing scripts must, at a minimum, include the test items listed below. After all six (6) Phases are completed for each site and have successfully passed preliminary acceptance testing, Provider will notify County in writing that the System is ready for Final Acceptance Testing. Each site may run after site Go-Live independent of the other sites and prior to Final Acceptance Testing.

County's Contract Administrator will provide written Final Acceptance only upon successful completion of all the Final Acceptance Test Criteria stated below:

| No. | Deliverable | Final Acceptance Test Criteria | Pass/Fail |
|---|---|---|---|
| 1. | Server and database function | County to confirm the server and database functions as described in Section 3 – Technical Approach and the Documentation | |
| 2. | Automatic pay-on-foot stations (cash, coins, and credit card payments) | County to confirm the automatic pay-on-foot stations functions as described in Section 3 – Technical Approach and the Documentation | |
| 3. | Central pay-on-foot stations (credit card only payments) | County to confirm the central pay-on-foot stations functions as described in Section 3 – Technical Approach and the Documentation | |
| 4. | Merchant validation stickers/labels | County to confirm the merchant validation stickers/labels function as described in Section 3 – Technical Approach and the Documentation | |
| 5. | Payment tenders | County to confirm the payment tenders are accepted as described in Section 3 – Technical Approach and the Documentation | |
| 6. | System reporting functions | County to confirm the System provides accurate System reporting as described in Section 3 – Technical Approach and the Documentation | |
| 7. | Proximity readers | County to confirm the proximity readers function as described in Section 3 – Technical Approach and the Documentation | |
| 8. | Vehicle loop detectors | County to confirm the vehicle detectors function as described in Section 3 – Technical Approach and the Documentation | |
| 9. | Double stroke red X/green arrow sign | County to confirm the red X green arrow sign functions as described in Section 3 – Technical Approach and the Documentation | |

| No. | Deliverable | Final Acceptance Test Criteria | Pass/Fail |
|---|---|---|---|
| 10. | LED Signs for pay-on-foot stations | County to confirm the LED Signs for pay-on-foot stations function as described in Section 3 – Technical Approach and the Documentation | |
| 11. | Barrier gate arms | County to confirm the barrier gate arms function as described in Section 3 – Technical Approach and the Documentation | |
| 12. | Barcodes, QR codes, scanner functionality | County to confirm the Equipment successfully accepts and processes barcodes, QR codes, and scanner scans as described in Section 3 – Technical Approach and the Documentation | |
| 13. | Commend VoIP digital intercom | County to confirm the Commend VoIP digital intercom functions as described in Section 3 – Technical Approach and the Documentation | |
| 14. | Verify ability to integrate with third-party pay by phone vendor | County to confirm ability to integrate with third-party pay by phone application in the future | |
| 15. | License plate recognition and inventory system | County to confirm the license plate inventory system functions and reports accurate data as further described in Section 3 – Technical Approach and the Documentation | |
| 16. | Data Conversions | County to confirm data converted from existing PARCS system to the System during the installation process; data must be historically accurate and complete. | |

## 8. Optional Services, Additional Software/Licenses:

### A. Transition & Disentanglement Services

The Parties acknowledge and agree that upon the expiration or termination of this Agreement, the good faith efforts of Provider to facilitate the smooth, efficient, and secure transition of data and services to another provider (or to County, to the extent applicable) without any unnecessary interruption or adverse impact on County operations ("Disentanglement") is a critical objective of the Parties and a material obligation of Provider under this Agreement. All obligations of Provider under this Agreement shall be construed consistent with this objective.

At request of County, Provider shall provide prompt, good faith, and reasonable assistance County in disentangling County data, business, and operations from the Software and, to the extent applicable, transitioning to a new software, system, or provider.

B. Additional Software Licenses, Modules, Equipment/Hardware, and Services

County may purchase additional software subscriptions, modules, equipment/hardware, and services, including modifications or configurations of the System for specific County requirements, per an agreed upon Work Authorization under this Agreement. Such Work Authorization and corresponding Statement of Work shall detail, at a minimum, the work to be performed or software or equipment to be provided by Provider, as well as any costs, applicable timelines, and acceptance criteria for any such configurations. All optional services shall be performed per the rates set forth in Exhibit B – Payment Schedule. If no rates are set forth for the optional services, the Parties shall agree on the costs for the optional services and include as part of the Work Authorization. Optional services may include, but are not limited to, the following:

a. Additional training sessions (for advanced training topics)
b. Additional sites (ex. Northport garage)
c. County-specific project requirements, documentation, and deliverables that are not specifically identified in this Exhibit A – Statement of Work and are not directly associated with tasks required for Provider resources to deploy the System.
d. Pre-paid parking reservation system integration: Integration with Park Jockey, ParkMobile, Parking Panda, and Spot Hero pre-paid parking reservation systems
e. Integration with Click'n'Park or ParkWhiz (or other agreed upon third-party provider only after County enters into an agreement with County-chosen carrier; County to notify Provider upon contracting with applicable carrier); shall be done as no cost Work Authorization “”
f. Fee Computers
g. Uninterruptible power supply units (UPS)
h. SunPass functionality (via E5 antenna/transcore readers to enable reading of Florida Department of Transportation toll passes)
i. PGS level count system:
   - Midport garage space counting system
   - T2/T4 garage space counting system
j. ParkBlue
   - ParkBlue Bluetooth readers
   - ParkBlue Bluetooth modules to convert a smartphone to an access credential
   - Monthly SaaS charge for ParkBlue
   - White label APP option as an add-on
   - Monthly charges for full monthly/reservation pre-sell
k. Provider's INDECT space count system & matrix signage
l. Test bed: The test bed would reside in a designated area on County property. All System software will be loaded and demonstrated on the test bed before being loaded on the on-premise servers for deployment. SunPass integration or future upgrades may require a test bed.
m. SunPass integration

Exhibit 2
Page 45 of 105

n. Factory Acceptance Test (FAT): The FAT is an alternative to setting up a test bed. Provider would set up a sample lane of County equipment at Provider's corporate office location. Provider would fly a team of up to four (4) people to Columbus, Ohio for a week of running through an approved script of all the functionality required.

## Exhibit A Attachment 1 – Equipment List by Location

**Back Office Hardware and Software (Site 1)**

| Qty | **Equipment** *(by model number or other specific identification)* | **Description** |
|---|---|---|
| 2 | DL360 Gen10 4112 85W 1P 16G-2R P408i-a 8SFF | Rack Mounted Servers |
| 3 | XPS 8930 Desktop Computer | Desktop Workstations |
| 1 | GE 300 | Commend GE 300 VoIP Digital Intercom Module |

**Terminal 19 Surface Lot (Site 2)**

| Qty | **Equipment** *(by model number or other specific identification)* | **Description** |
|---|---|---|
| 6 | IB-0310-1004 | Uninterruptible Power Supply Units, (UPS) |
| 5 | IB-0305-1018 | Commend VoIP Digital Intercom Substation |
| 2 | MP-30-ENT TIBA | MP-30 Entry Lane Equipment |
| 5 | PB-TG1A-1004 | Arm Barrier Gate |
| 2 | LL-1034-1021 | Vehicle Detector |
| 1 | IB-0310-1029 | Network Switch |
| 3 | PM-SW3S-1006 | SW-30 Exit Lane Equipment |
| 1 | PM-CP3C-1002 | Central Pay-on-Foot Station, Credit Card Only |
| 1 | APS-30-POF-3 Note 1.8 | Automatic Pay-on-Foot Station, Cash, Coins, and Credit Card |
| 5 | TCL1818RG-175DS | Double Stroke Red X/Green Arrow Sign |
| 5 | REDVision 550; includes infared (X-LPR-VRS-N70-IR) and white light (X-LPR-VRS-N70-OV) cameras | LPR Cameras |

**Terminal 18 Surface Lot (Site 3)**

| Qty | **Equipment** *(by model number or other specific identification)* | **Description** |
|---|---|---|
| 6 | IB-0310-1004 | Uninterruptible Power Supply Units, (UPS) |
| 5 | IB-0305-1018 | Commend VoIP Digital Intercom Substation |
| 2 | MP-30-ENT TIBA | MP-30 Entry Lane Equipment (No Scanner) |
| 5 | PB-TG1A-1004 | Auto Barrier Gate |
| 2 | LL-1034-1021 | Vehicle Detector |
| 1 | IB-0310-1029 | Network Switch |
| 3 | PM-SW3S-1006 | SW-30 Exit Lane Equipment |
| 1 | PM-CP3C-1002 | Central Pay-on-Foot Station, Credit Card Only |
| 1 | APS-30-POF-3 Note 1.8 | Automatic Pay-on-Foot Station, Cash, Coins, and Credit Card |
| 3 | TCL1818RG-175DS | Double Stroke Red X/Green Arrow Sign |
| 5 | REDVision 550; includes infared (X-LPR-VRS-N70-IR) and white light (X-LPR-VRS-N70-OV) cameras | LPR Cameras |

**Midport Parking Garage (Site 4)**

| Qty | **Equipment** *(by model number or other specific identification)* | **Description** |
|---|---|---|
| 2 | TCL1442R-D849 | LED Sign, pay-on-foot equipment |
| 11 | IB-0310-1004 | Uninterruptible Power Supply Units, (UPS) |
| 11 | IB-0305-1018 | Commend VoIP Digital Intercom Substation |
| 2 | MP-30-ENT TIBA | MP-30 Entry Lane Equipment (No Scanner) |
| 7 | PB-TG1A-1004 | Arm Barrier Gate |
| 4 | IB-0405-2949 | Proximity Card Reader |
| 2 | LL-1034-1021 | Vehicle Detector |
| 2 | IB-0310-1029 | Network Switch |
| 5 | PM-SW3S-1006 | SW-30 Exit Lane Equipment |
| 4 | PM-CP3C-1002 | Central Pay-on-Foot Station, Credit Card Only |
| 2 | APS-30-POF-3 Note 1.8 | Automatic Pay-on-Foot Station, Cash, Coins, and Credit Card |
| 5 | TCL1818RG-175DS | Double Stroke Red X/Green Arrow Sign |
| 7 | REDVision 550; includes infared (X-LPR-VRS-N70-IR) and white light (X-LPR-VRS-N70-OV) cameras | LPR Cameras |

**T2/T4 Parking Garage (Site 5)**

| Qty | **Equipment** *(by model number or other specific identification)* | **Description** |
|---|---|---|
| 5 | TCL1442R-D849 | LED Sign, pay-on-foot equipment |
| 11 | IB-0310-1004 | Uninterruptible Power Supply Units, (UPS) |
| 6 | IB-0305-1018 | Commend VoIP Digital Intercom Substation |
| 3 | MP-30-ENT TIBA | MP-30 Entry Lane Equipment (No Scanner) |
| 6 | PB-TG1A-1004 | Arm Barrier Gate |
| 2 | IB-0405-2949 | Proximity Card Reader |
| 3 | LL-1034-1021 | Vehicle Detector |
| 2 | IB-0310-1029 | Network Switch |
| 3 | PM-CP3C-1002 | Central Pay-on-Foot Station, Credit Card Only |
| 2 | APS-30-POF-3 Note 1.8 | Automatic Pay-on-Foot Station, Cash, Coins, and Credit Card |
| 3 | PM-SW3S-1006 | SW-30 Exit Lane Equipment |
| 6 | TCL1818RG-175DS | Double Stroke Red X/Green Arrow Sign |
| 6 | REDVision 550; includes infared (X-LPR-VRS-N70-IR) and white light (X-LPR-VRS-N70-OV) cameras | LPR Cameras |

## Exhibit B – Payment Schedule

The rates specified below shall be in effect for the entire term of the Agreement, including any renewal term, unless the contrary is expressly stated below. Any goods or services required under this Agreement for which no specific fee or cost is expressly stated in this Payment Schedule shall be deemed to be included, at no extra cost, within the costs and fees expressly provided for in this Exhibit B (inclusive of Attachment 1 to Exhibit B).

**Payment Milestones**

Contractor shall invoice for the Services performed pursuant this Agreement per the Payment Milestones listed below. Each Payment Milestone may only be invoiced upon County written notice of preliminary acceptance of the applicable Payment Milestone, except for the final Payment Milestone (Final Acceptance), which may only be invoiced upon County written notice of Final Acceptance.

| | |
|---|---|
| **Payment Milestone #1A** | |
| Effective Date | $400,000.00 |
| **Payment Milestone #1B** | |
| 30 days after Effective Date | $400,000.00 |
| **Payment Milestone #2*** | |
| County written notice of Preliminary Acceptance Terminal 19 and Terminal 18 and Go-Live at both sites | $317,191.00 |
| **Payment Milestone #3*** | |
| County written notice of Preliminary Acceptance of Midport Garage and Go-Live at site | $317,191.00 |
| **Payment Milestone #4**** | |
| County written notice of Preliminary Acceptance of T2/T4 Garage and Go-Live at site; County issuance of written Final Acceptance of System; written approval by both Parties of Installation Credit | $401,737.47 minus the Installation Credit (if any) |
| **Total (not to exceed):** | **$1,836,119.47** |

*For Payment Milestones 2 and 3, Provider will invoice County the set fee listed above. Along with such invoice, Provider must include, regardless of the dollar amount: (1) a detailed breakdown of all labor hours actually incurred on the applicable Milestone, (and associated labor rates) and the applicable category per Attachment 1 to this Exhibit B; (2) a detailed breakdown of all materials utilized by Provider on the applicable Milestone (e.g., number of feet of conduit; number of lanes; number of feet of fiber), including the applicable category per Attachment 1; and (3) breakdown of all items not specified in (1) and (2) but included in Attachment 1 to this Exhibit B, and justification for the fees. County may request additional information upon receipt of an invoice prior to County paying such invoice.

**For Payment Milestone 4, Provider will include with the invoice: (1) a detailed breakdown of all labor hours actually incurred on the applicable Milestone (and associated labor rates), and the applicable category per Attachment 1; (2) a detailed breakdown of all materials utilized by Provider on the applicable Milestone (e.g., number of feet of conduit; number of lanes; number of feet of fiber), including the applicable category per Attachment 1 to this Exhibit B; and (3) breakdown of all items not specified in (1) and (2) but included in Attachment 1 to this Exhibit B, and justification for the fees. County may request additional information upon receipt of an invoice prior to County paying such invoice.

Installation Credit: To the extent the detailed information for Milestones 2, 3, and 4, as determined by the Contract Administrator, does not substantiate labor hours, material, and other items included in Attachment 1, the Installation Credit shall be the difference between the "Installation Total" listed below (i.e., $688,491.00) and the total amount substantiated by the detailed information for Milestones 2, 3 and 4.

**Equipment Fees (for informational purposes only; Provider will only invoice County as set forth in the Payment Milestones above)**

| Qty | Description | Equipment Model [Back Office Hardware – Site #1] | Unit Price | Total Price |
|---|---|---|---|---|
| 2 | Rack Mounted Servers | DL360 Gen10 4112 85W 1P 16G-2R P408i-a 8SFF | $3,340.00 | $6,680.00 |
| 3 | Desktop Workstations | XPS 8930 Desktop Computer | $1,155.00 | $3,465.00 |
| 1 | Commend GE 300 VoIP Digital Intercom Module | IB-0305-1021 | $3,530.80 | $3,530.80 |
| **Qty** | **Description** | **Equipment Model [Terminal 19 Surface Lot – Site #2]** | **Unit Price** | **Total Price** |
| 6 | Uninterruptible Power Supply Units, (UPS) | IB-0310-1004 | $2,587.11 | $15,522.66 |
| 5 | Commend VoIP Digital Intercom Substation | IB-0305-1018 | $619.78 | $3,098.90 |
| 2 | MP-30 Entry Lane Equipment (No Scanner) | MP-30-ENT TIBA | $9,013.30 | $18,026.60 |
| 5 | Arm Barrier Gate | PB-TG1A-1004 | $3,028.35 | $15,141.75 |
| 2 | Vehicle Detector | LL-1034-1021 | $750.00 | $1,500.00 |
| 1 | Network Switch | IB-0310-1029 | $500.00 | $500.00 |
| 3 | SW-30 Exit Lane Equipment (CC Only) | PM-SW3S-1006 | $12,876.30 | $38,628.90 |
| 1 | Central Pay-on-Foot Station, Credit Card Only | PM-CP3C-1002 | $13,146.00 | $13,146.00 |
| 1 | Automatic Pay-on-Foot Station, Cash, Coins, and Credit Card | APS-30-POF-3 Note 1.8 | $29,669.32 | $29,669.32 |
| 5 | Double Stroke Red X/Green Arrow Sign | TCL1818RG-175DS | $700.00 | $3,500.00 |
| 5 | LPR Cameras | REDVision 550; includes infared (X-LPR-VRS-N70-IR) and white light (X-LPR-VRS-N70-OV) cameras | $10,500.00 | $52,500.00 |

Exhibit 2

| Qty | Description | Equipment Model [Terminal 18 Surface Lot – Site #3] | Unit Price | Total Price |
|---|---|---|---|---|
| 6 | Uninterruptible Power Supply Units, (UPS) | IB-0310-1004 | $2,587.11 | $15,522.66 |
| 5 | Commend VoIP Digital Intercom Substation | IB-0305-1018 | $619.78 | $3,098.90 |
| 2 | MP-30 Entry Lane Equipment (No Scanner) | MP-30-ENT TIBA | $9,013.30 | $18,026.60 |
| 5 | Barrier Gate | PB-TG1A-1004 | $3,028.35 | $15,141.75 |
| 2 | Vehicle Detector | LL-1034-1021 | $750.00 | $1,500.00 |
| 1 | Network Switch | IB-0310-1029 | $500 | $500 |
| 3 | SW-30 Exit Lane Equipment | PM-SW3S-1006 | $12,876.30 | $38,628.90 |
| 1 | Central Pay-on-Foot Station, Credit Card Only | PM-CP3C-1002 | $13,146.00 | $13,146.00 |
| 1 | Automatic Pay-on-Foot Station, Cash, Coins, and Credit Card | APS-30-POF-3 Note 1.8 | $29,669.32 | $29,669.32 |
| 3 | Double Stroke Red X/Green Arrow Sign | TCL1818RG-175DS | $700.00 | $2,100.00 |
| 5 | LPR Cameras | REDVision 550; includes infared (X-LPR-VRS-N70-IR) and white light (X-LPR-VRS-N70-OV) cameras | $10,500.00 | $52,500.00 |
| **Qty** | **Description** | **Equipment Model [Midport Parking Garage – Site #4]** | **Unit Price** | **Total Price** |
| 2 | LED Sign, pay-on-foot equipment | TCL1442R-D849 | $1,680.00 | $3,360.00 |
| 11 | Uninterruptible Power Supply Units, (UPS) | IB-0310-1004 | $2,587.11 | $28,458.21 |
| 11 | Commend VoIP Digital Intercom Substation | IB-0305-1018 | $619.78 | $6,817.58 |
| 2 | MP-30 Entry Lane Equipment (No Scanner) | MP-30-ENT TIBA | $9,013.30 | $18,026.60 |
| 7 | Arm Barrier Gate | PB-TG1A-1004 | $3,028.35 | $21,198.45 |
| 4 | Proximity Card Reader | IB-0405-2949 | $395.00 | $1,580.00 |
| 2 | Vehicle Detector | LL-1034-1021 | $750.00 | $1,500.00 |
| 2 | Network Switch | IB-0310-1029 | $500.00 | $1,000.00 |
| 5 | SW-30 Exit Lane Equipment | PM-SW3S-1006 | $12,876.30 | $64,381.50 |
| 4 | Central Pay-on-Foot Station, Credit Card Only | PM-CP3C-1002 | $13,146.00 | $52,584.00 |
| 2 | Automatic Pay-on-Foot Station, Cash, Coins, and Credit Card | APS-30-POF-3 Note 1.8 | $29,669.32 | $59,338.64 |
| 5 | Double Stroke Red X/Green Arrow Sign | TCL1818RG-175DS | $700.00 | $3,500.00 |

Exhibit 2

| | | | | |
|---|---|---|---|---|
| 7 | LPR Cameras | REDVision 550; includes infared (X-LPR-VRS-N70-IR) and white light (X-LPR-VRS-N70-OV) cameras | $9,500.00 | $66,500.00 |

| Qty | Description | Equipment [T2/T4 Parking Garage – Site #5] | Unit Price | Total Price |
|---|---|---|---|---|
| 5 | LED Sign, pay-on-foot equipment | TCL1442R-D849 | $1,680.00 | $8,400.00 |
| 11 | Uninterruptible Power Supply Units, (UPS) | IB-0310-1004 | $2,587.11 | $28,458.21 |
| 6 | Commend VoIP Digital Intercom Substation | IB-0305-1018 | $619.78 | $3,718.68 |
| 3 | MP-30 Entry Lane Equipment (No Scanner) | MP-30-ENT TIBA | $9,013.30 | $27,039.90 |
| 6 | Arm Barrier Gate | PB-TG1A-1004 | $3,028.35 | $18,170.10 |
| 2 | Proximity Card Reader | IB-0405-2949 | $395.00 | $790.00 |
| 3 | Vehicle Detector | LL-1034-1021 | $750.00 | $2,250.00 |
| 2 | Network Switch | IB-0310-1029 | $500.00 | $1,000.00 |
| 3 | SW-30 Exit Lane Equipment | PM-SW3S-1006 | $12,876.00 | $38,628.90 |
| 3 | Central Pay-on-Foot Station, Credit Card Only | PM-CP3C-1002 | $13,146.00 | $39,438.00 |
| 2 | Automatic Pay-on-Foot Station, Cash, Coins, and Credit Card | APS-30-POF-3 Note 1.8 | $29,669.32 | $59,338.64 |
| 6 | Double Stroke Red X/Green Arrow Sign | TCL1818RG-175DS | $700.00 | $4,200.00 |
| 6 | LPR Cameras | REDVision 550; includes infared (X-LPR-VRS-N70-IR) and white light (X-LPR-VRS-N70-OV) cameras | $9,500.00 | $57,000.00 |

**Software Fees** (for informational purposes only; Provider will only invoice County per the Payment Milestones above)

| Software Description | License Term | Invoicing | Fees |
|---|---|---|---|
| TIBA SmartPark Application Software | Perpetual | Part of final payment | $119,819.00 |

**Implementation Services Fees** (for informational purposes only; Provider will only invoice County per the Payment Milestones above)

| Description | Invoicing | Fees |
|---|---|---|
| Removal and Disposal of Existing Equipment | Per Payment Milestones Above | $16,388.00 |
| Installation Total (see Attachment 1 for further breakdown) | Per Payment Milestones Above | $688,491.00 |

**Support and Maintenance Services**

| Specific Support and Maintenance Services | Unit or Term | Invoicing | Annual Fee |
|---|---|---|---|
| Support and Maintenance Services per Exhibit C | Year 1 after Final Acceptance | N/A | No cost |
| Support and Maintenance Services per Exhibit C | Year 2 after Final Acceptance | Quarterly in arrears | $103,722 |
| Support and Maintenance Services per Exhibit C | Year 3 after Final Acceptance | Quarterly in arrears | $106,834 |
| Support and Maintenance Services per Exhibit C | Year 4 after Final Acceptance | Quarterly in arrears | $110,039 |
| Support and Maintenance Services per Exhibit C | Year 5 after Final Acceptance | Quarterly in arrears | $113,340 |

Any travel expenses or fees incurred by Provider under this Agreement shall be the sole responsibility of Provider, unless otherwise expressly stated in this Agreement or applicable Work Authorization.

Provider may increase the annual fees for Support and Maintenance Services above for each optional year after the Initial Term of the Agreement, provided that: (1) the percentage increase in the annual Support and Maintenance Services Fee shall not exceed the lesser of (i) three percent (3%) per annum, or (ii) the percentage increase in the “CPI” (as hereinafter defined) for the yearly period ending six months prior to the renewal year for which the increase applies, and (2) Provider provides written notice to County of any such increase not less than sixty (60) calendar days prior to the end of the then current term. The “CPI” shall be the unadjusted percent change to the Miami-Fort Lauderdale Consumer Price Index for all urban consumers, all items (1982-1984=100), as published by the Bureau of Labor Statistics, Southeastern Regional Office. The new rate may not be less than the current year rate. All such contract adjustments shall be made on an annual basis.

**Optional Services or Additional Software/Licenses**

| Description | Unit/Term | Invoicing | Fee |
|---|---|---|---|
| Consulting (including Transition & Disentanglement Services) | Hourly | Monthly in arrears | $300.00 per hour |
| Additional Training | Hourly | Monthly in arrears | $150.00 per hour |
| INDECT Sensor Level Count PGS System – Northport Garage | One-Time Fee | Upon Final Acceptance | Per applicable Work Authorization |
| INDECT Sensor Level Count PGS System – Midport Garage | One-Time Fee | Upon Final Acceptance | Per applicable Work Authorization |

All equipment listed under the section titled “**Equipment Fees (for informational purposes only; Provider will only invoice County as set forth in the Payment Milestones above)**” may be purchased by County as Optional Services as the “Unit Price” rates set forth above for the duration of the Agreement.

| Additional Optional Hardware Devices and Software | Unit Price (all qty 1 unless otherwise indicated) |
|---|---|
| ParkBlue Bluetooth Readers ($600 Hardware/$400 Install) | $1,000.00 |
| Monthly SaaS Charge for ParkBlue | $50.00 |
| White Label APP Option | $18,000.00 |
| Monthly hosting charges for White Lable APP Option | $125.00 |
| License Plate Recognition Cameras (LPR) | $9,500.00 |
| LED Sign, Equipment – POF | $1,680.00 |
| Uninterruptible Power Supply Units, (UPS) Office | $595.00 |
| Uninterruptible Power Supply Units, (UPS) Entry/Exit Lanes | $2,587.11 |
| VoIP Substation – Commend | $619.78 |
| Entry Lane Equipment - MP -30 | $9,013.30 |
| Exit Lane Equipment - SW 30 | $12,876.30 |
| Barrier Gate | $3,028.35 |
| Hand-Held Computers | $4,269.62 |
| Additional Straight Arms | $150.00 |
| Pay-on-Foot Station, Credit Card Only | $13,146.00 |
| Pay-on-Foot Station, Cash and Credit Card | $29,669.32 |
| Sunpass Reader | $21,770.00 |
| Double Stroke Red X Green Arrow Sign | $700.00 |
| Fee Computer | $6,510.00 |
| Hardware/Warranty Contingencies | $75,000.00 |

## Exhibit B - Attachment 1

| Task (Electrical Installation) | Qty | Unit Price | Total Price |
|---|---|---|---|
| Bore and install 1" conduit for 17 lanes (no conduit required at T2/T4). Provide and install handholds 12"x12"x 12". Utilizing existing conduit where applicable. | 1,600 feet | $18.00/ft | $28,800.00 |
| Saw cutting for 3 induction loops per lane; includes price for above ground loops at T2/T4 garage. | 69 lanes | $1,500.00/lane | $103,500.00 |
| Install 1' conduit above ground for POF machines (Parties to negotiate Work Authorization if boring required) | 1,100 feet | $12.50/ft | $13,750.00 |
| 5 or 6 strand OS2 armored fiber cable (run and install) | 7,500 feet | $16.00/ft | $120,000.00 |
| Terminate fiber and test. Includes the cost for termination of the fiberstrand. | 5 | $1,840.00 | $9,200.00 |
| Concrete Work per lane | 10 lanes | $4,000.00/lane | $40,000.00 |
| Certified Professional Drawings (full set) | 1 set | $35,000.00/set (estimated) | $35,000.00 |
| Permitting through Broward/Ft. Lauderdale and Hollywood | N/A | $3,866.00 (estimated) | $3,866.00 |
| Installation for conduit, cable runs and materials (includes termination of power and end to end testing) | 445 hours | $95.00/hour | $42,275.00 |
| | | **Total** | **$396,391.00** |
| **Task (Non-Electrical Installation)** | **Qty** | **Unit Price** | **Total Price** |
| Installation of Equipment and non-electrical cabling. Termination and end to end testing. Includes materials. | 490 hours | $95.00/hour | $46,550.00 |
| Cat 6 Cabling | 7,200 feet | $19.00/ft | $136,800.00 |
| Conduct Acceptance testing | N/A | N/A | $13,000.00 |
| Installation and configuring of IT Back office Equipment and Software | N/A | N/A | $25,900.00 |
| Training; per agreement | 40 hours | $150.00/hour | $6,000.00 |
| Training materials, Operating Manuals, Cut Sheets and Syllabus | N/A | N/A | $4,000.00 |
| Rate programming and reporting configuration per client specification | N/A | N/A | $14,850.00 |
| Project Management | N/A | N/A | $45,000.00 |
| | | **Total** | **$292,100.00** |

## Exhibit C - Support and Maintenance Services

### 1. System Support and Maintenance Services

Provider shall provide County with Support and Maintenance Services so as to ensure and maintain optimal performance of the System consistent with the Statement of Work and the Documentation, which service shall include the following:

- Timely response and resolution of any errors, defects, malfunctions or other issues affecting the use or performance of the System (collectively, "Events") in keeping with the Required Response Times stated below;
- Providing and facilitating the installation of updates, upgrades and releases as they are made available to Provider's other clients;
- Notification of patches and updates affecting security, and applying, testing, and validating the appropriate patches and updates and/or workarounds on a test version of the application before distribution.
- On-call availability via telephone and e-mail during normal business hours to receive and respond to inquiries or questions from County regarding use, operation, or functionality of the System;
- Emergency availability via telephone and e-mail after hours to receive and respond to specific technical problems and questions relating to the operation or functionality of the System;
- Use of ongoing best efforts to maintain the optimal functioning of the Software, to correct programming and coding errors, and to provide solutions to known errors affecting the operation of the System;
- Routine notification to County as it becomes available of new or updated information pertaining to the System and the Documentation.

Support and Maintenance Services shall be provided via telephone, electronic communication, on-site, or as otherwise appropriate to address the issue. Any update, upgrades, releases, or other modifications to the Software shall be provided via electronic communication and for download via the Internet, if practicable. To the extent necessary to resolve an Event or other support request, Provider shall provide support on-site at any office or location of a Broward County agency. Provider agrees that its personnel shall be suitably trained in the operation, support and maintenance of the Software and System. If in the reasonable opinion of County, the personnel provided are not acceptable, Provider agrees to provide suitable replacements.

Required Response Times. Upon notice by County of an Event, Provider shall address and resolve the Event consistent with the following priority, response and resolution levels:

| Priority Description | Definition | Response Time After Notice | Resolution Time after Notice |
|---|---|---|---|
| Critical | Event that renders the System and/or interfaces inoperable or allows unauthorized access. | 1 hour | Work until corrected |
| Severe | Event that results in a significant impairment of performance of the System or impairs essential operations or allows unauthorized access. | 1 hour | Work until corrected during normal business hours |
| Minor | Event that has minor impact to County's business and that does not impact normal operation of the System. | 2 hours during normal business hours; or next business day if outside of normal business hours | Future patch or release |
| Minimal | Event that has minimal impact or no impact on County's business. | 2 hours during normal business hours; or next business day if outside of normal business hours | Future release |

Notwithstanding the above-stated schedule, Provider shall use its continuing best efforts to correct the Event as expeditiously as it can. The Priority Description for each error or issue shall be reasonably determined by the Contract Administrator.

Records and Reports. Provider will maintain records of its Support and Maintenance Services, and provide County with online access to an Event ticketing system, which shall include at least the following:

a) Date, time, and name of contact for each Event;
b) Date and time of response by Provider;
c) Description of Event and analysis of error, defect, or other issue causing Event;
d) All steps and actions taken to resolve the Event;
e) Date and time of resolution and County representative notified of resolution; and
f) All equipment and/or labor costs associated with resolution.

At the request of County, Provider shall provide monthly reports of the foregoing records as well as statistics of Provider's average monthly compliance with the Required Response Times.

Failure to Meet Required Response Times. If Provider fails to meet the Required Response Times, County may offset against any sums due Provider up to 25% for each hour that Provider's average response time in the preceding month exceeds the Required Response Times, which the Parties agree is a fair and reasonable approximation of County's negative financial impact caused by the delay in Provider's response.

DownTime Maintenance Credit. If a Severe or Critical Event is not resolved or reduced to Minor or Minimal priority level within two (2) hours after notice to Provider, Provider will refund to

Exhibit 2

County five percent (5%) of the monthly fee (or monthly pro rata equivalent, if the fee is other than monthly) for Support and Maintenance Services for each additional business hour that the Event remains unresolved or at the Severe or Critical priority level. Such refunds will be paid within 10 days or, at County's option, may be credited against future sums due to Provider. This refund shall be in addition to any other remedy that is available in the event of a breach of the Agreement.

Hours of Service. Throughout the life of the Agreement, Provider shall furnish maintenance service as needed by County (including, to the extent required, on-site at any office or location of a Broward County agency) twenty-four (24) hours a day, seven (7) days a week, including holidays.

## 2. Equipment Support and Services

Provider shall provide both repair service and routine maintenance to the extent necessary in order to ensure continuous optimal functioning of the Equipment for the duration of the Agreement. Provider's support and maintenance obligations include on-site maintenance at any office or location of a Broward County agency, although to the extent reasonable and customary under the circumstances, Provider may provide services electronically.

For repair requests, Regular Response Times as indicated herein shall apply unless critical County operations are affected or County indicates the repair request is an emergency, in which event the Emergency Service Times shall apply. When the Equipment cannot be repaired on-site and/or if Provider cannot meet the required response times, a replacement component shall be provided and installed by Provider prior to the start of the next County work day, which replacement component must be of equal or better performance and compatible with County's existing systems. Notwithstanding the response time requirements, Provider shall use its continuing best efforts to correct any issue as expeditiously as it can.

Provider will ensure that it maintains adequate stock levels to assure timely delivery of any components that may require maintenance or repair. Provider agrees that its maintenance personnel shall be suitably trained in the operation of the Equipment and associated software and firmware. If, in the reasonable opinion of County, the personnel provided are not acceptable, Provider agrees to provide suitable replacements.

Telephone and Email Support. Provider shall provide designated contacts for telephone and email support that will be available during regular County business hours and after hours for specific technical problems and questions.

Routine Maintenance. Routine maintenance provided by Provider shall include the periodic cleaning, adjusting, calibrating, system diagnostics, and fine tuning of the Equipment; replacement or repair of worn parts; prompt installation of any updates, upgrades, or releases of embedded software or firmware; and component replacement with equal or better equipment with the approval of the Contract Administrator when the component is approaching the end of its useful life. Provider shall perform routine maintenance on at least a monthly basis (or more

Exhibit 2

frequently if appropriate as a result of equipment usage or standards set by the Equipment manufacturer). Provider shall contact the end user agency at least three (3) business days prior to arrival for the performance of routine maintenance.

Repair Service. Repair service includes prompt response and resolution of any repair request within the applicable Response Time, which includes identifying the cause of malfunction or problem; provision of any applicable temporary solutions or workarounds until repair can be completed; permanent repair of the problem; correction, to the extent necessary, of any repercussions of the problem; and thorough inspection of the Equipment post-repair to ensure optimal functioning of the Equipment.

Regular Response Times. Provider shall provide response times as follows from the time Provider receive a repair request from County (calculated according to regular business hours): two (2) hour telephone response, four (4) hour local arrival time (or networked access, if applicable), and eight (8) hour resolution time. All systems are to operate to the user's satisfaction within eight (8) business hours of the initial call to Provider.

Emergency Service Time: Emergency repairs shall be provided within two (2) hours of County's repair request and Provider's repair efforts shall continue without interruption until the issue is resolved. Emergency repairs will be authorized by the Contract Administrator if critical County operations are affected, and shall include whatever action is necessary to return the System's operation to a level that satisfies the user.

# Exhibit D – Minimum Insurance Requirements

**Project:** Parking access and revenue control system replacement
**Agency:** Port Everglades

| TYPE OF INSURANCE | ADDL INSD | SUBR WVD | MINIMUM LIABILITY LIMITS | | |
|---|---|---|---|---|---|
| | | | | **Each Occurrence** | **Aggregate** |
| **GENERAL LIABILITY - Broad form**<br>☑ Commercial General Liability<br>☑ Premises–Operations<br>☑ XCU Explosion/Collapse/Underground<br>☑ Products/Completed Operations Hazard<br>☑ Contractual Insurance<br>☑ Broad Form Property Damage<br>☑ Independent Contractors<br>☑ Personal Injury<br>**Per Occurrence or Claims-Made:**<br>☑ Per Occurrence □ Claims-Made<br>**Gen'l Aggregate Limit Applies per:**<br>□ Project □ Policy □ Loc. □ Other _______ | ☑ | ☑ | Bodily Injury | | |
| | | | Property Damage | | |
| | | | Combined Bodily Injury and Property Damage | **$ 1 mil** | **$ 2 mil** |
| | | | Personal Injury | | |
| | | | Products & Completed Operations | | |
| | | | | | |
| **AUTO LIABILITY**<br>☑ Comprehensive Form<br>☑ Owned<br>☑ Hired<br>☑ Non-owned<br>☑ Any Auto, If applicable<br>*Note: May be waived if no driving will be done in performance of services/project.* | ☑ | ☑ | Bodily Injury (each person) | | |
| | | | Bodily Injury (each accident) | | |
| | | | Property Damage | | |
| | | | Combined Bodily Injury and Property Damage | **$ 500 k** | |
| ☑ **EXCESS LIABILITY / UMBRELLA**<br>**Per Occurrence or Claims-Made:**<br>□ Per Occurrence □ Claims-Made<br>***Note: May be used to supplement minimum liability coverage requirements.*** | ☑ | ☑ | | **$ Optional** | |
| ☑ **WORKER'S COMPENSATION**<br>*Note: U.S. Longshoremen & Harbor Workers' Act & Jones Act is required for any activities on or about navigable water.* | N/A | ☑ | Each Accident | **STATUTORY LIMITS** | |
| ☑ **EMPLOYER'S LIABILITY** | | | Each Accident | **$ 500 k** | |
| ☐ **POLLUTION / ENVIRONMENTAL LIABILITY** | ☑ | ☑ | If claims-made form: | $ | |
| | | | Extended Reporting Period of: | 2 years | |
| | | | *Maximum Deductible: | | |
| ☐ **PROFESSIONAL LIABILITY (ERRORS & OMISSIONS)**<br>**All engineering, surveying and design professionals.** | N/A | ☑ | If claims-made form: | **$ 1 mil per occurrence** | |
| | | | Extended Reporting Period of: | 2 years | |
| | | | *Maximum Deductible: | $50,000 | |
| ☐ Installation floater is required if Builder's Risk or Property are not carried.<br>*Note: Coverage must be "All Risk", Completed Value.* | | | *Maximum Deductible (Wind and/or Flood): | Not to exceed 5% of completed value | **Completed Value** |
| | | | *Maximum Deductible: | $10 k | |

<u>Description of Operations</u>: "Broward County" shall be listed as Certificate Holder and endorsed as an additional insured for liability, except as to Professional Liability. County shall be provided 30 days written notice of cancellation, 10 days' notice of cancellation for non-payment. Contractors insurance shall provide primary coverage and shall not require contribution from the County, self-insurance or otherwise. Any self-insured retention (SIR) higher than the amount permitted in this Agreement must be declared to and approved by County and may require proof of financial ability to meet losses. Contractor is responsible for all coverage deductibles unless otherwise specified in the agreement.

**CERTIFICATE HOLDER:**

Broward County
115 South Andrews Avenue
Fort Lauderdale, Florida 33301

Attention: Angela Osorno-Belleme

09/17/18
Risk Management Division

## Exhibit E – Work Authorization Form

**WORK AUTHORIZATION FOR AGREEMENT ____________________**

**______________________________________________________________**

Contract Number: ________________
Work Authorization No. ___________

This Work Authorization is between Broward County and _________________ ("Provider") pursuant to the Agreement, executed on _____________________. In the event of any inconsistency between this Work Authorization and the Agreement, the provisions of the Agreement shall govern and control.

**Services to be provided:** [DESCRIBE IN DETAIL]

Agreement at issue is __ Lump Sum/ __Not-to-Exceed for amount: $____________________

The time period for this Work Authorization will be from the date of complete execution until ____ (___) days after County's Notice to Proceed for the Services to be provided under this Work Authorization, unless otherwise extended or terminated by the Contract Administrator.

**Fee Determination:** Payment for services under this Work Authorization is as follows:

| | |
|---|---|
| Professional Services | $____________________ |
| General Services | $____________________ |
| Goods/Equipment | $____________________ |
| Total Cost of this Work Authorization | $____________________ |

The foregoing amounts shall be invoiced by Provider upon written acceptance by County of all goods and services provided under this Work Authorization.

**County**

Contract Administrator Date

Project Manager Date

Board and/or Designee Date

**Provider**

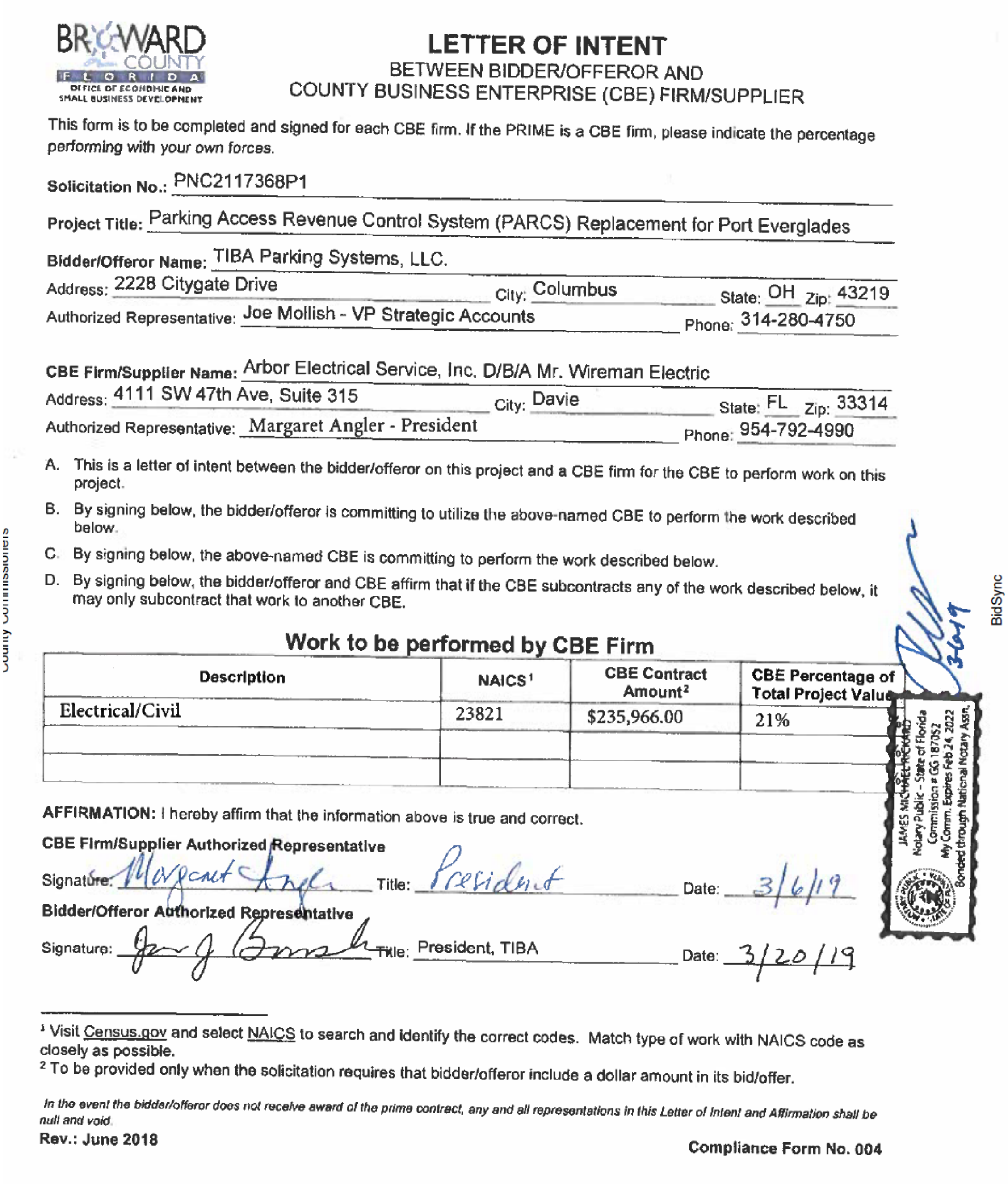
Signed Date

Attest

Typed Name

Title

## Exhibit F CBE Subcontractor Schedule and Letters of Intent



BROWARD COUNTY FLORIDA
OFFICE OF ECONOMIC AND SMALL BUSINESS DEVELOPMENT

# LETTER OF INTENT

BETWEEN BIDDER/OFFEROR AND
COUNTY BUSINESS ENTERPRISE (CBE) FIRM/SUPPLIER

This form is to be completed and signed for each CBE firm. If the PRIME is a CBE firm, please indicate the percentage performing with your own forces.

**Solicitation No.:** PNC2117368P1

**Project Title:** Parking Access Revenue Control System (PARCS) Replacement for Port Everglades

**Bidder/Offeror Name:** TIBA Parking Systems, LLC.

Address: 2228 Citygate Drive City: Columbus State: OH Zip: 43219

Authorized Representative: Joe Mollish - VP Strategic Accounts Phone: 314-280-4750

**CBE Firm/Supplier Name:** Arbor Electrical Service, Inc. D/B/A Mr. Wireman Electric

Address: 4111 SW 47th Ave, Suite 315 City: Davie State: FL Zip: 33314

Authorized Representative: Margaret Angler - President Phone: 954-792-4990

A. This is a letter of intent between the bidder/offeror on this project and a CBE firm for the CBE to perform work on this project.

B. By signing below, the bidder/offeror is committing to utilize the above-named CBE to perform the work described below.

C. By signing below, the above-named CBE is committing to perform the work described below.

D. By signing below, the bidder/offeror and CBE affirm that if the CBE subcontracts any of the work described below, it may only subcontract that work to another CBE.

3-6-19

### Work to be performed by CBE Firm

| Description | NAICS[1] | CBE Contract Amount[2] | CBE Percentage of Total Project Value |
|---|---|---|---|
| Electrical/Civil | 23821 | $235,966.00 | 21% |
| | | | |
| | | | |

JAMES MICHAEL RICKARD
Notary Public – State of Florida
Commission # GG 187052
My Comm. Expires Feb 24, 2022
Bonded through National Notary Assn.
NOTARY PUBLIC • STATE OF FLORIDA

**AFFIRMATION:** I hereby affirm that the information above is true and correct.

**CBE Firm/Supplier Authorized Representative**

Signature: Margaret Angler Title: President Date: 3/6/19

**Bidder/Offeror Authorized Representative**

Signature: Title: President, TIBA Date: 3/20/19

[1] Visit Census.gov and select NAICS to search and identify the correct codes. Match type of work with NAICS code as closely as possible.

[2] To be provided only when the solicitation requires that bidder/offeror include a dollar amount in its bid/offer.

*In the event the bidder/offeror does not receive award of the prime contract, any and all representations in this Letter of Intent and Affirmation shall be null and void.*

**Rev.: June 2018**

**Compliance Form No. 004**

## Exhibit G Port Security Requirements

A. The Port Everglades Department requires persons to present, at port entry, a valid driver's license, and valid reason for wishing to be granted port access in order to obtain a temporary/visitor ID badge. For persons who will visit the Port more than 15 times in a 90 day period, a permanent identification badge must be obtained and paid for by the contractor for all employees, subcontractors, agents and servants visiting or working on the port project. A restricted access badge application process will include fingerprints and a comprehensive background check. Badges must be renewed annually and the fees paid pursuant to Broward County Administrative Code, Section 42.6. For further information, please call 954-765-4225.

B. All vehicles that are used regularly on the dock apron must have a Dockside Parking Permit. Only a limited number of permits will be issued per business entity. The fee is $100.00 per permit/vehicle. Individuals requesting a permit must possess a valid Port-issued Restricted Access Area badge with a "Dock" destination. Requests for Dockside Parking Permits must be submitted in writing, on company letterhead, to the ID Badge Office. Applicants must demonstrate a need for access to the dock apron. Requests shall be investigated, and approved, if appropriate justification is provided. Supporting documentation must be supplied, if requested. Dock permits are not transferable and must be affixed to the lower left corner of the permitted vehicle's windshield. Should the permit holder wish to transfer the permit to another vehicle during the term of issuance, the permit will be removed and exchanged at no charge for a new permit. Only one business entity representative will be permitted on the dock at a time at the vessel location.

C. The Federal Government has instituted requirements for a Transportation Worker Identification Credential (TWIC) for all personnel requiring unescorted access to designated secure areas within Port Everglades. The contractor will be responsible for complying with the applicable TWIC requirements. For further information, please call 1- 855-347-8371, or go on line to https://www.tsa.gov/for-industry/twic.

## Exhibit H – PCI Responsibility Matrix

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 1.1 | Establish and implement firewall and router configuration standards that include the following: | | X | | | TIBA Provides a Firewall between the server and the network connection. |
| 1.1.1 | A formal process for approving and testing all network connections and changes to the firewall and router configurations | | | | X | TIBA will test its Network connections and adjust its Firewall and Router based on the County's or its operator's need or changes. |
| 1.1.2 | Current diagram that identifies all networks, network devices, and system components, with all connections between the CDE and other networks, including any wireless networks | | | | X | TIBA will provide a diagram of its Network and will need a master network design from the County to ensure that Parking Network is |
| 1.1.3 | Current diagram that shows all cardholder data flows across systems and networks | | X | | | TIBA and Payment Express will provide a diagram of for credit card transactions. |
| 1.1.4 | Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone | X | | | | |
| 1.1.5 | Description of groups, roles, and responsibilities for management of network components | | | X | | Through Parking Management company. |
| 1.1.6 | Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. | | X | | | |
| 1.1.7 | Requirement to review firewall and router rule sets at least every six months | | | | X | |
| 1.2 | Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.<br>Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage. | | | X | | The County will provide the Network Connection. |

Exhibit 2

| **PCI Responsibility Matrix** | | | | | | |
|---|---|---|---|---|---|---|
| | | **Responsibility of** | | | | |
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 1.2.1 | Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic. | | | | X | This will have to be reviewed during the design phase as some software functions and API may need to have outbound access. |
| 1.2.2 | Secure and synchronize router configuration files. | | | | X | |
| 1.2.3 | Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment. | X | | | | Our system will just have a firewall between the server and network access. There will be no wireless networks at the site. The firewall settings will be set up during the design phase. |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | | | | X | |
| 1.3.1 | Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. | | X | | | |
| 1.3.2 | Limit inbound Internet traffic to IP addresses within the DMZ. | X | | | | |
| 1.3.3 | Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.) | X | | | | |
| 1.3.4 | Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. | | | | X | Settings for Outbound traffic will be set during the design phase. |
| 1.3.5 | Permit only "established" connections into the network. | X | | | | |
| 1.3.6 | Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | X | | | | Card holder data is not stored on the server. Transactions are encrypted and immediately sent to Windcave cloud server outside the scope of PCI compliance for customer. |

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 1.3.7 | Do not disclose private IP addresses and routing information to unauthorized parties.<br>Note: Methods to obscure IP addressing may include, but are not limited to:<br>• Network Address Translation (NAT)<br>• Placing servers containing cardholder data behind proxy servers/firewalls,<br>• Removal or filtering of route advertisements for private networks that employ registered addressing<br>• Internal use of RFC1918 address space instead of registered addresses. | X | | | | More of a personnel security measure. |
| 1.4 | Install personal firewall software equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include:<br>• Specific configuration settings are defined for personal firewall software.<br>• Personal firewall software (or equivalent functionality) is actively running.<br>• Personal firewall (or equivalent functionality) is not alterable by users of mobile and/or employee-owned devices. | | | | X | |
| 1.5 | Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties. | | | | X | |
| 2.1 | Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.<br>This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale | | X | | | User develop their own passwords. They are not issued by Windcave or the software for on-line reporting. |

Exhibit 2

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| Req't. | Requirement Text | N/A | Provider | County | Joint | Notes |
| | (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.). | | | | | |
| 2.1.1 | For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. | X | | | | |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.<br>Sources of industry-accepted system hardening standards may include, but are not limited to:<br>• Center for Internet Security (CIS)<br>• International Organization for Standardization (ISO)<br>• SysAdmin Audit Network Security (SANS) Institute<br>• National Institute of Standards Technology (NIST). | | | | X | |
| 2.2.1 | Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)<br>Note: Where virtualization technologies are in use, implement only one primary function per virtual system component. | X | | | | All software functions will occur on one server. |

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| Req't. | Requirement Text | N/A | Provider | County | Joint | Notes |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | | | | X | |
| 2.2.3 | Implement additional security features for any required services, protocols, or daemons that are considered to be insecure. | | | | X | |
| 2.2.4 | Configure system security parameters to prevent misuse. | | | | X | |
| 2.2.5 | Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. | | X | | | |
| 2.3 | Encrypt all non-console administrative access using strong cryptography. | X | | | | |
| 2.4 | Maintain an inventory of system components that are in scope for PCI DSS. | | | | X | County is responsible for PCI through contracted merchant account provider. |
| 2.5 | Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. | X | | | | Through Parking Management company. |
| 2.6 | Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers. | X | | | | |
| 3.1 | Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:<br>• Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements<br>• Processes for secure deletion of data when no longer needed<br>• Specific retention requirements for cardholder data<br>• A quarterly process for identifying and | X | | | | All credit card transactions are not stored on the server. They are handled by the CC processor. |

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| | securely deleting stored cardholder data that exceeds defined retention. | | | | | |
| 3.2 | Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.<br>*It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:*<br>*• There is a business justification and*<br>*• The data is stored secur*ely.<br>Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3: | | X | | | Transaction data is not stored on the server. |
| 3.2.1 | Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization.<br>This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.<br>*Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:*<br>*• The cardholder's name*<br>*• Primary account number (PAN)*<br>*• Expiration date*<br>*• Service code*<br>*To minimize risk, store only these data elements as needed for business.* | | X | | | Transaction data is not stored on the server. |

Exhibit 2

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| **Req’t.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 3.2.2 | Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization. | | X | | | Transaction data is not stored on the server. |
| 3.2.3 | Do not store the personal identification number (PIN) or the encrypted PIN block after authorization. | | X | | | Transaction data is not stored on the server. |
| 3.3 | Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.<br>Note: This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point- of-sale (POS) receipts. | | | | X | As part of FACTA, TIBA only displays the last four digits of the transaction. Windcave is complaint with this requirement on its online portal.<br>County would supply personnel responsible for accessing the online portal. |
| 3.4 | Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:<br>• One-way hashes based on strong cryptography, (hash must be of the entire PAN)<br>• Truncation (hashing cannot be used to replace the truncated segment of PAN)<br>• Index tokens and pads (pads must be securely stored)<br>• Strong cryptography with associated key- management processes and procedures.<br>Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity’s environment, additional controls should be in place to ensure that the hashed and truncated versions | | X | | | Transaction data is not stored on the server. |

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| Req't. | Requirement Text | N/A | Provider | County | Joint | Notes |
| | cannot be correlated to reconstruct the original PAN. | | | | | |
| 3.4.1 | If disk encryption is used (rather than file or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.<br>*Note: This requirement applies in addition to all other PCI DSS encryption and key-management requirements.* | X | | | | |
| 3.5 | Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse:<br>*Note: This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key- encrypting keys must be at least as strong as the data-encrypting key.* | X | | | | |

Exhibit 2

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 3.5.1 | Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes:<br>• Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date<br>• Description of the key usage for each key.<br>• Inventory of any HSMs and other SCDs used for key management | X | | | | |
| 3.5.2 | Restrict access to cryptographic keys to the fewest number of custodians necessary. | X | | | | |
| 3.5.3 | Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times:<br>• Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data- encrypting key<br>• Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device)<br>• As at least two full-length key components or key shares, in accordance with an industry-accepted method<br>*Note: It is not required that public keys be stored in one of these forms.* | | X | | | 3DES encryption method |
| 3.5.4 | Store cryptographic keys in the fewest possible locations. | | X | | | Each device houses cryptographic keys |
| 3.6 | Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:<br>*Note: Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.* | X | | | | Does not apply to chip P2PE transactions |

Exhibit 2

**PCI Responsibility Matrix**

| | | Responsibility of | | | | |
|---|---|---|---|---|---|---|
| **Req’t.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 3.6.1 | Generation of strong cryptographic keys | X | | | | |
| 3.6.2 | Secure cryptographic key distribution | X | | | | |
| 3.6.3 | Secure cryptographic key storage | X | | | | |
| 3.6.4 | Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application Provider/Vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57). | X | | | | |
| 3.6.5 | Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised.<br>*Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.* | X | | | | |
| 3.6.6 | If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.<br>*Note: Examples of manual key-management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.* | X | | | | |
| 3.6.7 | Prevention of unauthorized substitution of cryptographic keys. | X | | | | |

Exhibit 2

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 3.6.8 | Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key- custodian responsibilities. | X | | | | |
| 3.7 | Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties. | | | | X | Windcave will provide P2PE PIM guides |
| 4.1 | Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following:<br>• Only trusted keys and certificates are accepted.<br>• The protocol in use only supports secure versions or configurations.<br>• The encryption strength is appropriate for the encryption methodology in use.<br>*Examples of open, public networks include but are not limited to:*<br>*• The Internet*<br>*• Wireless technologies, including 802.11 and Bluetooth*<br>*• Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)*<br>*• General Packet Radio Service (GPRS).*<br>*• Satellite communications.* | | X | | | Windcave deploys 3DES |
| 4.1.1 | Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission. | X | | | | |
| 4.2 | Never send unprotected PANs by end-user messaging technologies (for example, e- mail, instant messaging, SMS, chat, etc.). | | | | X | |
| 4.3 | Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are | X | | | | Through Parking Management company. |

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| Req't. | Requirement Text | N/A | Provider | County | Joint | Notes |
| | documented, in use, and known to all affected parties. | | | | | |
| 5.1 | Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). | | X | | | For SmartPark Web Application server and client workstations. |
| 5.1.1 | Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software. | | X | | | For SmartPark Web Application server and client workstations. |
| 5.1.2 | For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software. | | X | | | For SmartPark Web Application server and client workstations. |
| 5.2 | Ensure that all anti-virus mechanisms are maintained as follows:<br>• Are kept current,<br>• Perform periodic scans<br>• Generate audit logs which are retained per PCI DSS Requirement 10.7. | | X | | | For SmartPark Web Application server and client workstations. |
| 5.3 | Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by- case basis for a limited time period.<br>*Note: Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti- virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.* | | X | | | For SmartPark Web Application server and client workstations. |
| 5.4 | Ensure that security policies and operational procedures for protecting systems against malware are | | X | | | For SmartPark Web Application server and client workstations. |

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| Req't. | Requirement Text | N/A | Provider | County | Joint | Notes |
| | documented, in use, and known to all affected parties. | | | | | |
| 6.1 | Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.<br>*Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.* | | X | | | For SmartPark Web Application server and client workstations. |
| 6.2 | Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.<br>*Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.* | | X | | | For SmartPark Web Application server and client workstations. |

Exhibit 2

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 6.3 | Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:<br>• In accordance with PCI DSS (for example, secure authentication and logging)<br>• Based on industry standards and/or best practices.<br>• Incorporating information security throughout the software-development life cycle<br>Note: this applies to all software developed internally as well as bespoke or custom software developed by a third party. | | X | | | Payline Portal provided by Windcave/Payment Express is PCI DSS complaint along TIBA equipment. |
| 6.3.1 | Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to County. | | X | | | Payline provided by Windcave/Payment Expresswill handle credentials in a PCI complaint manner |
| 6.3.2 | Review custom code prior to release to production or County in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following:<br>• Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code- review techniques and secure coding practices.<br>• Code reviews ensure code is developed according to secure coding guidelines<br>• Appropriate corrections are implemented prior to release.<br>Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle.<br>Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing | X | | | | |

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| Req't. | Requirement Text | N/A | Provider | County | Joint | Notes |
| | threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6. | | | | | |
| 6.4 | Follow change control processes and procedures for all changes to system components. The processes must include the following: | | X | | | |
| 6.4.1 | Separate development/test environments from production environments, and enforce the separation with access controls. | | X | | | |
| 6.4.2 | Separation of duties between development/test and production environments | | X | | | |
| 6.4.3 | Production data (live PANs) are not used for testing or development | | X | | | |
| 6.4.4 | Removal of test data and accounts before production systems become active | | X | | | |
| 6.4.5 | Change control procedures for the implementation of security patches and software modifications must include the following: | | X | | | |
| 6.4.5.1 | Documentation of impact. | | X | | | |
| 6.4.5.2 | Documented change approval by authorized parties. | | X | | | |
| 6.4.5.3 | Functionality testing to verify that the change does not adversely impact the security of the system. | | X | | | |
| 6.4.5.4 | Back-out procedures. | | X | | | |
| 6.4.6 | Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated | | | | X | |

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 6.5 | Address common coding vulnerabilities in software-development processes as follows:<br>• Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory.<br>• Develop applications based on secure coding guidelines.<br><br>Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements. | X | | | | |
| 6.5.1 | Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws. | X | | | | |
| 6.5.2 | Buffer overflows | X | | | | |
| 6.5.3 | Insecure cryptographic storage | X | | | | |
| 6.5.4 | Insecure communications | X | | | | |
| 6.5.5 | Improper error handling | X | | | | |
| 6.5.6 | All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1). | X | | | | |
| 6.5.7 | Cross-site scripting (XSS) | X | | | | |
| 6.5.8 | Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions). | X | | | | |
| 6.5.9 | Cross-site request forgery (CSRF) | X | | | | |
| 6.5.10 | Broken authentication and session management | X | | | | |

Exhibit 2

| **PCI Responsibility Matrix** | | | | | | |
|---|---|---|---|---|---|---|
| | | **Responsibility of** | | | | |
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 6.6 | For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:<br>• Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes<br>Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2.<br>• Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic. | X | | | | May apply to Park Blue in the future if County elects the option |
| 6.7 | Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties. | | | | X | Through Parking Management company. |
| 7.1 | Limit access to system components and cardholder data to only those individuals whose job requires such access. | X | | | | Through Parking Management company. |
| 7.1.1 | Define access needs for each role, including:<br>• System components and data resources that each role needs to access for their job function<br>• Level of privilege required (for example, user, administrator, etc.) for accessing resources. | X | | | | Through Parking Management company. |
| 7.1.2 | Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. | X | | | | Through Parking Management company. |
| 7.1.3 | Assign access based on individual personnel's job classification and function. | X | | | | Through Parking Management company. |

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 7.1.4 | Require documented approval by authorized parties specifying required privileges. | X | | | | Through Parking Management company. |
| 7.2 | Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.<br>This access control system must include the following: | X | | | | Through Parking Management company. |
| 7.2.1 | Coverage of all system components | | | | X | |
| 7.2.2 | Assignment of privileges to individuals based on job classification and function. | X | | | | Through Parking Management company. |
| 7.2.3 | Default "deny-all" setting. | X | | | | Through Parking Management company. |
| 7.3 | Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties. | X | | | | Through Parking Management company. |
| 8.1 | Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows: | X | | | | Through Parking Management company. |
| 8.1.1 | Assign all users a unique ID before allowing them to access system components or cardholder data. | X | | | | Through Parking Management company. |
| 8.1.2 | Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. | X | | | | Through Parking Management company. |
| 8.1.3 | Immediately revoke access for any terminated users. | X | | | | Through Parking Management company. |
| 8.1.4 | Remove/disable inactive user accounts within 90 days. | X | | | | Through Parking Management company. |
| 8.1.5 | Manage IDs used by Provider/Vendors to access, support, or maintain system components via remote access as follows:<br>• Enabled only during the time period needed and disabled when not in use.<br>• Monitored when in use. | X | | | | Through Parking Management company. |
| 8.1.6 | Limit repeated access attempts by locking out the user ID after not more than six attempts. | | | | X | Payline can limit the number of access attempts and lock user ID. |

Exhibit 2

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 8.1.7 | Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. | X | | | | Through Parking Management company. |
| 8.1.8 | If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. | X | | | | Through Parking Management company. |
| 8.2 | In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:<br>• Something you know, such as a password or passphrase<br>• Something you have, such as a token device or smart card<br>• Something you are, such as a biometric. | X | | | | County will determine their own passwords Through Parking Management company. |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | | X | | | |
| 8.2.2 | Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys. | | X | | | |
| 8.2.3 | Passwords/phrases must meet the following:<br>• Require a minimum length of at least seven characters.<br>• Contain both numeric and alphabetic characters.<br>Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above. | | X | | | |
| 8.2.4 | Change user passwords/passphrases at least once every 90 days. | X | | | | Through Parking Management company. |
| 8.2.5 | Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used. | X | | | | Through Parking Management company. |

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| **Req’t.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 8.2.6 | Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use. | X | | | | |
| 8.3 | Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.<br>*Note: Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication* | X | | | | |
| 8.3.1 | Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access. | X | | | | |
| 8.3.2 | Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity's network. | | | X | | County uses Duo Security. TIBA will be required to enroll in Duo. |
| 8.4 | Document and communicate authentication procedures and policies to all users including:<br>• Guidance on selecting strong authentication credentials<br>• Guidance for how users should protect their authentication credentials<br>• Instructions not to reuse previously used passwords<br>• Instructions to change passwords if there is any suspicion the password could be compromised. | X | | | | |

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 8.5 | Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:<br>• Generic user IDs are disabled or removed.<br>• Shared user IDs do not exist for system administration and other critical functions.<br>• Shared and generic user IDs are not used to administer any system components. | X | | | | |
| 8.5.1 | Additional requirement for service providers only: Service providers with remote access to County premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.<br>*Note: This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.* | | | | X | |
| 8.6 | Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows:<br>• Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts.<br>• Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access. | X | | | | |

Exhibit 2

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 8.7 | All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:<br>• All user access to, user queries of, and user actions on databases are through programmatic methods.<br>• Only database administrators have the ability to directly access or query databases.<br>• Application IDs for database applications can only be used by the applications (and not by individual users or other non- application processes). | X | | | | |
| 8.8 | Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties. | X | | | | |
| 9.1 | Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment. | X | | | | |
| 9.1.1 | Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. *Note: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.* | X | | | | |
| 9.1.2 | Implement physical and/or logical controls<br>to restrict access to publicly accessible network jacks.<br>For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, | X | | | | |

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| Req't. | Requirement Text | N/A | Provider | County | Joint | Notes |
| | processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks. | | | | | |
| 9.1.3 | Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines. | X | | | | |
| 9.2 | Develop procedures to easily distinguish between onsite personnel and visitors, to include:<br>• Identifying onsite personnel and visitors (for example, assigning badges)<br>• Changes to access requirements<br>• Revoking or terminating onsite personnel and expired visitor identification (such as ID badges). | X | | | | |
| 9.3 | Control physical access for onsite personnel to the sensitive areas as follows:<br>• Access must be authorized and based on individual job function.<br>• Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled. | X | | | | |
| 9.4.x | Implement procedures to identify and authorize visitors. Procedures should include the following: | X | | | | |
| 9.4.1 | Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained. | X | | | | |
| 9.4.2 | Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel. | X | | | | |

Exhibit 2

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 9.4.3 | Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration. | X | | | | |
| 9.4.4 | A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted.<br>Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log.<br>Retain this log for a minimum of three months, unless otherwise restricted by law. | X | | | | |
| 9.5 | Physically secure all media. | X | | | | |
| 9.5.1 | Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually. | X | | | | |
| 9.6 | Maintain strict control over the internal or external distribution of any kind of media, including the following: | X | | | | |
| 9.6.1 | Classify media so the sensitivity of the data can be determined. | X | | | | |
| 9.6.2 | Send the media by secured courier or other delivery method that can be accurately tracked. | X | | | | |
| 9.6.3 | Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals). | X | | | | |
| 9.7 | Maintain strict control over the storage and accessibility of media. | X | | | | |
| 9.7.1 | Properly maintain inventory logs of all media and conduct media inventories at least annually. | X | | | | |
| 9.8 | Destroy media when it is no longer needed for business or legal reasons as follows: | X | | | | |
| 9.8.1 | Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed. | X | | | | |

Exhibit 2

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 9.8.2 | Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed. | X | | | | |
| 9.9 | Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.<br>Note: These requirements apply to card- reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads. | X | | | | |
| 9.9.1 | Maintain an up-to-date list of devices. The list should include the following:<br>• Make, model of<br>• Location of device (for example, the address of the site or facility where the device is located)<br>• Device serial number or other method of unique identification. | | | | X | |
| 9.9.2 | Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).<br>Note: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings. | | | | X | |

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 9.9.3 | Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following:<br>• Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.<br>• Do not install, replace, or return devices without verification.<br>• Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).<br>• Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). | | | | X | |
| 9.1 | Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties. | X | | | | |
| 10.1 | Implement audit trails to link all access to system components to each individual user. | X | | | | |
| 10.2 | Implement automated audit trails for all system components to reconstruct the following events: | X | | | | |
| 10.2.1 | All individual user accesses to cardholder data | X | | | | |
| 10.2.2 | All actions taken by any individual with root or administrative privileges | X | | | | |
| 10.2.3 | Access to all audit trails | X | | | | |
| 10.2.4 | Invalid logical access attempts | X | | | | |
| 10.2.5 | Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges | | | | X | |

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| Req't. | Requirement Text | N/A | Provider | County | Joint | Notes |
| 10.2.6 | Initialization, stopping, or pausing of the audit logs | | X | | | |
| 10.2.7 | Creation and deletion of system-level objects | X | | | | |
| 10.3 | Record at least the following audit trail entries for all system components for each event: | | X | | | |
| 10.3.1 | User identification | | X | | | |
| 10.3.2 | Type of event | | X | | | |
| 10.3.3 | Date and time | | X | | | |
| 10.3.4 | Success or failure indication | | X | | | |
| 10.3.5 | Origination of event | | X | | | |
| 10.3.6 | Identity or name of affected data, system component, or resource. | X | | | | Logs indicate inconsistencies in messaging communication only |
| 10.4 | Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. *Note: One example of time synchronization technology is Network Time Protocol (NTP).* | | X | | | |
| 10.4.1 | Critical systems have the correct and consistent time. | | X | | | |
| 10.4.2 | Time data is protected. | | X | | | |
| 10.4.3 | Time settings are received from industry- accepted time sources. | | X | | | |
| 10.5 | Secure audit trails so they cannot be altered. | | X | | | |
| 10.5.1 | Limit viewing of audit trails to those with a job-related need. | X | | | | |
| 10.5.2 | Protect audit trail files from unauthorized modifications. | X | | | | |
| 10.5.3 | Promptly back up audit trail files to a centralized log server or media that is difficult to alter. | X | | | | |
| 10.5.4 | Write logs for external-facing technologies onto a secure, centralized, internal log server or media device. | X | | | | |
| 10.5.5 | Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts | X | | | | |

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| | (although new data being added should not cause an alert). | | | | | |
| 10.6 | Review logs and security events for all system components to identify anomalies or suspicious activity.<br>Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement. | X | | | | |
| 10.6.1 | Review the following at least daily:<br>• All security events<br>• Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD<br>• Logs of all critical system components<br>• Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e- commerce redirection servers, etc.). | X | | | | |
| 10.6.2 | Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment. | X | | | | |
| 10.6.3 | Follow up exceptions and anomalies identified during the review process. | X | | | | |
| 10.7 | Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup). | **X** | | | | |

<table>
<tr><th colspan="7">PCI Responsibility Matrix</th></tr>
<tr><th></th><th></th><th colspan="4">Responsibility of</th><th></th></tr>
<tr><th>Req't.</th><th>Requirement Text</th><th>N/A</th><th>Provider</th><th>County</th><th>Joint</th><th>Notes</th></tr>
<tr><td>10.8</td><td>Additional requirement for service providers only:<br><br>Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of:<br>• Firewalls<br>• IDS/IPS<br>• FIM<br>• Anti-virus<br>• Physical access controls<br>• Logical access controls<br>• Audit logging mechanisms<br>• Segmentation controls (if used)</td><td></td><td>X</td><td></td><td></td><td></td></tr>
<tr><td>10.8.1</td><td>Additional requirement for service providers only:<br>Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include:<br>• Restoring security functions<br>• Identifying and documenting the duration (date and time start to end) of the security failure<br>• Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause<br>• Identifying and addressing any security issues that arose during the failure<br>• Performing a risk assessment to determine whether further actions are required as a result of the security failure<br>• Implementing controls to prevent cause of failure from reoccurring<br>• Resuming monitoring of security controls</td><td></td><td>X</td><td></td><td></td><td></td></tr>
<tr><td>10.9</td><td>Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.</td><td></td><td></td><td></td><td>X</td><td></td></tr>
</table>

Exhibit 2

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 11.1 | Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices. | | | X | | |
| 11.1.1 | Maintain an inventory of authorized wireless access points including a documented business justification. | | | | X | |
| 11.1.2 | Implement incident response procedures in the event unauthorized wireless access points are detected. | X | | | | |
| 11.2 | Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).<br>Note: Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.<br>For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan,<br>2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as | X | | | | |

Exhibit 2

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| Req't. | Requirement Text | N/A | Provider | County | Joint | Notes |
| | shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred. | | | | | |
| 11.2.1 | Perform quarterly internal vulnerability scans and rescans as needed, until all "high- risk" vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel. | X | | | | |
| 11.2.2 | Perform quarterly external vulnerability scans, via an Approved Scanning Provider/Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.<br>Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Provider/Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).<br>Refer to the ASV Program Guide published on the PCI SSC website for scan County responsibilities, scan preparation, etc. | X | | | | |

**PCI Responsibility Matrix**

| | | Responsibility of | | | | |
|---|---|---|---|---|---|---|
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 11.2.3 | Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel. | X | | | | |
| 11.3 | Implement a methodology for penetration testing that includes the following:<br>• Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)<br>• Includes coverage for the entire CDE perimeter and critical systems<br>• Includes testing from both inside and outside the network<br>• Includes testing to validate any segmentation and scope-reduction controls<br>• Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5<br>• Defines network-layer penetration tests to include components that support network functions as well as operating systems<br>• Includes review and consideration of threats and vulnerabilities experienced in the last 12 months<br>• Specifies retention of penetration testing results and remediation activities results. Note: This update to Requirement 11.3 is a best practice until June 30, 2015, after which it becomes a requirement. PCI DSS v2.0 requirements for penetration testing must be followed until v3.0 is in place. | X | | | | |
| 11.3.1 | Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). | X | | | | |

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| Req't. | Requirement Text | N/A | Provider | County | Joint | Notes |
| 11.3.2 | Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). | X | | | | |
| 11.3.3 | Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections. | X | | | | |
| 11.3.4 | If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out- of-scope systems from systems in the CDE. | X | | | | |
| 11.3.4.1 | Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods. | | | | X | |
| 11.4 | Use intrusion-detection and/or intrusion- prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.<br>Keep all intrusion-detection and prevention engines, baselines, and signatures up to date. | X | | | | |
| 11.5 | Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the | X | | | | |

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| Req't. | Requirement Text | N/A | Provider | County | Joint | Notes |
| | software to perform critical file comparisons at least weekly. | | | | | |
| 11.5.1 | Implement a process to respond to any alerts generated by the change-detection solution. | X | | | | |
| 11.6 | Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties. | X | | | | |
| 12.1 | Establish, publish, maintain, and disseminate a security policy. | X | | | | |
| 12.1.1 | Review the security policy at least annually and update the policy when the environment changes. | X | | | | |
| 12.2 | Implement a risk-assessment process that:<br>-Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.),<br>-Identifies critical assets, threats, and vulnerabilities, and<br>-Results in a formal, documented analysis of risk. | X | | | | |
| 12.3 | Develop usage policies for critical technologies and define proper use of these technologies.<br>Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.<br>Ensure these usage policies require the following: | X | | | | |
| 12.3.1 | Explicit approval by authorized parties | X | | | | |
| 12.3.2 | Authentication for use of the technology | X | | | | |
| 12.3.3 | A list of all such devices and personnel with access | | | | X | TIBA and Windcave can provide a list of devices to the County |

**PCI Responsibility Matrix**

| | | Responsibility of | | | | |
|---|---|---|---|---|---|---|
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 12.3.4 | A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices) | | | | X | |
| 12.3.5 | Acceptable uses of the technology | | X | | | |
| 12.3.6 | Acceptable network locations for the technologies | X | | | | |
| 12.3.7 | List of company-approved products | | X | | | |
| 12.3.8 | Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity | | X | | | |
| 12.3.9 | Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use | | X | | | |
| 12.3.10 | For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.<br>Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements. | X | | | | |
| 12.4 | Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. | X | | | | |
| 12.4.1 | Additional requirement for service providers only:<br>Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include:<br>• Overall accountability for maintaining PCI DSS compliance<br>• Defining a charter for a PCI DSS compliance program and communication to executive management | X | | | | |

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| Req't. | Requirement Text | N/A | Provider | County | Joint | Notes |
| 12.5 | Assign to an individual or team the following information security management responsibilities: | X | | | | |
| 12.5.1 | Establish, document, and distribute security policies and procedures. | X | | | | |
| 12.5.2 | Monitor and analyze security alerts and information, and distribute to appropriate personnel. | X | | | | |
| 12.5.3 | Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. | X | | | | |
| 12.5.4 | Administer user accounts, including additions, deletions, and modifications. | X | | | | |
| 12.5.5 | Monitor and control all access to data. | X | | | | |
| 12.6 | Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security. | | | | X | |
| 12.6.1 | Educate personnel upon hire and at least annually.<br>Note: Methods can vary depending on the role of the personnel and their level of access to the cardholder data. | | | | X | |
| 12.6.2 | Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures. | | | | X | |
| 12.7 | Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)<br>Note: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only. | | | | X | |
| 12.8 | Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, | X | | | | |

| **PCI Responsibility Matrix** | | | | | | |
|---|---|---|---|---|---|---|
| | | **Responsibility of** | | | | |
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| | or that could affect the security of cardholder data, as follows: | | | | | |
| 12.8.1 | Maintain a list of service providers. | X | | | | |
| 12.8.2 | Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the County, or to the extent that they could impact the security of the County's cardholder data environment.<br>*Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.* | X | | | | |
| 12.8.3 | Ensure there is an established process for engaging service providers including proper due diligence prior to engagement. | X | | | | |
| 12.8.4 | Maintain a program to monitor service providers' PCI DSS compliance status at least annually. | X | | | | |
| 12.8.5 | Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. | | | | X | |

Exhibit 2

| **PCI Responsibility Matrix** | | | | | | |
|---|---|---|---|---|---|---|
| | | **Responsibility of** | | | | |
| **Req’t.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 12.9 | Additional requirement for service providers only: Service providers acknowledge in writing to County that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the County, or to the extent that they could impact the security of the County’s cardholder data environment.<br>*Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.* | | X | | | |
| 12.1 | Implement an incident response plan. Be prepared to respond immediately to a system breach. | X | | | | |
| 12.10.1 | Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:<br>• Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum<br>• Specific incident response procedures<br>• Business recovery and continuity procedures<br>• Data backup processes<br>• Analysis of legal requirements for reporting compromises<br>• Coverage and responses of all critical system components<br>• Reference or inclusion of incident response procedures from the payment brands. | X | | | | |
| 12.10.2 | Test the plan at least annually. | X | | | | |
| 12.10.3 | Designate specific personnel to be available on a 24/7 basis to respond to alerts. | X | | | | |

Exhibit 2

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| 12.10.4 | Provide appropriate training to staff with security breach response responsibilities. | | | | X | |
| 12.10.5 | Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems. | | | | X | |
| 12.10.6 | Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. | X | | | | |
| 12.11 | Additional requirement for service providers only:<br>Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes:<br>• Daily log reviews<br>• Firewall rule-set reviews<br>• Applying configuration standards to new systems<br>• Responding to security alerts<br>• Change management processes | X | | | | |
| 12.11.1 | Additional requirement for service providers only:<br>Maintain documentation of quarterly review process to include:<br>• Documenting results of the reviews<br>• Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program | X | | | | |
| A.1 | Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4:<br><br>A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each | X | | | | |

| PCI Responsibility Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibility of | | | | |
| **Req't.** | **Requirement Text** | **N/A** | **Provider** | **County** | **Joint** | **Notes** |
| | entity must comply with the PCI DSS and validate compliance as applicable. | | | | | |
| A.1.1 | Ensure that each entity only runs processes that have access to that entity's cardholder data environment. | X | | | | |
| A.1.2 | Restrict each entity's access and privileges to its own cardholder data environment only. | X | | | | |
| A.1.3 | Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10. | X | | | | |
| A.1.4 | Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider. | X | | | | |

## Exhibit I – Security Requirements

Managed Services; Professional Services; Third-Party Vendors. Provider shall immediately notify County of any terminations or separations of Provider's employees who performed Services to County under the Agreement or who had access to County data or the County network, and Provider must ensure such employees' access to County data and network is promptly disabled. Provider must ensure all Provider's employees with access to County's network via an Active Directory account comply with all applicable County policies and procedures when accessing County's network. Provider shall provide privacy and information security training to its employees with access the County's network upon hire and at least once annually. If any unauthorized party is successful in accessing any information technology component related to the Provider, including but not limited to servers or fail-over servers where County data or files exist or are housed, Provider shall report to County within twenty-four (24) hours of becoming aware of such breach. Provider shall provide County with a detailed incident report within five (5) days after the breach, including remedial measures instituted and any law enforcement involvement. Provider shall fully cooperate with County on incident response, forensics, and investigations into Provider's infrastructure as it relates to any County data or County applications. Provider shall not release County data or copies of County data without the advance written consent of County.

Remote Access. Any remote access by Provider must be secure and strictly controlled with current industry standards for encryption (e.g., Virtual Private Networks) and strong pass-phrases. For any device Provider utilizes to remotely connect to County's network, Provider shall ensure the remote host device is not connected to any other network while connected to County's network, with the exception of personal networks that are under Provider's complete control or under the complete control of a user or third party authorized in advance by County in writing. Provider shall not use an open, unencrypted third party provided public WiFi network to remotely connect to County's network. Equipment used to connect to County's networks must: (a) utilize antivirus protection software; (b) utilize an updated operating system, firmware, and third-party application patches; and (c) be configured for least privileged access. Should Provider exceed the scope of remote access necessary to provide the required services under this Agreement, as determined in County's sole discretion, County may suspend Provider's access to County's network immediately without notice. Provider must utilize, at a minimum, industry standard security measures, as determined in County's sole discretion, to safeguard County data that resides in or transits through Provider's internal network from unauthorized access and disclosure.

Software Installed in County's Network. Provider shall advise County of any third-party software (e.g., Java, Adobe Reader/Flash, Silverlight) required to be installed and all versions supported. Provider shall support updates for critical vulnerabilities discovered in applicable third-party software. Provider shall ensure that the Software is developed based on industry standards and best practices, including following secure programming techniques and incorporating security throughout the software-development life cycle. Provider must develop and maintain the Software to operate on County-supported and approved operating systems and firmware versions. Provider must mitigate critical or high-risk vulnerabilities to the Provider platform as defined by Common Vulnerability and Exposures (CVE) scoring system within 30 days after patch release. If Provider is unable to apply a patch to remedy the vulnerability, Provider must notify County of proposed mitigation steps to be taken and timeline for resolution. Provider shall ensure the Software provides for role-based access controls and runs with least privilege access. Provider shall support electronic delivery of digitally signed upgrades from Provider's or the third-party licensor's website. Provider shall enable auditing by default in software for any privileged access or changes. The Software must not be within three (3) years from Software's end of life date and the Software must run as least privilege without using fixed or default passwords. Provider shall regularly provide County with end-of-life-schedules for all applicable Software. Provider will support encryption using at a minimum Advanced Encryption Standard 256-bit encryption keys ("AES-256") or current industry security standards, whichever is higher, for confidential data at rest. Provider will use transport layer security (TLS) 1.1 or current industry standards, whichever is higher, for data in motion.

Equipment Leased or Purchased from Provider. Provider shall ensure that physical security features to prevent tampering are included in any Equipment provided under this Agreement. Provider shall ensure, at a minimum, industry-standard security measures are followed during the manufacture of the Equipment provided under this Agreement. Any Equipment provided under this Agreement shall not contain any embedded remote- control features unless approved in writing by County's Contract Administrator. Provider shall disclose any default accounts or backdoors that exist for access to County's network. If a new critical or high security vulnerability is identified, Provider shall supply a patch, firmware update, or workaround approved in writing by County's Contract Administrator within thirty (30) days after identification of vulnerability and shall notify County of proposed mitigation steps taken. Provider must develop and maintain hardware to interface with County-supported and approved operating systems and firmware versions. If a Provider shall make available, upon County's request, any required certifications as may be applicable per compliance and regulatory requirements (e.g., Common Criteria, Federal Information Processing Standard 140). The Equipment must not be within three (3) years from Equipment's end of life date. Provider shall regularly provide County with end-of-life-schedules for all applicable Equipment. Provider shall support electronic delivery of digitally signed upgrades of any applicable Equipment firmware from Provider's or the original equipment manufacturer's website.

Payment Card Industry (PCI) Compliance. '""Provider shall comply with the most recent version of the Security Standards Council's Payment Card Industry ("PCI") Data Security Standard ("DSS"). Prior to the Effective Date, after any significant change to the CDE, and annually Provider shall provide to County: A copy of their Annual PCI DSS Attestation of Compliance ("AOC"); A written acknowledgement of responsibility for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the County, or to the extent that the service provider could impact the security of the county's cardholder data environment. A PCI DSS responsibility matrix that outlines the exact PCI DSS Controls are the responsibility of the service provider and which controls the service provider shares responsibility with the County. Provider shall follow the VISA Cardholder Information Security Program ("CISP") payment

Exhibit 2

Application Best Practices and Audit Procedures and maintain current validation. If Provider subcontracts or in any way outsources credit card processing, or provides an API which redirects or transmits County data to a payment gateway, Provider is responsible for maintaining PCI compliance for their API and providing the AOC for the subcontractor or payment gateway to the County. Mobile payment application providers must follow industry best practices such as VISA Cardholder Information Security Program ("CISP") or OWASP for secure coding and transmission of payment card data. Provider agrees that it is responsible for the security of the County's cardholder data that it possesses, including the functions relating to storing, processing, and transmitting of the cardholder data. Provider will immediately notify County if it learns that it is no longer PCI DSS compliant and will immediately provide County the steps being taken to remediate the noncompliant status. In no event should Provider's notification to County be later than seven (7) calendar days after Provider learns it is no longer PCI DSS complaint. Provider shall enforce automatic disconnect of sessions for remote access technologies after a specific period of inactivity with regard to connectivity into County infrastructure. Provider shall activate remote access from vendors and business partners into County network only when needed by vendors and partners, with immediate deactivation after use. Provider shall implement encryption and two-factor authentication for securing remote access (non-console access) from outside the network into the County's environment with access to any stored credit card data. Provider shall maintain a file integrity monitoring program to ensure critical file system changes are monitored and approved with respect to County data. All inbound and outbound connections to County's CDE must use Transport Layer Security (TLS) 1.2 or current industry equivalent (whichever is higher).

Fair and Accurate Credit Transaction Act of 2003 (FACTA) Compliance. Provider and the System shall comply with FACTA, as amended, including ensuring that all records and receipts are compliant with FACTA requirements, and providing reporting on transaction activity within the Software including transient, contract, event, valet validations, prepaid, and other transactions.