Exhibit 2
Page 1 of 102

AGREEMENT BETWEEN BROWARD COUNTY AND SP PLUS CORPORATION FOR PARKING MANAGEMENT SERVICES FOR PORT EVERGLADES (RFP # PNC2116816P1)

This Agreement ("Agreement") is made and entered by and between Broward County, a political subdivision of the State of Florida ("County"), and SP Plus Corporation, a Delaware corporation authorized to transact business in the state of Florida ("Contractor") (each a "Party" and collectively referred to as the "Parties").

RECITALS

A. County issued RFP # PNC2116816P1 ("RFP") soliciting proposals from qualified vendors to provide parking management services for various County agencies.

B. The RFP separated the various facilities on or in which services are to be performed into two (2) groups: Group 1 – County Facilities Management parking facilities; and Group 2 – Port Everglades parking facilities and ground lots; with a separate contract to be awarded for each group.

C. Contractor was the top ranked proposer for Group 2, County and Contractor entered into negotiations, and this Agreement represents the final and complete understanding of the Parties regarding Contractor's performance of parking management services for Port Everglades parking facilities and ground lots.

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

ARTICLE 1. DEFINITIONS

1.1. **Board** means the Board of County Commissioners of Broward County, Florida.

1.2. **Contract Administrator** means the Port Director, the Assistant Port Director, or such other person designated by the Port Director in writing.

1.3. **Contract Year or Agreement Year** means the period beginning on the Commencement Date and ending twelve (12) months from such date, and each twelve (12) month period thereafter until the termination of this Agreement.

1.4. **County Business Enterprise** or **CBE** means an entity certified as meeting the applicable requirements of Section 1-81, Broward County Code of Ordinances.

1.5. **Port or Port Department** means Port Everglades Department of Broward County.

1.6. **Purchasing Director** means County's Director of Purchasing as appointed by the Broward County Administrator.

1.7. **Services** means all work required by Contractor under this Agreement, including without limitation all deliverables, consulting, training, project management, or other services specified in Exhibit A ("Scope of Services").

1.8. **Small Business Enterprise** or **SBE** means an entity certified as meeting the applicable requirements of Section 1-81, Broward County Code of Ordinances.

1.9. **Subcontractor** means an entity or individual providing services to County through Contractor for all or any portion of the work under this Agreement. The term "Subcontractor" shall include all subconsultants.

ARTICLE 2. EXHIBITS

Exhibit A	**Scope of Services**
Exhibit B	**Payment Schedule**
Exhibit C	**Minimum Insurance Coverages**
Exhibit D	**Not Used**
Exhibit E	**CBE Subcontractor Schedule and Letters of Intent**
Exhibit F	**Port Everglades Security Requirements**
Exhibit G	**Certification of Payments to Subcontractors and Suppliers**
Exhibit H	**PCI Responsibility Matrix**
Exhibit I	**Security Requirements**

ARTICLE 3. SCOPE OF SERVICES

Contractor shall perform all Services required under this Agreement including, without limitation, the work specified in Exhibit A (the "Scope of Services"). The Scope of Services is a description of Contractor's obligations and responsibilities and is deemed to include preliminary considerations and prerequisites, and all labor, materials, equipment, and tasks that are such an inseparable part of the work described that exclusion would render performance by Contractor impractical, illogical, or unconscionable. Contractor's performance of the Services shall at all times comply with the requirements set forth in Exhibit I.

ARTICLE 4. TERM AND TIME OF PERFORMANCE

4.1. Term. This Agreement shall become effective on the date it is fully executed by the Parties ("Effective Date"). The term of this Agreement shall commence on November 1, 2020 ("Commencement Date") and shall end at 11:59 PM on the day prior to the third anniversary of the Commencement Date ("Initial Term"), it being the intention of the Parties that the Initial Term be for a period of three (3) years.

4.2. Extensions. County may renew this Agreement for up to two (2) additional one (1) year terms (each an "Extension Term") by sending notice of renewal to Contractor at least thirty (30) days prior to the expiration of the then-current term. The Purchasing Director is authorized to exercise this renewal option.

4.3. Additional Extension. If unusual or exceptional circumstances, as determined in the sole discretion of the Purchasing Director, render the exercise of an Extension Term not practicable, or if no extension is available and expiration of this Agreement would, as determined by the Purchasing Director, result in a gap in the provision of Services necessary for the ongoing operations of County, then the Purchasing Director may extend this Agreement on the same terms and conditions for period(s) not to exceed six (6) months in the aggregate, provided that any such extension is within the authority of the Purchasing Director or otherwise authorized by the Board. The Purchasing Director may exercise this option by written notice to Contractor stating the duration of the extended period, at least thirty (30) days prior to the end of the then-current term.

4.4. Extension Rates and Terms. For any extension beyond the Initial Term, Contractor shall be compensated at the rates in effect when the extension was invoked by County, unless otherwise expressly stated in Exhibit B. Contractor shall continue to provide the Services upon the same terms and conditions as set forth in this Agreement for such extended period.

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

4.6. Time of the Essence. Unless otherwise agreed by the Parties in writing, all duties, obligations, and responsibilities of Contractor required by this Agreement shall be completed no later than the date or time specified for completion. Time is of the essence in performing the duties, obligations, and responsibilities required by this Agreement.

ARTICLE 5. COMPENSATION

5.1 Maximum Amounts. Contractor shall invoice County, and County shall pay Contractor, for Services provided under this Agreement only in accordance with Exhibit B (Payment Schedule), up to the maximum amounts as follows:

Total Fees/Expenses	Not-To-Exceed Amount
Management Fee, Initial Term	$217,550.00
Reimbursable Expenses, Initial Term	$4,374,776.00
TOTAL NOT TO EXCEED	$4,592,326.00

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

5.2 Subcontractors. Contractor shall invoice all Subcontractor fees, whether paid on a "lump sum" or other basis, to County with no markup. All Subcontractor fees shall be invoiced to County in the actual amount paid by Contractor.

5.3 Withholding by County. Notwithstanding any provision of this Agreement to the contrary, County may withhold, in whole or in part, payment to the extent necessary to protect itself from loss on account of inadequate or defective work that has not been remedied or resolved in a manner satisfactory to the Contract Administrator or failure to comply with any provision of this Agreement. The amount withheld shall not be subject to payment of interest by County.

ARTICLE 6. REPRESENTATIONS AND WARRANTIES

6.1. Representation of Authority. Contractor represents and warrants that this Agreement constitutes the legal, valid, binding, and enforceable obligation of Contractor, and that neither the execution nor performance of this Agreement constitutes a breach of any agreement that Contractor has with any third party or violates any law, rule, regulation, or duty arising in law or equity applicable to Contractor. Contractor further represents and warrants that execution of this Agreement is within Contractor's legal powers, and each individual executing this Agreement on behalf of Contractor is duly authorized by all necessary and appropriate action to do so on behalf of Contractor and does so with full legal authority.

6.2. Solicitation Representations. Contractor represents and warrants that all statements and representations made in Contractor's proposal, bid, or other supporting documents submitted to County in connection with the solicitation, negotiation, or award of this Agreement, including during the procurement or evaluation process, were true and correct when made and are true and correct as of the date Contractor executes this Agreement, unless otherwise expressly disclosed in writing by Contractor.

6.3. Contingency Fee. Contractor represents that it has not paid or agreed to pay any person or entity, other than a bona fide employee working solely for Contractor, any fee, commission, percentage, gift, or other consideration contingent upon or resulting from the award or making of this Agreement.

6.4. Truth-In-Negotiation Representation. Contractor's compensation under this Agreement is based upon its representations to County, and Contractor certifies that the wage rates, factual unit costs, and other information supplied to substantiate Contractor's compensation, including without limitation those made by Contractor during the negotiation of this Agreement, are accurate, complete, and current as of the date Contractor executes this Agreement. Contractor's compensation will be reduced to exclude any significant sums by which the contract price was increased due to inaccurate, incomplete, or noncurrent wage rates and other factual unit costs.

6.5. Public Entity Crime Act. Contractor 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. Contractor further represents that there has been no determination that it committed a "public entity crime" as

Exhibit 2

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 Contractor has been placed on the convicted vendor list.

6.6. Discriminatory Vendor and Scrutinized Companies Lists. Contractor represents that it has not been placed on the "discriminatory vendor list" as provided in Section 287.134, Florida Statutes, and that it is not a "scrutinized company" pursuant to Section 215.473, Florida Statutes. Contractor represents and certifies that it is not ineligible to contract with County on any of the grounds stated in Section 287.135, Florida Statutes.

6.7. Claims Against Contractor. Contractor represents and warrants that there is no action or proceeding, at law or in equity, before any court, mediator, arbitrator, governmental or other board or official, pending or, to the knowledge of Contractor, threatened against or affecting Contractor, the outcome of which may (a) affect the validity or enforceability of this Agreement, (b) materially and adversely affect the authority or ability of Contractor to perform its obligations under this Agreement, or (c) have a material and adverse effect on the consolidated financial condition or results of operations of Contractor or on the ability of Contractor to conduct its business as presently conducted or as proposed or contemplated to be conducted.

6.8. Warranty of Performance. Contractor represents and warrants that it possesses the knowledge, skill, experience, and financial capability required to perform and provide all Services and that each person and entity that will provide Services is duly qualified to perform such services by all appropriate governmental authorities, where required, and is sufficiently experienced and skilled in the area(s) for which such person or entity will render such Services. Contractor represents and warrants that the Services shall be performed in a skillful and respectful manner, and that the quality of all such services shall equal or exceed prevailing industry standards for the provision of such services.

6.9. Domestic Partnership Requirement. Unless this Agreement is exempt from the provisions of the Broward County Domestic Partnership Act, Section 16½-157, Broward County Code of Ordinances, Contractor certifies and represents that it will comply with the provisions of Section 16½-157 for the duration of this Agreement. The contract language referenced in Section 16½-157 is deemed incorporated in this Agreement as though fully set forth in this section.

6.10. Warranty Regarding PCI Compliance. Contractor warrants that, to the extent applicable, Contractor will comply with the most recent version of the Payment Card Industry Data Security Standard ("PCI DSS"). The Parties agree to adhere to the PCI Responsibility Matrix set forth in Exhibit H.

6.11. Breach of Representations. In entering into this Agreement, Contractor acknowledges that County is materially relying on the representations, warranties, and certifications of Contractor stated in this article. County shall be entitled to recover any damages it incurs to the extent any such representation or warranty is untrue. In addition, if any such representation, warranty, or certification is false, County shall have the right, at its sole discretion, to terminate this Agreement without any further liability to Contractor, to deduct from any amounts due

Contractor under this Agreement the full amount of any value paid in violation of a representation or warranty, and to recover all sums paid to Contractor under this Agreement. Furthermore, a false representation may result in debarment from County's procurement activities.

ARTICLE 7. INDEMNIFICATION

Contractor shall indemnify, hold harmless, and defend County and all of County's current, past, and future officers, agents, servants, and employees (collectively, "Indemnified Party") from and against any and all causes of action, demands, claims, losses, liabilities, and expenditures of any kind, including attorneys' fees, court costs, and expenses, including through the conclusion of any appellate proceedings, raised or asserted by any person or entity not a party to this Agreement, and caused or alleged to be caused, in whole or in part, by any intentional, reckless, or negligent act or omission of Contractor, its officers, employees, agents, or servants, arising from, relating to, or in connection with this Agreement (collectively, a "Claim"). If any Claim is brought against an Indemnified Party, Contractor shall, upon written notice from County, defend each Indemnified Party against each such Claim by counsel satisfactory to County or, at County's option, pay for an attorney selected by the County Attorney to defend the Indemnified Party. The obligations of this section shall survive the expiration or earlier termination of this Agreement. If considered necessary by the Contract Administrator and the County Attorney, any sums due Contractor under this Agreement may be retained by County until all Claims subject to this indemnification obligation have been settled or otherwise resolved. Any amount withheld shall not be subject to payment of interest by County.

ARTICLE 8. INSURANCE

8.1. For the duration of the Agreement, Contractor shall maintain the minimum insurance coverages stated in Exhibit C in accordance with the terms and conditions of this article. Contractor shall maintain insurance coverage against claims relating to any act or omission by Contractor, its agents, representatives, employees, or Subcontractors in connection with this Agreement. County reserves the right at any time to review and adjust the limits and types of coverage required under this article.

> 8.1.1 Workers Compensation Insurance reimbursement, as provided under Exhibit B, shall be based on the published rate by the National Council of Compensation Insurance in the state of Florida, as applied to actual salaries by job categories paid bi-weekly.

8.2. Contractor shall ensure that "Broward County" is listed and endorsed as an additional insured as stated in Exhibit C on all policies required under this article.

8.3. On or before the Effective Date or at least fifteen (15) days prior to commencement of Services, Contractor shall provide County with a copy of all Certificates of Insurance or other documentation sufficient to demonstrate the insurance coverage required in this article. County reserves the right to receive a copy of any policy required by this article within fourteen (14) days after written request to Contractor, either by personal inspection of the policy at County's offices, or by receiving a copy of the policy.

8.4. Contractor shall ensure that all insurance coverages required by this article shall remain in full force and effect for the duration of this Agreement and until all performance required by Contractor has been completed, as determined by Contract Administrator. Contractor or its insurer shall provide notice to County of any cancellation or modification of any required policy at least thirty (30) days prior to the effective date of cancellation or modification, and at least ten (10) days prior to the effective date of any cancellation due to nonpayment, and shall concurrently provide County with a copy of its updated Certificates of Insurance evidencing continuation of the required coverage(s). Contractor shall ensure that there is no lapse of coverage at any time during the time period for which coverage is required by this article.

8.5. Contractor shall ensure that all required insurance policies are issued by insurers: (1) assigned an A. M. Best rating of at least "A-" with a Financial Size Category of at least Class VII; (2) authorized to transact insurance in the State of Florida; or (3) a qualified eligible surplus lines insurer pursuant to Section 626.917 or 626.918, Florida Statutes, with approval by County's Risk Management Division.

8.6. If Contractor maintains broader coverage or higher limits than the minimum insurance requirements stated in Exhibit C, County shall be entitled to any such broader coverage and higher limits maintained by Contractor. All required insurance coverages under this article shall provide primary coverage and shall not require contribution from any County insurance, self-insurance or otherwise, which shall be in excess of and shall not contribute to the insurance required and provided by Contractor.

8.7. Contractor shall declare in writing any self-insured retentions or deductibles over the limit(s) prescribed in Exhibit C and submit to County for approval at least fifteen (15) days prior to the Effective Date or commencement of Services. Contractor shall be solely responsible for and shall pay for its deductibles or self-insured retention applicable to any claim against County, with the exception of the allowances outlined in Exhibit B, paragraph 2.1.12. County may, at any time, require Contractor to purchase coverage with a lower retention or provide proof of ability to pay losses and related investigations, claim administration, and defense expenses within the retention. Contractor agrees that any deductible or self-insured retention may be satisfied by either the named insured or County, if so elected by County, and Contractor agrees to obtain same in endorsements to the required policies.

8.8. Unless prohibited by the applicable policy, Contractor waives any right to subrogation that any of Contractor's insurer may acquire against County, and agrees to obtain same in an endorsement of Contractor's insurance policies.

8.9. Contractor shall require that each Subcontractor maintains insurance coverage that adequately covers the Services provided by that Subcontractor on substantially the same insurance terms and conditions required of Contractor under this article. Contractor shall ensure that all such Subcontractors comply with these requirements and that "Broward County" is named as an additional insured under the Subcontractors' applicable insurance policies.

8.10. If Contractor or any Subcontractor fails to maintain the insurance required by this Agreement, County may pay any costs of premiums necessary to maintain the required coverage and deduct such costs from any payment otherwise due to Contractor. Contractor shall not permit any Subcontractor to provide Services unless and until the requirements of this article are satisfied. If requested by County, Contractor shall provide, within one (1) business day, evidence of each Subcontractor's compliance with this section.

8.11. If any of the policies required under this article provide claims-made coverage: (1) any retroactive date must be prior to the Effective Date; (2) the required coverage must be maintained after termination or expiration of the Agreement for at least the duration stated in Exhibit C, and (3) if coverage is canceled or nonrenewed and is not replaced with another claims-made policy form with a retroactive date prior to the Effective Date, Contractor must obtain and maintain "extended reporting" coverage that applies after termination or expiration of the Agreement for at least the duration stated in Exhibit C.

ARTICLE 9. TERMINATION

9.1. This Agreement may be terminated for cause by the aggrieved Party if the Party in breach has not corrected the breach within ten (10) days after receipt of written notice from the aggrieved Party identifying the breach. This Agreement may also be terminated for convenience by the Board. Termination for convenience by the Board shall be effective on the termination date stated in written notice provided by County, which termination date shall be not less than thirty (30) days after the date of such written notice. This Agreement may also be terminated by the County Administrator upon such notice as the County Administrator deems appropriate under the circumstances if the County Administrator determines that termination is necessary to protect the public health, safety, or welfare. If County erroneously, improperly, or unjustifiably terminates for cause, such termination shall be deemed a termination for convenience and shall be effective thirty (30) days after such notice of termination for cause was provided and Contractor shall be eligible for the compensation provided in Section 9.4 as its sole remedy.

9.2. This Agreement may be terminated for cause by County for reasons including, but not limited to, any of the following:

9.2.1. Contractor's failure to suitably or continuously perform the Services in a manner calculated to meet or accomplish the objectives in this Agreement or Work Authorization, or repeated submission (whether negligent or intentional) for payment of false or incorrect bills or invoices;

9.2.2. By the Contract Administrator or the Director of Office of Economic and Small Business Development ("OESBD") for any fraud, misrepresentation, or material misstatement by Contractor in the award or performance of this Agreement or that otherwise violates any applicable requirement of Section 1-81, Broward County Code of Ordinances; or

9.2.3. By the Director of OESBD upon the disqualification of Contractor as a CBE or SBE if Contractor's status as a CBE or SBE was a factor in the award of this Agreement and such status was misrepresented by Contractor, or upon the disqualification of one or more of Contractor's CBE or SBE participants by County's Director of OESBD if any such participant's status as a CBE or SBE firm was a factor in the award of this Agreement and such status was misrepresented by Contractor during the procurement or the performance of this Agreement.

9.3. Notice of termination shall be provided in accordance with the "Notices" section of this Agreement except that notice of termination by the County Administrator to protect the public health, safety, or welfare may be oral notice that shall be promptly confirmed in writing.

9.4. If this Agreement is terminated for convenience by County, Contractor shall be paid for any Services properly performed through the termination date specified in the written notice of termination, subject to any right of County to retain any sums otherwise due and payable. Contractor acknowledges that it has received good, valuable, and sufficient consideration for County's right to terminate this Agreement for convenience in the form of County's obligation to provide advance notice to Contractor of such termination in accordance with Section 9.1. Contractor further acknowledges that County would not enter into this Agreement if it did not contain a right for County to terminate for convenience if it determined that such termination was warranted under the circumstances presented.

9.5. In addition to any right of termination stated in this Agreement, County shall be entitled to seek any and all available remedies, whether stated in this Agreement or otherwise available at law or in equity.

ARTICLE 10. EQUAL EMPLOYMENT OPPORTUNITY AND CBE COMPLIANCE

10.1. 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. Contractor 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.

10.2. Contractor 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 Contractor 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.

10.3. Contractor will meet the required CBE goal by utilizing the CBE firms listed in Exhibit E (or a CBE firm substituted for a listed firm, if permitted) for twenty-five percent (25%) of total Services (the "Commitment").

10.4. In performing the Services, Contractor shall utilize the CBE firms listed in Exhibit E 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, Contractor shall enter into formal contracts with the firms listed in Exhibit E and, upon request, shall provide copies of the contracts to the Contract Administrator and OESBD.

10.5. Each CBE firm utilized by Contractor to meet the CBE goal must be certified by OESBD. Contractor shall inform County immediately when a CBE firm is not able to perform or if Contractor believes the CBE firm should be replaced for any other reason, so that OESBD may review and verify the good faith efforts of Contractor to substitute the CBE firm with another CBE firm, as applicable. Whenever a CBE firm is terminated for any reason, Contractor 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 if the termination results from modification of the Scope of Services and no CBE firm is available to perform the modified Scope of Services; in which event, Contractor shall notify County, and OESBD may adjust the CBE goal by written notice to Contractor. Contractor shall not terminate a CBE firm for convenience without County's prior written consent, which consent shall not be unreasonably withheld.

10.6. The Parties stipulate that if Contractor fails to meet the Commitment, the damages to County arising from such failure are not readily ascertainable at the time of contracting. If Contractor fails to meet the Commitment and County determines, in the sole discretion of the OESBD Program Director, that Contractor failed to make Good Faith Efforts (as defined in Section 1-81, Broward County Code of Ordinances) to meet the Commitment, Contractor shall pay County liquidated damages in an amount equal to fifty percent (50%) of the actual dollar amount by which Contractor 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 Contractor'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 Contractor to meet the Commitment.

10.7. Contractor 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 Contractor and shall include a deadline for Contractor to notify County in writing if Contractor concludes that the modification exceeds the authority under this section. Failure of Contractor to timely notify County of its conclusion that the modification exceeds such authority shall be deemed acceptance of the modification by Contractor.

10.8. County may modify the required participation of CBE firms 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. Contractor 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.

10.9. Contractor shall provide written monthly reports to the Contract Administrator attesting to Contractor's compliance with the CBE goal stated in this article. In addition, Contractor shall allow County to engage in onsite reviews to monitor Contractor's progress in achieving and maintaining Contractor'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.

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

ARTICLE 11. MISCELLANEOUS

11.1. Contract Administrator Authority. The Contract Administrator is authorized to coordinate and communicate with Contractor 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 in connection with the day-to-day management of this Agreement. The Contract Administrator may approve in writing minor modifications to the Scope of Services provided that such modifications do not increase the total cost to County or waive any rights of County.

11.2. Rights in Documents and Work. Any and all reports, photographs, surveys, documents, materials, or other work created by Contractor in connection with performing Services shall be owned by County, and Contractor hereby transfers to County all right, title, and interest, including any copyright or other intellectual property rights, in or to the work. Upon termination of this Agreement, any reports, photographs, surveys, and other data and documents prepared by Contractor, whether finished or unfinished, shall become the property of County and shall be delivered by Contractor to the Contract Administrator within seven (7) days after termination of this Agreement. Any compensation due to Contractor may be withheld until all documents are received as provided in this Agreement. Contractor shall ensure that the requirements of this section are included in all agreements with its Subcontractor(s).

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

11.3.1. Keep and maintain public records required by County to perform the Services;

11.3.2. 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;

11.3.3. 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

11.3.4. Upon completion or termination of this Agreement, transfer to County, at no cost, all public records in possession of Contractor or keep and maintain public records required by County to perform the services. If Contractor transfers the records to County, Contractor shall destroy any duplicate public records that are exempt or confidential and exempt. If Contractor keeps and maintains the public records, Contractor 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.

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. Contractor will provide any requested records to County to enable County to respond to the public records request.

Any material submitted to County that Contractor contends constitutes or contains trade secrets or is otherwise exempt from production under Florida public records laws (including Chapter 119, Florida Statutes) ("Trade Secret Materials") must be separately submitted and conspicuously labeled "EXEMPT FROM PUBLIC RECORD PRODUCTION – TRADE SECRET." In addition, Contractor 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 Section 812.081, Florida Statutes, and stating the factual basis for same. If a third party submits a request to County for records designated by Contractor 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 Contractor. Contractor 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 any Trade Secret Materials in response to a records request by a third party.

IF CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO CONTRACTOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS AGREEMENT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT (954) 468-3501, JORHERNANDEZ@BROWARD.ORG, 1850 ELLER DR., SUITE 603, FORT LAUDERDALE, FLORIDA 33316.

11.4. Audit Rights and Retention of Records. County shall have the right to audit the books, records, and accounts of Contractor and its Subcontractors that are related to this Agreement. Contractor and its Subcontractors shall keep such books, records, and accounts as may be necessary in order to record complete and correct entries related to this Agreement and performance under this Agreement. All such books, records, and accounts 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, Contractor or its Subcontractor shall make same available in written form at no cost to County.

Contractor and its Subcontractors shall preserve and make available, at reasonable times within Broward County, Florida, for examination and audit, all financial records, supporting documents, statistical records, and any other documents pertinent to this Agreement for at least three (3) years after expiration or termination of this Agreement or until resolution of any audit findings, whichever is longer. Any audit or inspection pursuant to this section may be performed by any County representative (including any outside representative engaged by County). Contractor hereby grants County the right to conduct such audit or review at Contractor'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 Contractor 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 Contractor in addition to making adjustments for the overcharges. Any adjustments or payments due as a result of such audit or inspection shall be made within thirty (30) days after presentation of County's findings to Contractor.

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

11.5. Independent Contractor. Contractor is an independent contractor of County, and nothing in this Agreement shall constitute or create a partnership, joint venture, or any other relationship between the Parties. In providing Services, neither Contractor nor its agents shall act as officers, employees, or agents of County. Contractor shall not have the right to bind County to any obligation not expressly undertaken by County under this Agreement.

11.6. Regulatory Capacity. Notwithstanding the fact that County is a political subdivision with certain regulatory authority, County's performance under this Agreement is as a Party to this Agreement and not in its regulatory capacity. If County exercises its regulatory authority, the exercise of such authority and the enforcement of any rules, regulation, laws, and ordinances shall have occurred pursuant to County's regulatory authority as a governmental body separate and apart from this Agreement, and shall not be attributable in any manner to County as a party to this Agreement.

11.7. Sovereign Immunity. Except to the extent sovereign immunity may be deemed to be waived by entering into this Agreement, nothing herein is intended to serve as a waiver of sovereign immunity by County nor shall anything included herein be construed as consent by County to be sued by third parties in any matter arising out of this Agreement. County is a political subdivision as defined in Section 768.28, Florida Statutes, and shall be responsible for the negligent or wrongful acts or omissions of its employees pursuant to Section 768.28, Florida Statutes.

11.8. Third-Party Beneficiaries. Neither Contractor nor County intends to directly or substantially benefit a third party by this Agreement. Therefore, the Parties acknowledge that there are no third-party beneficiaries to this Agreement and that no third party shall be entitled to assert a right or claim against either of them based upon this Agreement.

11.9. 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, hand delivery, or commercial overnight delivery, each with a contemporaneous copy via email, to the addresses listed below and shall be effective upon mailing or hand delivery (provided the contemporaneous email is also sent). The addresses for notice shall remain as set forth in this section unless and until changed by providing notice of such change in accordance with the provisions of this section.

FOR COUNTY:
Broward County Port Everglades Department
Attn: Chief Executive/Port Director
1850 Eller Drive
Fort Lauderdale, FL 33316
Email address: jdaniels@broward.org

FOR CONTRACTOR:

SP Plus Corporation
Attn: Thomas Hagerman, SVP
3340 Peachtree Road, NE, #675
Atlanta, GA 30346
Email address: thagerman@spplus.com

With copy to:
SP Plus Corporation
Attn: Legal Department
200 E. Randolph Street, #7700
Chicago, IL 60601

11.10. Assignment. All Subcontractors must be expressly identified in this Agreement or otherwise approved in advance and in writing by County's Contract Administrator. Except for subcontracting approved by County in advance, neither this Agreement nor any right or interest in it may be assigned, transferred, subcontracted, or encumbered by Contractor without the prior written consent of County. Any assignment, transfer, encumbrance, or subcontract in violation of this section shall be void and ineffective, constitute a breach of this Agreement, and permit County to immediately terminate this Agreement, in addition to any other remedies available to County at law or in equity.

11.11. Conflicts. Neither Contractor nor its employees shall have or hold any continuing or frequently recurring employment or contractual relationship that is substantially antagonistic or incompatible with Contractor's loyal and conscientious exercise of judgment and care related to its performance under this Agreement. During the term of this Agreement, none of Contractor's officers or employees shall serve as an expert witness against County in any legal or administrative proceeding in which he, she, or Contractor 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 that 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 Contractor or any persons in any way from representing themselves, including giving expert testimony in support of such representation, in any action or in any administrative or legal proceeding. If Contractor is permitted pursuant to this Agreement to utilize Subcontractors to perform any Services required by this Agreement, Contractor shall require such Subcontractors, by written contract, to comply with the provisions of this section to the same extent as Contractor.

11.12. Materiality and Waiver of Breach. Each requirement, duty, and obligation set forth in this Agreement was bargained for at arm's-length and is agreed to by the Parties. Each requirement, duty, and obligation set forth in this Agreement is substantial and important to the formation of this Agreement, and each is, therefore, a material term of this Agreement. County's failure 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 of a provision of this Agreement shall not be deemed a waiver of any subsequent breach and shall not be construed to be a modification of the terms of this Agreement. To be effective, any waiver must be in writing signed by an authorized signatory of the Party granting the waiver.

11.13. Compliance with Laws. Contractor and the Services must comply with all applicable federal, state, and local laws, codes, ordinances, rules, and regulations including, without limitation, American with Disabilities Act, 42 U.S.C. § 12101, Section 504 of the Rehabilitation Act of 1973, and any related federal, state, or local laws, rules, and regulations.

11.14. Severability. If 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.

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

11.16. Interpretation. The titles and 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. Whenever reference is made to a section or article of this Agreement, such reference is to the section or article as a whole, including all of the subsections of such section, unless the reference is made to a particular subsection or subparagraph of such section or article. Any reference to "days" means calendar days, unless otherwise expressly stated. Any referenced to "business day" means any calendar day other than federal and County holidays, Saturdays, and Sundays.

11.17. Priority of Provisions. If there is a conflict or inconsistency between any term, statement, requirement, or provision of any document or exhibit attached to, referenced by, or incorporated in this Agreement and any provision of Articles 1 through 11 of this Agreement, the provisions contained in Articles 1 through 11 shall prevail and be given effect.

11.18. Law, Jurisdiction, Venue, 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 exclusive venue for any lawsuit arising from, related to, or in connection with this 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 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, CONTRACTOR AND COUNTY HEREBY EXPRESSLY WAIVE ANY RIGHTS EITHER PARTY MAY HAVE TO A TRIAL BY JURY OF ANY CIVIL LITIGATION RELATED TO THIS AGREEMENT. IF A PARTY FAILS TO WITHDRAW A REQUEST FOR A JURY TRIAL IN A LAWSUIT ARISING OUT OF THIS AGREEMENT AFTER WRITTEN NOTICE BY THE OTHER PARTY OF VIOLATION OF THIS SECTION, THE PARTY MAKING THE REQUEST FOR JURY TRIAL SHALL BE LIABLE FOR THE REASONABLE ATTORNEYS' FEES AND COSTS OF THE OTHER PARTY IN CONTESTING THE REQUEST FOR JURY TRIAL, AND SUCH AMOUNTS SHALL BE AWARDED BY THE COURT IN ADJUDICATING THE MOTION.**

11.19. Amendments. No modification, amendment, or alteration in the terms or conditions contained in this Agreement shall be effective unless contained in a written document prepared with the same or similar formality as this Agreement and executed by duly authorized representatives of County and Contractor.

11.20. Prior Agreements. This Agreement represents the final and complete understanding of the Parties regarding the subject matter 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.

11.21. HIPAA Compliance. County has access to protected health information ("PHI") that is subject to the requirements of 45 C.F.R. Parts 160, 162, and 164 and related regulations. If Contractor is considered by County to be a covered entity or business associate or is 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"), Contractor shall fully protect individually identifiable health information as required by HIPAA or HITECH and, if requested by County, shall execute a Business Associate Agreement in the form set forth at http://www.broward.org/Purchasing/Pages/StandardTerms.aspx. The County Administrator is authorized to execute a Business Associate Agreement on behalf of County. Where required, Contractor shall handle and secure such PHI in compliance with HIPAA, HITECH, and related regulations and, if required by HIPAA, HITECH, or other laws, include in its "Notice of Privacy Practices" notice of Contractor's and County's uses of client's PHI. The requirement to comply with this provision, HIPAA, and HITECH shall survive the expiration or earlier termination of this Agreement. Contractor shall ensure that the requirements of this section are included in all agreements with its Subcontractors.

11.22. Payable Interest

11.22.1. Payment of Interest. County shall not be liable to pay any interest to Contractor for any reason, whether as prejudgment interest or for any other purpose, and in furtherance thereof Contractor 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 for interest, including for post-judgment interest, if such application would be contrary to applicable law.

11.22.2. 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, one quarter of one percent (0.25%) simple interest (uncompounded).

11.23. Incorporation by Reference. Any and all Recital clauses stated above are true and correct and are incorporated in this Agreement by reference. The attached Exhibits are incorporated into and made a part of this Agreement.

11.24. Prevailing Wage Requirement. If construction work in excess of Two Hundred Fifty Thousand Dollars ($250,000.00) is required of, or undertaken by, Contractor as a result of this Agreement, Section 26-5, Broward County Code of Ordinances, shall be deemed to apply to such construction work. Contractor shall fully comply with the requirements of such ordinance.

11.25. Counterparts and Multiple Originals. 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.

11.26. Use of County Logo. Contractor 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.

11.27. Drug-Free Workplace. To the extent required under Section 21.31(a)(2), Broward County Administrative Code, or Section 287.087, Florida Statutes, Contractor certifies that it has a drug-free workplace program that it will maintain such drug-free workplace program for the duration of this Agreement.

11.28. Living Wage Requirement. If Contractor is a "covered employer" within the meaning of the Broward County Living Wage Ordinance, Sections 26-100 through 26-105, Broward County Code of Ordinances, Contractor agrees to and shall pay to all of its employees providing "covered services," as defined in the ordinance, a living wage as required by such ordinance, and Contractor shall fully comply with the requirements of such ordinance. Contractor shall ensure all of its Subcontractors that qualify as "covered employers" fully comply with the requirements of such ordinance.

11.29. Workforce Investment Program. This Agreement constitutes a "Covered Contract" under the Broward Workforce Investment Program, Section 19.211, Broward County Administrative Code ("Workforce Investment Program"). Contractor affirms it is aware of the requirements of the Workforce Investment Program and agrees to use good faith efforts to meet the First Source Referral Goal and the Qualifying New Hires Goal as set forth the Workforce Investment Program, including by (a) publicly advertising exclusively with CareerSource Broward for at least five (5) business days any vacancies that are the direct result of this Agreement (whether those vacancies are with Contractor or its Subcontractors) and using good faith efforts to interview any qualified candidates referred under the Workforce Investment Program, and (b) using good faith efforts to hire Qualifying New Hires, as defined by the Workforce Investment Program, for at least fifty percent (50%) of the vacancies that are the direct result of this Agreement. Until at least one year after the conclusion of this Agreement, Contractor shall maintain and make available to County upon request all records documenting Contractor's compliance with the requirements of the Workforce Investment Program, and shall submit the required Workforce Investment Reports to the Contract Administrator annually by January 31 and within thirty (30) days after the conclusion of this Agreement. Failure to demonstrate good faith efforts to meet the First Source Referral Goal and the Qualifying New Hires Goal shall constitute a material breach of this Agreement.

11.30. Additional Security Requirements. Contractor shall comply with the Port Everglades Security Requirements attached hereto as Exhibit F.

(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 _______________, 20__, and SP PLUS CORPORATION, signing by and through its Vice President 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___________________________
Mayor

____ day of _______________, 20__

Approved as to form by
Andrew J. Meyers
Broward County Attorney
Port Everglades Department
1850 Eller Drive, Suite 502
Fort Lauderdale, Florida 33316
Telephone: (954) 523-3404
Telecopier: (954) 468-3690

By______________ 10/6/2020
Al A DiCalvo (Date)
Assistant County Attorney

By______________ 10/6/2020
Russell J. Morrison (Date)
Senior Assistant County Attorney

AAD
SPPlus-ParkingMgmtAgmt(RFP-PNC2116816P1)_v6Final-2020-1005
9/30/20, 10/5/20
#19-3000.03

AGREEMENT BETWEEN BROWARD COUNTY AND SP PLUS CORPORATION FOR PARKING MANAGEMENT SERVICES FOR PORT EVERGLADES (RPF NO. PNC2116816P1)

CONTRACTOR

WITNESSES:

____
Signature

Jheimy VÁsquez
Print Name of Witness above

____
Signature

Giovanni Garzón
Print Name of Witness above

SP PLUS CORPORATION

By: _______________________________
Authorized Signor

Chester Escobar, Vice President
Print Name and Title

5th day of October, 20 20

ATTEST:

____
Corporate Secretary or other person authorized to attest

(CORPORATE SEAL OR NOTARY)

Notary Public State of Florida
Suray Delgado Jimenez
My Commission GG 972011
Expires 03/22/2024

NOTARY PUBLIC STATE OF FLORIDA

Exhibit A
Scope of Services
Parking Management Services for Port Everglades
PNC2116816P1

Responsibilities of Contractor

1. **General Terms**

During the term of this Agreement, SP Plus Corporation ("Contractor") shall manage and operate all parking operations at the Parking Facilities at Port Everglades, including shuttle bus service and additional services, as may be specified, in a safe, efficient, and cost-effective manner. Contractor shall provide the highest level of professional management and operational services on a continuous basis, twenty-four (24) hours a day, seven (7) days a week, 365 days a year including holidays.

2. **Adding or Removing Available Parking Spaces**

2.1. County may, in its absolute discretion during the term of this Agreement, unilaterally add to or remove Parking Facilities (as defined in Section 3.1 below), wholly or in part.

2.2. If County takes such action, Contract Administrator shall provide Contractor with written notice of the change at least thirty (30) days prior to the change and the management fee will be adjusted as provided in Exhibit B.

3. **Facility Description**

3.1. The Port Everglades parking facilities (individually a "Parking Facility" or "Facility," and collectively "Parking Facilities" or "Facilities) are comprised of the following, totaling 4788 spaces:

3.1.1. *Northport Garage: parking garage located at 2000 Eisenhower Boulevard, Fort Lauderdale, FL 33316 with a capacity of 1,524 parking spaces.

3.1.2. T2/T4 Parking Garage: parking garage located at 2050 Eisenhower Boulevard, Fort Lauderdale, FL 33316 with a capacity of 1,818 parking spaces.

3.1.3. Midport Garage: parking garage located at 2020 Eller Drive, Hollywood, FL 33316 with a capacity of 1,966 parking spaces.

3.1.4. Surface Lot 18: parking facility adjacent to Terminal 18 located at 1901 SE 32nd Street, Hollywood, FL 33316 with a capacity of 600 parking spaces.

3.1.5. Surface Lot 19: parking facility adjacent to Terminal 19 located at 2019 Eller Drive, Hollywood, FL 33316 with a capacity of 404 parking spaces.

3.1.6. Contract Administrator will notify Contractor of other parking areas that may be temporarily designated, throughout the term of the Agreement to provide overflow parking for cruise passengers, events, cruise line shore staff (Shore Staff), or valet parking, which may require Contractor to temporarily provide parking management services. Any parking management services associated with a temporary location will be provided by Contractor with no change to the management fee.

*SP Plus will manage the Northport garage only until the T2/T4 Garage is opened. Upon completion of the T2/T4 Garage, the Northport Garage will be eliminated from the Parking Facilities. For the purposes of this agreement, the Northport Garage is being replaced by the T2/T4 Garage. The spaces located within the T2/T4 Garage will be used in the calculation of the total number of spaces available in Parking Facilities at the time of this Agreement. The spaces located in the Northport Garage will not be included in the calculation of the total number of spaces available in Parking Facilities.

4. **Parking Management Office**
County will provide Contractor with an onsite parking management office (Office). The current Office is located in a building in front of the Midport Garage. Upon completion of the T2/T4 Garage, the Office will be relocated to the first floor of the T2/T4 Garage.

5. **Hours of Operation**
Contractor is responsible for the management and operations of all Parking Facilities twenty-four (24) hours a day, seven (7) days a week, 365 days a year including holidays. The Contract Administrator and Contractor will determine which Parking Facilities will be open or closed based on the parking demands of the business operations at Port Everglades.

6. **Parking Fees**
For each Parking Facility, fees will be in accordance with the fee schedule set forth in Port Everglades' Tariff No. 12, Item No. 1135, as may be amended from time to time.

7. **General Management - Contractor shall:**

7.1. Provide parking management services at each Facility in a manner to maximize revenues and minimize costs, while providing the highest level of professional and courteous customer service in all phases of parking transactions and operations.

7.2. Manage all parking operations and render other parking related services as may be requested by Contract Administrator.

7.3. Manage vouchers and validations for parking for Shore Staff or special events as requested by Contract Administrator. At the sole direction of the Contract Administrator, Contractor will print parking vouchers to be applied to patron parking tickets for authorized discounted parking fees. Contractor will be responsible for reporting the number of vouchers printed and number of vouchers validated and submit a report with this information to the Contract Administrator and designated Port Everglades Finance Division staff daily, as applicable, via e-mail, in an acceptable format approved by the Contract Administrator.

7.4. Manage and operate the County-owned Parking Access and Revenue Control System (PARCS) at Parking Facilities. The major components include Entry/Exit Lane Equipment, Intercom System, Pay-On-Foot Stations, Vehicle Count System, License Plate Recognition (LPR), License Plate Pay-By-Phone Service, Reservation System, and Manual Handheld Credit Card Machines. County may add additional components to PARCS during the course of this Agreement.

7.4.1. Contractor shall monitor the intercom system that is integrated in PARCS and respond to calls for assistance received from guest already in a Parking Facility in five (5) minutes or less. Calls for assistance at an entry or exit gate should receive an immediate response

7.4.2. Contractor shall report any known malfunctions in PARCS withing ten (10) minutes of discovery to Contract Administrator.

7.5. Open and close Parking Facilities for special events, cleaning and maintenance, repairs, and construction activities, as directed by Contract Administrator.

7.6. Prepare Management and Operations Plan.

7.7. Respond to on site patron complaints timely and submit monthly Incident Reports accompanied by Contractors' resolution of any such complaints to Contract Administrator. Incident Report must provide patron information, date, description of complaint, staff/witness, staff handling complaint, and resolution. If the complaint is transferred to Contract Administrator, update log to reflect transfer and resolution.

7.7.1 For patron questions or complaints submitted in writing to Contractor, Contractor will provide a written response within three (3) business days following submission.

7.8 Provide and deploy portable message signs (Wind-Master or compatible, A Frame) as directed by Contract Administrator.

7.9 As may be requested by the Contract Administrator, Contractor shall prepare monthly, quarterly, and annual reports detailing revenue information, operational statistics, budget information, daily utilization, and historical comparison and submit to the Contract Administrator.

7.10 Contractor possesses specialized knowledge of the parking industry and management of parking facilities. Contractor shall strive to develop and partner with Port Everglades to implement innovative programs that may include promotional activities, products, or services, that will increase revenue and enhance the experience of patrons utilizing the Parking Facilities.

7.11 The Contractor shall submit a written business plan for each new product or service to the Contract Administrator for approval, and the implementation of new products or services shall be at the sole risk of Contractor. The implementation of any new products or services by Contractor must be approved in writing, in advance, by the Contract Administrator.

7.12 Attend parking-related meetings and events as directed by Contract Administrator.

7.13 Not place any advertising in any Parking Facility without the prior written consent of Contract Administrator.

7.14 Be responsible for maintaining a record of active and deactivated proximity cards for all Parking Facilities and reporting monthly via e-amil to Contract Administrator. New activations and deactivations will be provided to Contractor via e-mail by the Contract Administrator.

8 **Staffing**

8.1 Contractor shall provide qualified and adequate staffing at each Parking Facility to facilitate activities related to parking and for valet parking, when required.

8.1.1 Contractor shall assign a Parking Facilities manager to lead the operation and management of Parking Facilities. Contractor shall assign a qualified Assistant Parking Facilities manager to be available in the absence of the Parking Facilities manager. Either the Parking Facilities manager or Assistant Parking Facilities manager must be on-site as scheduled, or available on-call, twenty-four (24) hours a day, seven (7) days a week, 365 days a year including holidays.

8.1.2 Contractor's appointment of the Parking Facilities manager and Assistant Parking Facilities manager shall be subject to the prior written approval of Contract Administrator, in his or her sole discretion.

8.1.3 Contractor shall annually submit resumes of all its management and supervisory level employees thirty (30) days prior to the first day of each Agreement year or upon replacement of any referenced employee during the term of the agreement.

8.1.4 Contractor shall provide customer service representatives and traffic attendants for Parking Facilities according to passenger traffic and business demands.

8.1.5 Contractor shall maintain a friendly and cooperative relationship with other Port tenants on the premises of Port Facilities, and shall not engage in open or public disputes, disagreements, or conflicts, tending to deteriorate the quality of the services offered at Parking Facilities or be incompatible to the best interest of the public or County.

8.1.6 Contractor shall provide its employees with uniforms that promote consistency and visibility to cruise passengers, visitors, and Port employees. All employees shall be required to obtain and prominently wear a Port ID badge displaying their name.

8.1.7 All Contractor's employees must pass a Florida Department of Law Enforcement (FDLE) background check in order to receive a Port ID badge. Contractor shall obtain background checks for each of its employee from the FDLE or from other sources approved by the Contract Administrator. Contractor shall submit the written results of the background checks if requested by the Contract Administrator. The Contract Administrator shall have the right to approve or disapprove all personnel.

8.1.8 The Contractor's subcontractor, in similar fashion to the Contractor as described in above, must obtain background checks from the State of Florida Department of Law Enforcement or from other services approved by the Contract Administrator. Contractor shall submit the written results of the background checks, on behalf of Subcontractor, if requested by the Contract Administrator. The Contract Administrator shall have the right to approve or disapprove all personnel.

8.1.9 Contractor shall inform each of its employees of the pertinent County rules and regulations and the applicable provisions of this Agreement.

8.1.10 Contractor's employees are required to review customer service training materials provided by COUNTY.

8.1.11 Contractor shall use only the Parking Facilities designated by the Contract Administrator for use by its employees and Subcontractors only during regularly scheduled working hours at Parking Facilities.

8.1.12 Hire and manage custodial service for all Parking Facilities. Including but not limited to, cleaning all surfaces, sidewalks leading to, from and within the Parking Facilities, exit booths, facility entrance and exit lanes, ramps, stairwells, vestibules, PARCS equipment including Pay-on-Foot stations, and parking administrative offices.

8.1.13 Hire and manage an accounting and staffing firm to provide auditors to audit and oversee gross revenue cash receipts, deposits, and credit card reconciliation for the daily operations of the Parking Facilities in accordance with Government Auditing Standards.

8.1.13.1 Contractor may ask the accounting and staffing firm to provide staffing for non-revenue related tasks subject to the advanced written approval of Contract Administrator.

8.1.14 Contractor shall immediately remove and keep removed from Parking Facilities any employee who participates in illegal acts, violates County rules and regulations, or provisions of this Agreement, or who, in the opinion of Contractor or Contract Administrator is otherwise detrimental to the operations of the Parking Facilities.

8.1.15 If theft, fraud, or embezzlement or suspicion of same occurs, it is Contractor's responsibility to immediately notify Contract Administrator, via phone or text, of the incident or suspected incident as soon as Contractor becomes aware. Following the immediate notification, Contractor shall provide via email, courier, or mail full disclosure including, but not limited to, copies of police reports of investigation, reports to bonding and insurance companies, bonding and insurance companies' findings, and reports of any action taken against an employee. Contractor shall cooperate with the prosecution of any employee alleged to be involved in theft, fraud, embezzlement, or any similar activity.

8.1.16 All employees of Contractor assigned to work under this Agreement must sign a pre-employment statement, provided by Contractor, stating they are aware they will be fully investigated and may be prosecuted to the fullest extent of the law for any theft, fraud, embezzlement, or similar activity.

9 Monthly Staffing Plan

9.1 Contractor shall develop and submit by the 5th of each month, a written staffing plan to Contract Administrator, for approval, outlining the base number of employees the Contractor will use for the following month to operate each Parking Facility during various hours of the day.

9.1.1 The proposed staffing plan shall be based upon generally anticipated normal operations at each Parking Facility, as well as staffing needs during peak seasons. The staffing plan shall include the classifications of employee position and the responsibilities of each position.

9.1.2 Contractor’s proposed staffing plan shall be reviewed by Contract Administrator by the fifteenth (15th) of each month prior to the month for which the services will be rendered to ensure all peak or slow periods and holidays are properly covered. Contract Administrator and Contractor will discuss the proposed staffing plan, and the Contract Administrator will notify the Contractor in writing via e-mail with an authorization to proceed with the approved staffing plan. Changes to the staffing plan must be pre-approve in writing by the Contract Administrator.

9.2 Deep Cleaning. Contract Administrator will notify Contractor in writing, via e-mail, ("Notification") when Contractor is required to deep clean certain areas identified in the Notification, Contractor shall follow the disinfecting protocols identified below for Deep Cleaning.

9.2.1 Disinfecting Protocols for Deep Cleaning. To perform Deep Cleaning, Contractor will be required to use cleaning products that are recommended by the Center for Disease Control (CDC) and approved by the Environmental Protection Agency (EPA) as identified on List N: Disinfectants for Use Against SARS-CoV-2 or any other EPA product list issued to address public health emergencies or pandemics. Use of these products must be as described by the EPA. Contractor shall prepare and submit in writing, via e-mail, their proposed staffing plan to meet the level of the requested Deep Cleaning service.

9.2.2 Contract Administrator and Contractor will discuss their proposed staffing plan, and the Contract Administrator will notify the Contractor in writing, via e-mail, with an authorization to perform the requested Deep Cleaning services as agreed upon. Deep Cleaning services will be provided at the same hourly rate as set forth under reimbursable expenses for Contract Cleaning custodial services inclusive of cleaning supplies in Exhibit B.

9.3 Staffing under unforeseen conditions will require a revision to the then current staffing plan. Upon notification by the Contract Administrator that an unforeseen condition exists, Contractor will submit a revised staffing plan within seven (7) business days for review and approval by the Contract Administrator.

10 Shuttle Bus Services

10.1 Contractor shall be responsible for contracting with a subcontractor to provide a readily available shuttle bus service fleet to meet the scheduling requirements for cruise passenger, Shore Staff, or special events, 365 days per year. Contractor will serve as the liaison for the Subcontractor between the Contract Administrator in conjunction with Ports' Business Development Division. Shuttle bus service will be provided by Contractor on an actual cost basis, as invoiced to the Contractor by the Subcontractor, as detailed in Exhibit B.

10.2 Ports' Business Development Division in conjunction with the Contract Administrator will provide Contractor a cruise schedule to forecast the number of wheelchair accessible and non-wheelchair accessible vehicles required for the cruise season. Ports' Business Development Division in conjunction with the Contract Administrator will confirm or may provide revisions to the schedule a on a weekly basis.

10.3 Shuttle bus service fleet shall consist of: Mini-Buses, with interior luggage storage and a capacity of 14 to 17-passenger, and Mid-Size buses, with rear luggage storage and a capacity of 23 to 30-passenger. The fleet shall include a minimum of five (5) Mini-Buses that are wheelchair accessible vehicles. Shuttle bus service fleet shall also have available Motor Coaches, with a capacity of 40 to 55-passenger with panoramic front window for tours and special events, as requested by Ports' Business Development Division in conjunction with Contract Administrator. Contractor will be notified in advance of any upcoming special event or tour date. Port will provide parking spaces on the first floor of the Midport Parking Garage for Contractor to keep the Subcontractor's shuttle bus service vehicles that are to be used only to provide shuttle bus services within Port Everglades.

10.4 Shuttle bus service operators must provide cruise passengers with assistance, as needed, with baggage handling, and boarding and exiting of vehicles. Shuttle bus services for cruise or Shore Staff will not require baggage handling.

11 Other Subcontracted Services:

11.1 Services provided by Contractor shall not be performed by any party other than the Contractor without prior written approval from the Contract Administrator.

11.2 Contractor may provide valet parking as a subcontracted service when requested by Port tenants or Contract Administrator as follows:

11.2.1 Valet service will be provided on an actual cost basis with no allowance for any additional Management Fee.

11.2.2 Contractor shall invoice the valet parking service provider for use Parking Facilities using the parking rates published in Tariff No. 12, Item No. 1135. Contractor shall be responsible for all costs associated with valet parking service.

11.2.3 Contractor shall request approval from the Contract Administrator no less than seven (7) days prior to the date valet services will be needed. Such notice shall include the relevant date(s), hour(s), and location(s) needed for valet parking service operations.

12 Equipment and Furnishing Ownership

12.1 County owns all existing equipment and furnishings that are located at Parking Facilities and Office.

12.1.1 Title to all items that are paid for by County as a Reimbursable Expense shall be vested in County, upon payment of such Reimbursable Expense to the Contractor.

12.1.2 Contractor shall not dispose of any equipment or furnishings except in accordance with County procedures and with the prior written consent from Contract Administrator.

12.1.3 Work performed by Contractor must be done in accordance with formal procedures and training provided by TIBA Parking Systems, LLC (TIBA). Work performed by Contractor on the PARCS equipment, outside the formal procedures and training by TIBA, are subject to the provisions in 13.5.

12.2 County motor vehicle(s) may be assigned to Contractor during the course of this Agreement.

12.2.1 Contractor’s or Subcontractor’s employees must receive authorization to drive County or personal vehicles in the course of Facilities operations. Continued authorization is subject to the maintenance of proper licenses and a satisfactory driving record as reported by the State and County.

12.2.2 Contractor’s employees are not authorized to operate County vehicles or equipment for private purposes; therefore, County accepts no liability for the Contractor’s employees driving County vehicles for their personal use, such as take-home, or errands outside of business operations.

13 Inspections and Repairs

13.1 Contractor shall manage, troubleshoot, and provide routine maintenance on the exterior of PARCS, which shall include wiping down all PARCS equipment, minor repair of broken gate arms, loading of tickets, clearing ticket jams, proximity card readers and pay-on-foot stations.

13.1.1 Contractor shall perform inspections of Parking Facilities to ensure all PARCS equipment, elevators, lighting fixtures and other infrastructures are in proper working condition and report any deficiencies to Contractor Administrator.

13.1.2 Preventive maintenance, beyond routine maintenance, and repairs of the PARCS is the responsibility of the Port's contracted certified service provider.

13.2 Contractor shall perform regular Parking Facility inspections to ensure all safety standards are met or exceeded. Inspections should include surface areas, doors/walls, stairwells etc. Attention should be given to identify areas that are isolated where it may be more likely for damage, theft of vehicles, equipment, or vandalism may occur.

13.2.1 Any hazardous conditions found must immediately be reported to Contract Administrator. Contractor shall use Port and/or vendor-provided visible barriers to protect and ensure safety of patrons. .

13.3 If structural or permanent portions of any Parking Facilities is damaged by fire or other casualty, the Contractor shall give immediate notice thereof to Contract Administrator, and the same shall be repaired at the expense of County without unreasonable delay unless County determines that the damage is so extensive that repair is not feasible.

13.3.1 The management obligations of the Contractor hereunder shall not cease or be abated during any repair period.

13.3.2 If County elects to repair or rebuild the damage to any Parking Facility, County shall notify the Contractor of such intention within sixty (60) days after the date of the damage; otherwise, the Facility will be removed from the list of Parking Facilities as provided in Exhibit B.

13.4 Contractor shall notify Contract Administrator in writing when striping, re-striping, re-lamping, or other maintenance item becomes necessary in any Parking Facility.

13.5 Contractor shall not cause to be damaged or destroyed any County fixtures, equipment, furnishing, or property. If Contract Administrator determines that any County fixtures, equipment, furnishings, or property was destroyed or damaged by Contractor, Contractor shall make all repairs or replacements of same at the Contractor's own expense within thirty (30) days of notification by Contract Administrator.

13.6 County shall not be liable to the Contractor for any damage caused by disrepair of any kind of County fixtures, equipment, or property until County has had reasonable opportunity to perform repairs after being notified in writing of the need for same by Contractor.

13.7 County shall not be liable to the Contractor for any damage to merchandise, trade fixtures, or personal property of the Contractor caused by water leakage from any cause or source whatsoever, including, but not limited to, a Facility's roof, water lines, sprinkler, or heating and air conditioning equipment.

13.8 Contractor shall process claims and report in writing, satisfactory to Contract Administrator, all claims made for losses or damages to or within all Parking Facilities and assigned areas.

13.9 Contractor shall, to the extent of its actual knowledge, promptly report any suspicious or illegal activities, and incidents involving property damages to Parking Facilities to the Contract Administrator. A written report of every reported event shall be kept on file by Contactor unless otherwise specified by Contract Administrator and shall be provided to Contract Administrator upon request.

14 Management and Operations Plan

14.1 Within thirty (30) business days after the Effective Date, the Contractor shall prepare and submit in writing to the Contract Administrator a written Management and Operations Plan ("Plan").

14.2 Contractor shall provide the Contract Administrator with emergency telephone numbers where the Contractor's manager or designee may be reached on a 24-hour basis.

14.3 Contract Administrator must approve all revisions and updates to the Plan in writing. Contractor's failure to comply with the Plan that has been approved by the Contract Administrator shall be a default under this Agreement, entitling the County to exercise any and all remedies available hereunder. The burden of proving compliance with the Plan rests with the Contractor.

14.4 Reasonable questions or complaints regarding the Contractor's compliance with the Plan, whether raised by patron's or Contract Administrator's own initiative, or otherwise, may be submitted in writing by the Contract Administrator to Contractor, and Contractor's written response must be provided to the Contract Administrator within seven (7) days thereafter. In addition, at Contract Administrator's request, Contractor shall meet with the Contract Administrator to review any complaints or concerns and to promptly correct any deficiencies.

14.5 Contractor shall provide the Contract Administrator with a written emergency evacuation and continuity of operations plan ("COOP"), outlining the steps and process for resumption of business following major business disruptions. The COOP shall detail the procedures and actions to be taken by the Contractor before, during and after an event. The COOP is to be annually updated and submitted to the Contract Administrator.

15 Operating Budget

15.1 Subsequent to the first year of the Agreement, in accordance with the County's annual budget preparation schedule, prior to March 31st of each year, Contract Administrator and Contractor shall meet to jointly prepare the annual operating expense budget for the next County fiscal year, October 1st through September 30th, using the annual operating expense budget form similar to Attachment 1 in Exhibit B. The Contract Administrator will approve the jointly prepared annual operating expense budget form in writing.

15.2 The annual operating expense budget will be subject to review from time to time, if requested by either the Contractor or the Contract Administrator. All approvals or revisions of said annual operating expense budget by the Contract Administrator shall be set forth in writing and shall thereafter be binding upon the Contractor.

15.3 The approved annual operating expense budget may be increased or decreased by the Contract Administrator from time to time, but only if and to the extent that Contract Administrator in its sole discretion, deems such revisions necessary and appropriate under this Agreement.

16 Monthly Reports

On or before the fifteenth (15th) day of each calendar month, Contractor shall submit to the Contract Administrator a written monthly revenue report and monthly expense report along with supporting documentation, by category of parking services, certified by an officer of the Contractor on a form approved in advance by the Contract Administrator. This report shall serve as a summary of parking gross Revenues and Reimbursable Expenses.

17 Unaccounted Tickets

17.1 The Contractor will be invoiced for unaccounted tickets at the maximum daily rate of applicable Parking Facility per ticket for all tickets over one percent (1%) of tickets issued each month. Contract Administrator will notify Contractor in writing when unaccounted tickets exceed 1%. Contractor will have five (5) business days to submit documentation to dispute the number of unaccounted tickets. If Contractor disputes the number of unaccounted tickets the Contract Administrator, after review of the dispute documentation, will determine if the Contractor will be invoiced for the unaccounted tickets. If the Contractor fails to dispute the number of unaccounted tickets within the five (5) business days, the Contract Administrator shall invoice Contractor for the amount of the unaccounted tickets.

17.2 Contractor's procedure for unaccounted tickets will be incorporated by Contractor into the Management and Operations Plan.

18 Revenues

18.1 All gross Revenues derived from the Contractor's performance of services shall belong to County and shall be held in trust by the Contractor while the funds are in its custody and control.

18.2 Should any gross Revenues be lost or stolen, or otherwise removed without the prior authorization of County, from the custody and control of the Contractor prior to their deposit in the bank account designated by County, the Contractor shall be responsible for and shall deposit in said account a like sum of monies within forty eight (48) hours of such loss, theft, or removal.

18.3 Should said loss, theft, or removal be insured or otherwise secured by the Contractor, payments made to County on account thereof shall, if appropriate, be reimbursed to the Contractor.

19 Revenue Collection and Control

19.1 Contractor shall be the merchant of record for all parking transactions and shall contract with a credit card clearinghouse, approved by Contract Administrator, compatible with the Parking Facilities' PARCS, capable of fully processing a credit card transaction and with transaction fees that are competitive and acceptable to the Contract Administrator. The Parking Facilities' PARCS shall be able to accept, at a minimum, MasterCard, Visa, Discover, and American Express.

19.2 Contractor shall obtain appropriate certifications and maintain Payment Card Industry ("PCI") Data Security Standards ("DSS") Best Practices, as applicable, when entering into any agreements with third parties for the benefit of the County.

19.3 Contractor further agrees that its employees, agents, and Subcontractors will follow PCI-DSS Best Practices, as applicable (Exhibit "H").

19.4 Contractor shall resolve fraud problems at the sole expense of the Contractor unless the fraud is solely attributable to the negligence or willful misconduct of County, its employees, or contractors. In a case where the fraud is attributable to both Parties, cost shall be shared.

19.5 Contractor shall assume all financial responsibility for loss of funds or non-collected funds, except that Contractor shall not be responsible for non-collected funds if, at the sole but reasonable discretion of the Contract Administrator, Contractor shows it diligently attempted to collect such funds in a manner satisfactory to the Contract Administrator.

19.6 If Contractor charges any patron a price in excess of the sparking rates, the amount by which the actual charge exceeds the parking rate shall constitute an overcharge, which upon demand by the patron or by the Contract Administrator, the overcharge must be promptly refunded to the patron by the Contractor. The amount of any such refund will be deducted from the gross Revenues, provided that suitable substantiating evidence of such refund is provided to the Contract Administrator by Contractor, and provided further that the amount of said overcharge is, or has been, deposited as part of gross Revenues in the bank account designated by County.

19.7 If Contractor charges any patron a price that is less than the parking rates, the amount by which the actual charge is less than the parking rate will constitute an undercharge; an amount equivalent thereto shall be deposited by Contractor into the bank account designated by County for the deposit of gross Revenues hereunder, upon demand by Contract Administrator.

19.8 Contractor shall monitor receipts issued by the pay stations located at the Parking Facilities, for compliance with the Fair and Accurate Credit Transactions Act (FACTA) of 2003, 15 U.S.C.A. Section 1681c(g)(1).

19.8.1 Contractor shall check, on a daily basis, one (1) credit or debit card receipt issued by each of the pay stations at the Parking Facilities to determine if the card numbers and expiration dates of the cards used are properly truncated in accordance with the requirements of FACTA.

19.8.2 In the event Contractor discovers any receipt that does not comply with FACTA, Contractor shall (i) close the affected pay station; (ii) promptly report the non-compliant receipt to County and its equipment and software vendor; and (iii) re-open the affected pay station only after County and/or its equipment and software vendor produce a compliant receipt from the affected pay station verifying that the issue has been corrected.

19.8.3 All reasonable costs associated with the services set forth herein, including, but not limited to, the cost of any credit or debit card transaction made to cause the receipt to be issued for the purposes set forth herein as well as Contractor's personnel costs directly related to time spent providing such services shall be a Reimbursable Expense, as defined in Exhibit B.

20 Armored Car Service

20.1 Contractor shall collect, account for, and deposit daily, through an armored car service provided by County, by 5:00 P.M. in a bank account designated by County, in the name of Broward County Board of County Commissioners, Port Everglades Department, all gross Revenues, including sales tax, collected on the previous day from the operation of all Parking Facilities.

20.2 The armored car service shall pick up daily deposits including weekends and holidays and will deposit funds in the bank no later than 5:00 P.M. on the next business day. This schedule may be adjusted by the Contract Administrator in coordination with the armored car service and the Contractor. Any adjustment in the schedule will be communicated by the Contract Administrator via e-mail.

20.3 Contractor shall provide Contract Administrator and Port Finance Division with written daily report of deposits no later than 2:00 P.M. (EST) the next business day after each deposit.

21 Emergency Relocation

21.1 It may be necessary from time to time to relocate Contractor from a Parking Facility, or to suspend the Contractor's provision of services during periods of heightened security requirements. If such conditions exist, Contract Administrator will attempt to find suitable location(s) from which Contractor may provide Services; Contract Administrator may suspend Contractor's provision of services completely, for a period determined at the sole discretion of the Contract Administrator to be necessary to satisfy any security needs.

21.2 Contract Administrator shall give Contractor reasonable notice of any such change of location(s) or suspension of Services or any portion thereof with such notice being at least 24-hours prior written notice to Contractor, except in the case of an emergency when such notice can only be provided as soon the emergency becomes known to the Contract Administrator

22 Hazardous Materials

22.1 Contractor shall have a folder in each Facility that contains the Safety Data Sheet information for all cleaning and maintenance chemicals used on site by Contractor or its Subcontractors.

22.2 Contractor shall allow inspection by appropriate agency personnel of all Contractor’s business premises storing, using, or generating hazardous materials or bio-hazardous waste prior to the commencement of operation, and periodically thereafter to assure that adequate facilities and procedures are in place to properly manage hazardous materials and bio-hazardous waste projected to be located on the site.

22.3 Provide for proper maintenance, operation, and monitoring of hazardous materials management systems, including spill, hazardous materials and bio-hazardous waste containment systems, and equipment necessary on-site for the handling of first response to releases of oil or hazardous materials along with the capacity to employ such equipment; contract with a licensed hazardous waste transporter and/or treatment and disposal facility to assure proper pretreatment of wastewater and sludge and the treatment of disposal of hazardous waste and shall keep all required records of such transactions, including but not limited to, hazardous waste manifests.

22.4 Contractor shall describe design features, response actions, and procedures to be followed in case of spills or other accidents involving hazardous materials, bio-hazardous waste, or oil spills.

22.5 Contractor shall comply with applicable reporting provisions of Title III of Superfund Amendment and Reauthorization Act (SARA) of the Emergency Planning and Community Right-to-know Act (EPCRA) and Department of Natural Resource Protection (DNRP), Chapter 27 of Broward County Code.

Responsibilities of County

23 **General Management – County**

23.1 Maintain and make necessary structural repairs to Parking Facilities and the fixtures, including, without limitation, the interior windows, doors and entrances, floors, interior walls and ceiling, the interior surface, the surfaces of interior columns, elevators, and escalators.

23.2 Provide a PARCS or equivalent revenue control system. County shall be responsible for the replacement, repair, and modification of the PARCS or equivalent revenue control system.

23.2.1 The Contract Administrator shall enforce the County’s Enterprise Technology Services (ETS) policies, procedures, and best practices for IT Infrastructure, Applications, Security and Compliance. In addition, the Contract Administrator shall be the system administrator to maintain user privileges and access for all users of the system.

23.3 Provide public utilities service lines where water and applicable utilities will be metered for usage.

23.4 Provide elevators, fire and security alarms, permanent lighting, and air conditioning for offices.

23.5 Provide landscaping.

23.6 Provide dumpsters for the removal of trash and recycling.

23.7 Provide permanent signage for Parking Facilities and roadways.

23.8 Provide armored car service.

23.9 Provide pest control.

Exhibit B
Payment Schedule
Parking Management Services for Port Everglades
PNC2116816P1

The rates specified below shall be in effect for the entire term of the Agreement, including any renewal or extension term(s), unless otherwise 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**.

1. <u>Management Fee:</u>

1.1. Commencing on the Commencement Date, for the management and operation of the Parking Facilities, County shall pay Contractor an annual dollar amount ("Annual Management Fee"), payable in arrears in twelve (12) equal monthly payments. The initial Annual Management Fee for Agreement Year 1 shall be Seventy Thousand Three Hundred Eighty-Four Dollars ($70,384), which comes to a per space fee, based on the existing 4788 spaces, of Fourteen and 70/100 Dollars ($14.70).

The Annual Management Fee shall be for the following:

1.1.1. Administrative, bookkeeping, including all reports, excluding the annual audit report, legal costs, and expenses associated with this Agreement;

1.1.2. Operation of the County’s Parking Access Revenue Control System (PARCS);

1.1.3. Serving as the Merchant of Record for credit card processing;

1.1.4. Costs associated with long-distance phone calls and sending mail from the Parking Facilities to Contractor's corporate offices, and vice versa;

1.1.5. Costs associated with obtaining all licenses and permits required by this Agreement;

1.1.6. Costs associated with promoting the Parking Facilities including placement on Operators website: Parking.com, and pay-by-phone service, excluding credit card processing fees;

1.1.7. Management of Shuttle Bus Services; and

1.1.8. Any other costs or expenses incurred by Contractor that are necessary to provide Services under this Agreement and that are not Reimbursable Expenses.

1.2. Adjustment to the Annual Management Fee.

1.2.1. The Annual Management Fee shall remain fixed through any Agreement Year, subject to the addition or removal of parking spaces or as noted below under unforeseen conditions.

1.2.2. Notwithstanding the above, for any subsequent Agreement Year, Contractor may request a price adjustment to the Annual Management Fee. This request must be in writing and submitted to the Contract Administrator sixty (60) days prior to the renewal date, accompanied by documentation to substantiate the need for the price increase. The Contract Administrator, in its sole discretion, will determine if the requested adjustment is in the best interest of the County, based upon current market conditions and information regarding similar services in the area. Written notification will be sent to the Contractor by the Contract Administrator of the decision to accept or decline the price increase.

1.2.3. Any price adjustment requested by Contractor pursuant to above section 1.2.2 will be limited to the lesser of the change in cost of living or three percent (3%). The increase or decrease in the cost of living will be based on the Consumer Price Index ("CPI") and will be calculated as follows: the difference of CPI current period less CPI previous period, divided by CPI previous period, multiplied by one-hundred (100). The CPI current period means the most recently published monthly index prior to contract anniversary. The CPI previous period means for the same month of the prior year. All CPI indices must be obtained from the U.S. Department of Labor table for Consumer Price Index - All Urban Consumers (Series ID CUURA320SA0) for the area of Miami-Fort Lauderdale, FL (All Items), with a base period of 1982-84 = 100. If there is no change in the CPI, there will not be an increase or decrease in the Annual Management Fee. Should the Bureau of Labor Statistics cease publishing the above-described index, then such other index as may be published by the United States Department of Labor that most nearly approximates the discontinued index will be used in making the adjustments described above. Should the United States Department of Labor discontinue publication of an index approximating the index contemplated, then such index as may be published by another United States governmental agency that most nearly approximates the index first referenced above will govern and be substituted as the index to be used. Any changes to the Annual Management Fee shall be set forth in writing by the Contract Administrator as set forth in 1.2.2.

1.2.4. Any addition or removal of parking spaces will reduce or increase the Annual Management Fee based upon the number of parking spaces added or removed, times the per-space fee. The adjustment in billing will be made on the first day of the month following the date of the addition or removal of parking spaces. The Contract Administrator will notify the Contractor of the increase or reduction of parking spaces, in writing, within thirty (30) days after the addition or removal of parking spaces.

1.2.5. Unforeseen conditions may arise that will temporarily supersede the above-calculated Annual Management Fee. When for reasons beyond the control of the Port, such as but not limited to the temporary suspension of cruise services at the Port, that result in there being limited to no usage of the Parking Facilities, County and Contractor agree to a minimum flat, fixed management fee of Two Thousand Dollars ($2,000) per month. Contract Administrator will notify the Contractor in writing, via e-mail, as soon as possible when such unforeseen conditions are known, but with no less than fifteen (15) days' notice, that the County is requesting the temporary minimum flat, fixed management fee of Two Thousand Dollars ($2,000) per month to commence the first day of the month following notification.

2. **Reimbursable Expenses:**

2.1. In addition to the Annual Management Fee, County shall pay Contractor for Reimbursable Expenses incurred after the Commencement Date and before the expiration or earlier termination of this Agreement that have been approved in advance and in writing by the Contract Administrator, that have been substantiated by invoices, proof of payment, and any other documentation required by the Contract Administrator, and that are not otherwise prohibited by this Agreement. "Reimbursable Expenses" are limited to the following:

2.1.1. Salaries and wages of Contractor's staff as approved by the Contract Administrator in the Staffing Plan, as may be amended upon approval by the Contract Administrator;

2.1.2. Actual costs associated with obtaining the ticket stock and employee parking decals issued to the users of the Parking Facilities;

2.1.3. Actual costs associated with the towing of vehicles directed by the Contract Administrator;

2.1.4. Actual costs incurred for purchasing Equipment/Furnishings and the subsequent maintenance and repair of such Equipment/Furnishings;

2.1.5. Actual costs incurred for any subcontracted services needed to fulfill the requirements of this Agreement;

2.1.6. Contract cleaning for providing custodial services in the Parking Facilities, based on the actual hours of services provided at the agreed upon rate of Twenty-four and 20/100 Dollars ($24.20) per hour for Agreement Year 1; Twenty-four and 75/100 Dollars ($24.75) per hour for Agreement Year 2; and Twenty-five and 30/100 Dollars ($25.30) per hour for Agreement Year 3, which is inclusive of all equipment and supplies;

2.1.7. Contract staffing for auditors based on the actual hours of services provided at the agreed upon rate of Twenty-five and 76/100 Dollars ($25.76) per hour for Agreement Year 1; Twenty-six and 36/100 Dollars ($26.36) per hour for Agreement Year 2; and Twenty-six and 96/100 Dollars ($26.96) per hour for Agreement Year 3.

2.1.7.1. Contract staffing for non-revenue related task subject to the advanced written approval of Contract Administrator, based on the actual hours of services provided at the agreed upon rate of Twenty-one and 76/100 Dollars ($21.76) per hour for Agreement Year 1; Twenty-two and 26/100 Dollars ($22.26) per hour for Agreement Year 2; and Twenty-two and 76/100 Dollars ($22.76) per hour for Agreement Year 3.

2.1.8. Credit card transaction fees paid by Contractor on the gross revenues collected by Contractor;

2.1.9. Temporary signage for Parking Facilities and roadways;

2.1.10. Actual costs incurred for employee uniforms, including name badges, except that the County shall be entitled to a credit for uniforms not returned by terminated employees or for excessive uniform replacement (excessive shall be reasonably determined by the Contract Administrator);

2.1.11. Actual costs incurred for obtaining background checks from the State of Florida Department of Law Enforcement or from other sources approved by the Contract Administrator, including, but not limited to, drug testing and motor vehicle reports;

2.1.12. Actual costs incurred for insurance at the required coverage and deductible limits, and actual costs incurred for voluntary settlement of patrons' claims for vehicle damage or loss of contents if authorized by the Contract Administrator. Reimbursement shall not exceed Two Thousand Five Hundred Dollars ($2,500) per occurrence for each claim, and Five Thousand Dollars ($5,000.00) per occurrence for each stolen vehicle;

2.1.13. Actual costs incurred relating to the approved Hurricane contingency plan;

2.1.14. Actual costs incurred for postage directly used in the operation of the Parking Facilities;

2.1.15. Actual costs incurred for rental of vehicles, such as golf carts;

2.1.16. Actual costs incurred for fuel for vehicles used in the operation of the Parking Facilities;

2.1.17. Actual costs incurred for cellular phones and any other phones needed by Contractor's key personnel to provide Services; and

2.1.18. Unanticipated costs and expenses to the extent approved in advance and in writing by the Contract Administrator.

2.1.19. Actual costs incurred in performing the FACTA compliance services by Contractor's personnel per FACTA compliance service provided in Exhibit A, Section 19.8.

2.2. Shuttle bus services will be provided by Contractor on an actual cost basis, as invoiced to the Contractor by the Subcontractor based on the hourly rate, on the Shuttle Rate Schedule (Attachment 2). Cancellations to a scheduled shuttle bus service made with less than 36 hours' notice to Contractor may incur a charge as specified in Attachment 2. Any revisions to pricing reflected in Attachment 2 must be approved in advanced in writing by Contract Administrator.

2.3. Any unforeseen Reimbursable Expenses not included in the annual operating expense budget may be approved at the discretion of the Contract Administrator.

3. Non-Reimbursable Expenses

3.1. The approved annual operating expense budget shall specifically exclude the items listed below, which are deemed to be included in the Management Fee.

3.1.1. Administration, bookkeeping, and legal costs and expenses associated with general home office matters.

3.1.2. Travel, accommodation, and general home office expenses, including long distance calls, and postage in connection with general home office matters.

3.1.3. Late fees, interests, penalties, and fines of any kind.

3.1.4. Maintenance and repair expenses related to the Contractor's own equipment and furnishings.

4. Method of Billing and Payment:

4.1. Contractor shall submit invoices for compensation on a bi-weekly basis, provided the Services for which the invoices are submitted have been completed and the Reimbursable Expenses have been incurred. Invoices shall be on the Bi-Weekly Expense Invoice form (Attachment 3) and shall identify the Management Fee and the Reimbursable Expenses actually incurred for the previous bi-weekly period.

4.1.1. Documentation of Reimbursable Expenses, including copies of invoices stamped paid, indicating date and check numbers, shall accompany the invoice, including all premium billings and annual premium adjustment billings as submitted by the Contractor’s insurance company providing workers' compensation coverage, supporting payroll logs, and any other detailed documentation. The Contract Administrator reserves the right to request copies of the front and back of canceled checks prior to reimbursement. No invoice for reimbursement of Reimbursable Expenses will be paid by County if invoiced to County more than thirty (30) days after such Reimbursable Expenses are paid by Contractor.

4.1.2. The invoices shall include a statement from Contractor indicating, on a bi-weekly basis, the actual number of eight-hour employee shifts, and part-time and overtime hours worked during the month, including any additional personnel requested by the Contract Administrator.

4.1.3. Contractor shall submit with each invoice a Certification of Payments to Subcontractors and Suppliers (Exhibit G). The certification shall be accompanied by a copy of the notification sent to each Subcontractor and supplier listed on the form, explaining the good cause why payment has not been made.

4.1.4. County shall pay Contractor within thirty (30) calendar days after receipt of Contractor's proper invoice, as required under the "Broward County Prompt Payment Ordinance," Section 1-51.6, Broward County Code of Ordinances. To be deemed proper, all invoices must comply with the requirements set forth in this Agreement and must be submitted on the form and pursuant to instructions prescribed by the Contract Administrator. Payment may be withheld for failure of Contractor to comply with a term, condition, or requirement of this Agreement. Payment shall be made to Contractor at the address designated in the Notices section

4.1.5. Contractor shall pay its Subcontractors and suppliers within fifteen (15) days following receipt of payment from County for such subcontracted work or supplies. Contractor agrees that if it withholds an amount as retainage from Subcontractors or suppliers, it will release such retainage and pay same within fifteen (15) days following receipt of payment of retained amounts from County. Failure to pay a Subcontractor or supplier in accordance with this subsection shall be a material breach of this Agreement unless Contractor demonstrates that such failure to pay results from a bona fide dispute with the Subcontractor or supplier.

4.2. Notwithstanding any provision of this Agreement to the contrary, County may withhold, in whole or in part, payment to the extent necessary to protect itself from loss on account of inadequate or defective work which has not been remedied or resolved in a manner satisfactory to the Contract Administrator or failure to comply with any provision of this Agreement. The amount withheld shall not be subject to payment of interest by County.

5. Miscellaneous:

5.1. Annual Audit Report. Contractor shall provide to the Finance Division of the Port Everglades Department an annual audit report of all gross revenues and operating expenses from its operations at the Port and from the operations of related or affiliated companies involved in providing Services covered by this Agreement. The annual audit report shall show all net revenue of the self-parking services, valet parking services, and all Reimbursable Expenses. The annual audit report shall be prepared by an independent certified public accountant in accordance with Government Auditing Standards. The annual audit report shall be submitted to the Port Everglades Department within ninety (90) days after the end of each Fiscal Year of the County and shall include, but not be limited to, the following:

5.1.1. Schedule of all gross revenues by category, by month, and by the separate services of: self-parking services and valet parking services.

5.1.2. Schedule of all operating expenses, including Reimbursable Expenses, by category, by month, and by the separate services of: self-parking and valet parking. All Reimbursable Expenses for self-parking services and valet parking services shall be designated as such, and all non-Reimbursable Expenses shall be so designated.

5.1.3. Differences, if any, by category between audited revenue and expenses and the sum of the invoices that are provided pursuant to this Agreement.

5.1.4. Failure of the Contractor to file the annual audit report within ninety (90) calendar days after the end of each Fiscal Year shall result in a reduction to the reimbursement for the annual audit report as follows:

5.1.4.1. Up to thirty days late — a reduction of One Thousand Dollar ($1,000);

5.1.4.2. Thirty-one to sixty days late — a reduction of Two Thousand Five Hundred Dollars ($2,500);

5.1.4.3. Sixty-one to ninety days late — a reduction of Four Thousand Five Hundred Dollars ($4,500); and

5.1.4.4. Ninety-one days or later — there will be no reimbursement payable for the annual audit report.

5.2. Contractor shall fund a Change Fund in an amount agreed to by the Contract Administrator and Contractor to be sufficient to meet daily change fund requirements ("Change Fund") associated with the cash accepting pay-on-foot stations.

5.3. Contractor shall assume all financial responsibility for dishonored credit cards, and loss of funds or non-collected funds, except that Contractor shall not be responsible for non-collected funds if, at the sole discretion of the Contract Administrator, Contractor shows it attempted to collect such funds in a manner satisfactory to the Contract Administrator.

<u>Attachments:</u>

1. Annual Operating Expense Budget
2. Shuttle Rate Schedule
3. Bi-Weekly Expense Invoice

Exhibit 2

Attachment 1 to Exhibit B
Annual Operating Expense Budget

MANAGEMENT FEE: $14.70 per space	**Annual Total Year 1**
Northport Garage / T2/T4 Garage (1,818 spaces)	**$26,725**
Midport Garage (1,966 spaces)	**$28,900**
Terminal 18 Surface Lot (600 spaces)	**$8,820**
Terminal 19 Surface Lot (404 spaces)	**$5,939**
Total Annual Management Fees:	**$ 70,384**
PAYROLL EXPENSES:	
Salaries & Wages Fringe Benefits: Wages for employees, including management	**$310,418**
Payroll Taxes: Wage Taxes	**$26,439**
Workers Compensation: Workers Compensation Insurance	**$8,226**
Employee Medical Insurance: Medical insurance participation for employees	**$4,573**
Total Annual Payroll Expenses:	**$ 349,656.00**
OTHER EXPENSES:	
Audit Fees: On-site external audit, as well as an audit of corporate and office records.	**$10,000.00**
Personnel Record Checks: Pre-employment criminal background check	**$2,000.00**
Contract Cleaning: Daily garage cleaning	**$199,046.00**
Contract Staffing: Auditors and staffing for non-revenue tasks	**$120,895.00**
Patron Car Damage: Deductible and voluntary settlement of patrons' claim for vehicle damage or loss of contents	**$5,000**
Signage: Special events signage, sandwich board signage, directional services, etc.	**$5,000**
Towing: Tow a vehicle or tow to relocate vehicle	**$1,000**
Hurricane Contingency: Funds available for emergency situations	**$15,000**
Postage: Postage stamp and packages	**$250**
Equipment Rental-Golf Carts: 6 - Golf cart rentals and maintenance	**$25,000**
General Liability Insurance: Insurance (per agreement insurance requirements)	**$50,000**
Printing/Ticket Stock: Yearly expense to purchase spitter tickets	**$10,000**
Licenses & Fees: Business and Occupational Licenses	**$250**
Office Supplies: Including but not limited to water, paper, ink cartridges, etc.	**$10,000**
Cost of Fuel/Service: Fuel for Broward County vehicle	**$1,500**
Optional Services: Garage pressure cleaning, striping, equipment, supplies and uneforeseen conditions.	**$45,000**
Wearing Apparel: Uniforms for all employees and accessories	**$5,000**
Total Annual Other Expenses:	**$504,941.00**

TOTAL OVERALL PARKING ANNUAL OPERATING EXPENSE BUDGET:	**$ 924,981**

Shuttle Bus Services: 14-17 passengers, 23 - 30 passengers, or 40 - 55 passengers	**$ 484,945**

Total Annual Operating Expense Budget:	**$ 1,409,926**

Attachment 2 to Exhibit B
Shuttle Rate Schedule

FORT LAUDERDALE TRANSPORTATION, INC. RATES AT PORT EVERGLADES
HOURLY RATES EFFECTIVE November 1, 2020

Cruise Passenger Shuttle

Capacity	Description	Rate Per Hour	Minimum Hours
14 - 17 Passengers	Shuttle bus with interior luggage, wheel chair accessible available	$114 per hour	4 hours minimum
23 - 30 Passengers	Mini-Bus with rear luggage	$129 per hour	4 hours minimum
49 - 55 Passengers	Motor Coach		N/A

Employee Shuttle

Capacity	Description	Rate Per Hour	Minimum Hours
14 - 70 Passengers	Shuttle bus with interior luggage, wheel chair accessible available	$119 per hour	4 hours minimum
23 - 30 Passengers	Mini-Bus with rear luggage	$134 per hour	4 hours minimum

All vehicles must be reserved in advance and are subject to availability.

Cancellation Policy

All reservations cancelled at least 36 hours in advance of the scheduled reservation time will not be subject to a charge for the cancellation. All reservations cancelled less than 36 hours may be charged 25% of the rate assigned to the vehicle for the hours the vehicle was reserved.

FORT LAUDERDALE TRANSPORTATION, INC. RATES AT PORT EVERGLADES
HOURLY RATES EFFECTIVE November 1, 2021

Cruise Passenger Shuttle

Capacity	Description	Rate Per Hour	Minimum Hours
14 - 17 Passengers	Shuttle bus with interior luggage, wheel chair accessible available	$125 per hour	4 hours minimum
23 - 30 Passengers	Mini-Bus with rear luggage	$142 per hour	4 hours minimum
49 - 55 Passengers	Motor Coach		N/A

Employee Shuttle

Capacity	Description	Rate Per Hour	Minimum Hours
14 - 17 Passengers	Shuttle bus with interior luggage, wheel chair accessible available	$131 per hour	4 hours minimum
23 - 30 Passengers	Mini-Bus with rear luggage	$147 per hour	4 hours minimum

All vehicles must be reserved in advance and are subject to availability.

Cancellation Policy

All reservations cancelled at least 36 hours in advance of the scheduled reservation time will not be subject to a charge for the cancellation. All reservations cancelled less than 36 hours may be charged 25% of the rate assigned to the vehicle for the hours the vehicle was reserved.

FORT LAUDERDALE TRANSPORTATION, INC. RATES AT PORT EVERGLADES
HOURLY RATES EFFECTIVE November 1, 2022

Cruise Passenger Shuttle

Capacity	Description	Rate Per Hour	Minimum Hours
14 - 17 Passengers	Shuttle bus with interior luggage, wheel chair accessible available	TBD	4 hours minimum
23 - 30 Passengers	Mini-Bus with rear luggage	TBD	4 hours minimum
49 - 55 Passengers	Motor Coach		N/A

Employee Shuttle

Capacity	Description	Rate Per Hour	Minimum Hours
14 - 17 Passengers	Shuttle bus with interior luggage, wheel chair accessible available	TBD	4 hours minimum
23 - 30 Passengers	Mini-Bus with rear luggage	TBD	4 hours minimum

All vehicles must be reserved in advance and are subject to availability.

Cancellation Policy

All reservations cancelled at least 36 hours in advance of the scheduled reservation time will not be subject to a charge for the cancellation. All reservations cancelled less than 36 hours may be charged 25% of the rate assigned to the vehicle for the hours the vehicle was reserved.

Attachment 3 to Exhibit B
Bi-Weekly Expense Invoice

Parking Facility:		
Pay Period Ending:		
Invoice Number:		
Invoice Date:		**PO#**
Management Fee - T2/T4	512700	$ -
Management Fee - MP	512700	$ -
Management Fee - T18	512700	$ -
Management Fee - T19	512700	$ -
Subtotal Management Fees	512700	**$ -**
Payroll Expenses		
Salaries & Wages	512700	$ -
Payroll Taxes	512700	$ -
Medical Insurance	512700	$ -
Worker's Comp.	512700	$ -
Total Payroll Expenses		**$ -**
Other Expenses		
Personnel Record Checks	512700	$ -
Optional Service: Contract Labor	512700	$ -
Contract Cleaning	512700	$ -
Contract Staffing	512700	$ -
Patron Car Damage	512700	$ -
Signage	512700	$ -
Credit Card Service Fees	512700	$ -
Towing	512700	$ -
Hurricane contingency	512700	$ -
Subtotal 512700 Expenses		**$ -**
Audit Fees	512510	$ -
Shuttle Bus	512720	$ -
Postage	522010	$ -
Equipment Rental-Golf Carts-Trucks	526020	$ -
General Liability Ins.	530702	$ -
Auto Insurance	530513	$ -
Optional Service: Equipment/supplies	540030	$ -
Printing/Ticket Stock	545010	$ -
Web/On-line Transaction Services	546010	$ -
Licenses & Fees	547280	$ -
Office Supplies	552310	$ -
Cost of Fuel/Service	555330	$ -
Wearing Apparel	555410	$ -
Total Other Expenses		**$ -**
Total Overall Operating Expenses		

I certify that the above expenses have been paid or incurred on behalf of the Port Everglades Parking Facilities, owned by Broward County and administered by Port Everglades Department. Further I certify there are no provisions for refunds, rebates, credits or any other return of funds reimbursed to SP Plus Corporation for costs incurred related to operation of Port Everglades' Parking Facilities.

Signature___________________________ Date:______________________

Exhibit C

INSURANCE REQUIREMENTS

Project: PNC2116816P1 Parking Management Services for Various County Agencies (FMD and PORT)

TYPE OF INSURANCE	ADDL INSD	SUBR WVD	MINIMUM LIABILITY LIMITS		
				Each Occurrence	**Aggregate**
GENERAL LIABILITY - Broad form ☑ Commercial General Liability ☑ Premises–Operations □ XCU Explosion/Collapse/Underground ☑ Products/Completed Operations Hazard ☑ Contractual Insurance ☑ Broad Form Property Damage ☑ Independent Contractors ☑ Personal Injury **Per Occurrence or Claims-Made:** ☑ Per Occurrence □ Claims-Made **Gen'l Aggregate Limit Applies per:** □ Project □ Policy □ Loc. □ Other _______	☑	☑	Bodily Injury		
			Property Damage		
			Combined Bodily Injury and Property Damage	**$1,000,000**	**$2,000,000**
			Personal Injury		
			Products & Completed Operations		
AUTO LIABILITY ☑ Comprehensive Form ☑ Owned ☑ Hired ☑ Non-owned ☑ Any Auto, If applicable *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	**$1,000,000**	
□ **EXCESS LIABILITY / UMBRELLA** **Per Occurrence or Claims-Made:** □ Per Occurrence □ Claims-Made *Note: May be used to supplement minimum liability coverage requirements.*	☑	☑			
☑ **WORKER'S COMPENSATION** *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	**$500,000**	
☑ **CRIME & FIDELITY / EMPLOYEE DISHONESTY**	☑	☑	Each Claim	**$100,000**	
☑ **GARAGE LIABILITY / GARAGE KEEPERS LIABILITY**			Each Occurrence	**$1,000,000**	
□ Installation floater is required if Builder's Risk or Property are not carried. *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	

Description of Operations: "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

CPounall Digitally signed by cpounall@broward.org
DN: cn=cpounall@broward.org
Date: 2018.08.08 16:44:30 -04'00'

Risk Management Division

Exhibit E

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.: PNC2116816P1

Project Title: Parking Management Services for Various County Agencies

Bidder/Offeror Name: SP Plus Corporation
Address: 444 Brickell Ave, Suite 200 **City:** Miami **State:** FL **Zip:** 33131
Authorized Representative: Chester Escobar **Phone:** (305) 218 9032

CBE Firm/Supplier Name: S. Davis & Associates, P.A.
Address: 2521 Hollywood Boulevard **City:** Hollywood **State:** FL **Zip:** 33020
Authorized Representative: Shaun Davis **Phone:** (954) 927-5900

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.

Work to be performed by CBE Firm

Description	NAICS[1]	CBE Contract Amount[2]	CBE Percentage of Total Project Value	
Accounting Services-Staffing-Port		$225,225	13 %	- Group 1
Auditing Services-Broward		$ 7,500	1 %	- Group 1
			%	

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

CBE Firm/Supplier Authorized Representative

Signature: ______ **Title:** Managing Partner **Date:** 07/26/2019

Bidder/Offeror Authorized Representative

Signature: Chet. Escobar **Title:** Vice President **Date:** 8/7/19

[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.

Exhibit E

LETTER OF INTENT

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

BROWARD COUNTY FLORIDA
OFFICE OF ECONOMIC AND SMALL BUSINESS DEVELOPMENT

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.: PNC 2116816P1

Project Title: Parking Management Services for Various County Agencies

Bidder/Offeror Name: SP Plus Corp.

Address: 444 Brickell Ave #200 City: Miami State: Fl Zip: 33131

Authorized Representative: Chester Escobar Phone: (305)218-9032

CBE Firm/Supplier Name: Ann's Janitorial Services Inc

Address: 11846 SW 8th St **City:** Pembroke Pines **State:** FL **Zip:** 33025

Authorized Representative: Norma Ann Kendall **Phone:** 954-593-0707

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.

Work to be performed by CBE Firm

Description	NAICS[1]	CBE Contract Amount[2]	CBE Percentage of Total Project Value	
Janitorial Services - Port Everglades		$216,100	12 %	- Group 2
" Broward		$215,964	25 %	- Group 1
			%	

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

CBE Firm/Supplier Authorized Representative

Signature: Norma Ann Kendall Title: President Date: July 24, 2019

Bidder/Offeror Authorized Representative

Signature: Title: Vice President Date: 8-7-19

[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 F

Port Everglades 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 online to https://www.tsa.gov/for-industry/twic.

Exhibit G
Certification of Payments to Subcontractors and Suppliers

RLI/Bid/Contract No. _______________
Project Title _______________________

The undersigned Contractor hereby swears under penalty of perjury that:

1. Contractor has paid all Subcontractors and suppliers all undisputed contract obligations for labor, services, or materials provided on this project in accordance with the "Compensation" article of this Agreement, except as provided in paragraph 2 below.

2. The following Subcontractors and suppliers have not been paid because of disputed contractual obligations; a copy of the notification sent to each, explaining in reasonably specific detail the good cause why payment has not been made, is attached to this form:

Subcontractor or supplier's name and address	Date of disputed invoice	Amount in dispute

3. The undersigned is authorized to execute this Certification on behalf of Contractor.

Dated _____________, 20___

____
Contractor
By________________________________
(Signature)
By_________________________________
(Name and Title)

STATE OF)
)
COUNTY OF)

Sworn to (or affirmed) and subscribed before this _____ day of _______________, ____, by _______________________________ who is personally known to me or who has produced ______________________ as identification.

____
Signature of Notary Public

(NOTARY SEAL)

____
Print, Type or Stamp Name of Notary

Exhibit H

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/Vendor**	**County**	**Joint**	**Notes**
1.1	Establish and implement firewall and router configuration standards that include the following:	x				
1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations	x				
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				
1.1.3	Current diagram that shows all cardholder data flows across systems and networks	x				
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				
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				

Exhibit H

1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. 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				
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				
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				
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				

Exhibit H

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				
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				
1.3.7	Do not disclose private IP addresses and routing information to unauthorized parties. Note: Methods to obscure IP addressing may include, but are not limited to: • Network Address Translation (NAT) • Placing servers containing cardholder data behind proxy servers/firewalls, • Removal or filtering of route advertisements for private networks that employ registered addressing • Internal use of RFC1918	x				

Exhibit H

	address space instead of registered addresses.					
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: • Specific configuration settings are defined for personal firewall software. • Personal firewall software (or equivalent functionality) is actively running. • 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. 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 (POS) terminals, Simple Network Management	x				

Exhibit H

	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. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • 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.) Note: Where virtualization	x				

Exhibit H

	technologies are in use, implement only one primary function per virtual system component.					
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				
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				
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				

Exhibit H

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: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements • Processes for secure deletion of data when no longer needed • Specific retention requirements for cardholder data • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.	x				
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. *It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:* • *There is a business justification and* • *The data is stored secur*ely. Sensitive authentication data includes the data as	x				

Exhibit H

	cited in the following Requirements 3.2.1 through 3.2.3:					
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. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. *Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* *• The cardholder's name* *• Primary account number (PAN)* *• Expiration date* *• Service code* *To minimize risk, store only these data elements as needed for business.*	x				
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				
3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.	x				
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.	x				

Exhibit H

	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.					
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: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures. 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 cannot be correlated to reconstruct the original PAN.	x				
3.4.1	If disk encryption is used (rather than file or column-level database encryption),	x				

Exhibit H

	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. *Note: This requirement applies in addition to all other PCI DSS encryption and key-management requirements.*					
3.5	Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse: *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				
3.5.1	Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes: • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date • Description of the key usage for each key. • Inventory of any HSMs and	x				

Exhibit H

	other SCDs used for key management					
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: • 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 • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As at least two full-length key components or key shares, in accordance with an industry-accepted method *Note: It is not required that public keys be stored in one of these forms.*	x				
3.5.4	Store cryptographic keys in the fewest possible locations.	x				
3.6	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: *Note: Numerous industry standards for key management are available from various resources*	x				

Exhibit H

	including NIST, which can be found at http://csrc.nist.gov.					
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. *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				

Exhibit H

3.6.6	If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. *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				
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				
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: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. *Examples of open, public*	x				

Exhibit H

	networks include but are not limited to: *• The Internet* *• Wireless technologies, including 802.11 and Bluetooth* *• Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)* *• General Packet Radio Service (GPRS).* *• Satellite communications.*					
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 documented, in use, and known to all affected parties.	x				
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	x				
5.1.1	Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	x				

Exhibit H

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				
5.2	Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current, • Perform periodic scans • Generate audit logs which are retained per PCI DSS Requirement 10.7.	x				
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. *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				
5.4	Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and	x				

Exhibit H

	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. *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*	x				

Exhibit H

	systems that store, process, or transmit cardholder data.					
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. *Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.*	x				
6.3	Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle Note: this applies to all software developed internally as well as bespoke or custom software developed by a third party.	x				
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				
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	x				

Exhibit H

	processes) to include at least the following: • Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code- review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines • Appropriate corrections are implemented prior to release. Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. 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 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				

Exhibit H

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 as applicable.	x				
6.5	Address common coding vulnerabilities in software-development processes as follows: • Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. • Develop applications based on secure coding guidelines. Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this	x				

Exhibit H

	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.					
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				
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:	x				

Exhibit H

	• Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2. • 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.					
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	
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.		x			
7.1.1	Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources.		x			
7.1.2	Restrict access to privileged user IDs to least privileges		x			

Exhibit H

	necessary to perform job responsibilities.					
7.1.3	Assign access based on individual personnel’s job classification and function.		x			
7.1.4	Require documented approval by authorized parties specifying required privileges.	x				
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. This access control system must include the following:	x				
7.2.1	Coverage of all system components	x				
7.2.2	Assignment of privileges to individuals based on job classification and function.	x				
7.2.3	Default “deny-all” setting.	x				
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			
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				
8.1.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	x				
8.1.2	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.		x			

Exhibit H

8.1.3	Immediately revoke access for any terminated users.		x			
8.1.4	Remove/disable inactive user accounts within 90 days.		x			
8.1.5	Manage IDs used by Provider/Vendors to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use.	x				
8.1.6	Limit repeated access attempts by locking out the user ID after not more than six attempts.	x				
8.1.7	Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	x				
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				
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: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric.	x				
8.2.1	Using strong cryptography, render all authentication credentials (such as	x				

Exhibit H

	passwords/phrases) unreadable during transmission and storage on all system components.					
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: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. 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				
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				
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. *Note: Multi-factor authentication requires that a minimum of two of the three authentication*	x				

Exhibit H

	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					
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				
8.4	Document and communicate authentication procedures and policies to all users including: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions to change passwords if there is any suspicion the password could be compromised.		x			
8.5	Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for system administration and other	x				

Exhibit H

	critical functions. • Shared and generic user IDs are not used to administer any system components.					
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. *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: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	x				
8.7	All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through	x				

Exhibit H

	programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non- application processes).					
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 to restrict access to publicly accessible network jacks. For example, network jacks	x				

Exhibit H

	located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, 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: • Identifying onsite personnel and visitors (for example, assigning badges) • Changes to access requirements • 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: • Access must be authorized and based on individual job function. • Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.		x			

Exhibit H

9.4	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				
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. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. 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	x				

Exhibit H

	media, including the following:					
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	County shares responsibility only to the extent County obtains access to cardholder data
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. Note: These requirements apply to card- reading devices used in card-present transactions (that is, card swipe or dip) at the point of	x				

Exhibit H

	sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.					
9.9.1	Maintain an up-to-date list of devices. The list should include the following: • Make, model of • Location of device (for example, the address of the site or facility where the device is located) • 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). 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	It is expected that the software/equipment provider will also be responsible for periodically inspecting devices when on site.
9.9.3	Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: • Verify the identity of any third-party persons claiming to be repair or maintenance				x	

Exhibit H

	personnel, prior to granting them access to modify or troubleshoot devices. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).					
9.9.4	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				x	Port's software/equipment vendor for its PARCS will also be responsible for administering roles.

Exhibit H

	changes, additions, or deletions to accounts with root or administrative privileges					
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				
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	x				

Exhibit H

	server or media that is difficult to alter.					
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 (although new data being added should not cause an alert).	x				
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.	x				
10.6.1	Review the following at least daily: • All security events • 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 • Logs of all critical system components • 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	x				

Exhibit H

	organization's policies and risk management strategy, as determined by the organization's annual risk assessment.					
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				
10.8	Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used)	x				
10.8.1	Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and	x				

Exhibit H

	documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls					
10.9	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.				x	
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				

Exhibit H

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). 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. 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, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-	x				

Exhibit H

	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. 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). Refer to the ASV Program Guide published on the PCI SSC website for scan County responsibilities, scan preparation, etc.	x				
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:	x				

Exhibit H

	• Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) • Includes coverage for the entire CDE perimeter and critical systems • Includes testing from both inside and outside the network • Includes testing to validate any segmentation and scope-reduction controls • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 • Defines network-layer penetration tests to include components that support network functions as well as operating systems • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months • 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.					
11.3.1	Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or	x				

Exhibit H

	modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).					
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	x				

Exhibit H

	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. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.					
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 software to perform critical file comparisons at least weekly.	x				
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: -Is performed at least	x				

Exhibit H

	annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), -Identifies critical assets, threats, and vulnerabilities, and -Results in a formal, documented analysis of risk.					
12.3	Develop usage policies for critical technologies and define proper use of these technologies. 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. 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				
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				

Exhibit H

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. 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: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance • Defining a charter for a PCI DSS compliance program and communication to executive management	x				
12.5	Assign to an individual or team the following information security	x				

Exhibit H

	management responsibilities:					
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. 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.)		x			

Exhibit H

	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.					
12.8	Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:		x			
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. *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		x			

Exhibit H

	including proper due diligence prior to engagement.					
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	
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. *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			
12.10	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				x	

Exhibit H

	the following, at a minimum: • Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data backup processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands.					
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	
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: Perform reviews at least quarterly to confirm	x				

Exhibit H

	personnel are following security policies and operational procedures. Reviews must cover the following processes: • Daily log reviews • Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts • Change management processes					
12.11.1	Additional requirement for service providers only: Maintain documentation of quarterly review process to include: • Documenting results of the reviews • 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: 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 entity must comply with the PCI DSS and validate compliance as applicable.	x				

Exhibit H

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

For the purposes of this Exhibit I, the following definitions shall apply:

"County Confidential Information" means any County Data that includes employee information, financial information, or 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 or applicable regulatory body).

"County Data" means the data and information (including text, pictures, sound, graphics, video and other data) relating to County or its employees or agents, or made available or provided by County or its agents to Contractor, for or in the performance of this Agreement, including all derivative data and results derived therefrom, whether or not derived through the use of the Contractor's services, whether or not electronically retained, and regardless of the retention media.

All other capitalized terms not expressly defined within this exhibit shall retain the meaning ascribed to such terms in the Agreement (and if not so defined, then the plain language meaning appropriate to the context in which it is used).

Security and Access. If Contractor will have access to any aspect of County's network via an Active Directory account, onsite access, remote access, or otherwise, Contractor must:

(a) comply at all times with all applicable County access and security standards, policies, and procedures related to County's network, as well as any other or additional restrictions or standards for which County provides written notice to Contractor;
(b) provide any and all information that County may reasonably request in order to determine appropriate security and network access restrictions and verify Contractor's compliance with County security standards;
(c) provide privacy and information security training to its employees with access to County's network upon hire and at least once annually; and
(d) notify County of any terminations or separations of Contractor's employees who had access to County's network.

In addition, if and to the extent Contractor will have any remote access to County's network, Contractor must:

(e) utilize secure, strictly-controlled industry standards for encryption (e.g., Virtual Private Networks) and passphrases and safeguard County Data that resides in or transits through Contractor's internal network from unauthorized access and disclosure;
(f) ensure the remote host device used for access is not connected to any other network, including an unencrypted third party public WiFi network, while connected to County's network, with the exception of networks that are under Contractor's complete control or under the complete control of a person or entity authorized in advance by County in writing;
(g) enforce automatic disconnect of sessions for remote access technologies after a specific period of inactivity with regard to connectivity into County infrastructure;
(h) utilize equipment that contains antivirus protection software, an updated operating system, firmware, and third party-application patches, and that is configured for least privileged access;
(i) 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 Contractor's internal network from unauthorized access and disclosure; and

(j) activate remote access from Contractor and its approved subcontractors into the County network only to the extent necessary to perform services under this Agreement, deactivating such access immediately after use.

If at any point in time County, in the sole discretion of its Chief Information Officer (CIO), determines that Contractor's access to any aspect of County's network presents an unacceptable security risk, or if Contractor exceeds the scope of access required to perform the required services under the Agreement, County may immediately suspend or terminate Contractor's access and, if the risk is not promptly resolved to the reasonable satisfaction of the County's CIO, may terminate this Agreement or any applicable Work Authorization upon ten (10) business days' notice (including, without limitation, without restoring any access to County network to Contractor).

Data and Privacy. To the extent applicable to the services being provided by Contractor under the Agreement, Contractor shall comply with all applicable data and privacy laws and regulations, including without limitation Florida Statutes Section 501.171, and shall ensure that County Confidential Data processed, transmitted, or stored by Contractor or in Contractor's system is not accessed, transmitted or stored outside the United States. Contractor shall not sell, market, publicize, distribute, or otherwise make available to any third party any personal identification information (as defined by Florida Statutes Section 501.171, Section 817.568, or Section 817.5685, as amended) that Contractor may receive or otherwise have access to in connection with this Agreement, unless expressly authorized in advance by County. If applicable and requested by County, Contractor 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 DOD 5220.22-M, and that an appropriate data wipe certification is provided to the satisfaction of the Contract Administrator.

Managed or Professional Services. Contractor shall immediately notify County of any terminations or separations of Contractor's employees who performed services under the Agreement and who had access to County Confidential Information or the County network. If any unauthorized party is successful in accessing any area, including any information technology component related to Contractor, where County Data or files exist or are housed, Contractor shall notify County within twenty-four (24) hours after becoming aware of such breach, unless an extension is granted by County's CIO. Contractor shall provide County with a detailed incident report within five (5) days after becoming aware of the breach, including remedial measures instituted and any law enforcement involvement. Contractor shall fully cooperate with County on incident response, forensics, and investigations into Contractor's infrastructure as it relates to any County Data or County applications. Contractor shall not release County Data or copies of County Data without the advance written consent of County. Contractor shall ensure adequate background checks have been performed on any personnel having access to County Confidential Information. To the extent permitted by such checks, Contractor shall not knowingly allow convicted felons or other persons deemed by Contractor to be a security risk to access County Data. Contractor shall ensure the use of any open source or third-party software or hardware does not undermine the security posture of the Contractor or County.

System and Organization Controls (SOC) Report. Contractor shall provide County a redacted SOC 1 Type II Report provided that such redactions shall not misrepresent or cause any remaining portion of the report to be false or misleading.

Payment Card Industry (PCI) Compliance. If and to the extent at any point during the Agreement that Contractor accepts, transmits, or stores any credit cardholder data or is reasonably determined by County to potentially impact the security of County's cardholder data environment ("CDE"), Contractor must:

(a) comply with the most recent version of VISA Cardholder Information Security Program ("CISP") Payment Application Best Practices and Audit Procedures including Security Standards Council's PCI DSS and the functions relating to storing, processing, and transmitting of the cardholder data to the extent applicable to Contractor and set forth in the PCI DSS responsibility matrix (see Exhibit H);

(b) Maintain PCI DSS validation throughout the Agreement;

(c) prior to commencement of the Agreement, and annually, provide to County: a Self Assessment Questionnaire ("SAQ") for SP Plus Corporation and a written acknowledgement of responsibility for the security of cardholder data Contractor possesses or otherwise stores, processes, or transmits, and for any service Contractor provides that could impact the security of County's CDE (if Contractor subcontracts or in any way outsources the credit card processing, or provides an API that redirects or transmits cardholder to a payment gateway, Contractor is responsible for maintaining PCI compliance for the API and providing the AOC for the subcontractor or payment gateway to County);

(d) maintain and provide to County a PCI DSS responsibility matrix (see Exhibit H) that outlines the exact PCI DSS controls that are not applicable to the Agreement, are the responsibility of either Party, or that are the shared responsibility of Contractor and County (or another entity);

(e) immediately notify County, and to the extent applicable the vendor providing the equipment and software that accepts or processes payments, if Contractor learns or suspects that Contractor, the equipment or software that accepts or process payments or any component thereof is no longer PCI DSS compliant and to the extent applicable, provide County the steps being taken to remediate the noncompliant status no later than seven (7) calendar days after Contractor learns or suspects an issue related to PCI DSS compliance; and

(f) activate remote access from Contractor and its approved subcontractors into County's network only to the extent necessary to perform services under this Agreement, deactivating such access immediately after use.