TECHNOLOGY PRODUCTS AGREEMENT BETWEEN BROWARD COUNTY AND DESIGNA ACCESS CORPORATION FOR PARKING ACCESS AND REVENUE CONTROL EQUIPMENT AND MAINTENANCE FOR FORT LAUDERDALE-HOLLYWOOD INTERNATIONAL AIRPORT (RLI # PNC2119994R1)

This Technology Products Agreement between Broward County and Designa Access Corporation, for Parking Access and Revenue Control Equipment and Maintenance for Fort Lauderdale-Hollywood International Airport ("Agreement") is made and entered by and between Broward County, a political subdivision of the State of Florida ("County"), and Designa Access Corporation, a Georgia corporation authorized to transact business in the State of Florida ("Provider") (each a "Party" and collectively referred to as the "Parties").

RECITALS

A. County conducted a solicitation for Parking Access and Revenue Control Equipment and Maintenance ("PARCS") for the Airport (hereinafter defined), Request for Letters of Interest ("RLI") No. PNC2119994R1. Provider submitted a proposal to the RLI and received the highest ranking during the RLI process.

B. Provider will provide County with all necessary equipment, software, and services, including ongoing support and maintenance, for a comprehensive PARCS to be implemented at the Airport.

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. **Active and Passive Network Equipment** means all active and passive network equipment, including, but not limited to, fiber enclosures, media convertors, patch panels, small form factor pluggable ("SFP") units, patch cables, all racks/storage cabinets, and any other required equipment to enable the PARCS (hereinafter defined) devices to operate correctly.

1.2. **Agreement Year** means the twelve (12) month period beginning on the Effective Date and ending twelve (12) months thereafter ("Agreement Year 1"), and each twelve (12) month period thereafter until the date this Agreement expires or terminates.

1.3. **Airport** means Fort Lauderdale-Hollywood International Airport ("FLL"), located in Broward County, Florida, as described in the Master Plan Update, including such additional property that may be acquired by County to implement development as described therein.

1.4. **Airport Employees** means the employees of concessionaires, airlines, service providers at the Airport, Aviation Department employees, and all other persons considered by County as Airport employees.

1.5. **Applicable Law** means all applicable laws, codes, advisory circulars, rules, regulations, or ordinances of any federal, state, county, municipal, or other governmental entity, as may be amended.

1.6. **Aviation Department** means the Broward County Aviation Department, or any successor agency.

1.7. **Barrier Gate** means an automated gated utilized by PARCS to control ingress and egress of the Parking Facilities.

1.8. **Barrier Gate Arm** means a rectangular aluminum section of varying length which will span the width of the entry or exit lane and will be connected to the Barrier Gate mechanism using bolts which provide for breakaway functionality in the event of a vehicle impact.

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

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

1.11. **Code** means the Broward County Code of Ordinances.

1.12. **Contract Administrator** means the Director of Aviation or such other person designated by the Director of Aviation in writing.

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

1.14. **Credit Card** means any card or other credit device existing for the purpose of obtaining money, property, labor, or services on credit.

1.15. **Director of Aviation** means the Director or Acting Director of the Aviation Department, or such other person or persons as may from time to time be authorized in writing by the Board, County Administrator, or the Director of Aviation to act for the Director of Aviation with respect to any or all matters pertaining to this Agreement.

1.16. **Documentation** means all manuals, user documentation, specifications, and other related materials pertaining to the Software that Provider customarily furnishes to licensees of the Software or purchasers of the services covered by this Agreement.

1.17. **Equipment** means the hardware and other property listed in **Exhibit A** being provided to County pursuant to this Agreement, including any embedded software and firmware incorporated therein or customarily provided to purchasers of such hardware or other property.

1.18. **Federal Aviation Administration** or **FAA** means the agency of the United States Government established under 49 U.S.C. § 106, or its successor.

1.19. **Hosted Service** or **Subscription** means any cloud or subscription-based service or solution provided to County by Provider (including Software as a Service ("SaaS") or Platform as a Service ("PaaS")), as further described in **Exhibit A**.

1.20. **In Revenue Service** means an entry lane or exit lane, that is properly completed and is placed into service for the purposes of collecting parking revenue.

1.21. **Intercom System** means a digital voice over internet protocol ("VoIP") two-way communication system between in-field devices and the Parking Operations Office.

1.22. **License Fee** or **Subscription Fee** means the fee associated with granting County use of the Software or Hosted Service as outlined in **Exhibit B**, Payment Schedule.

1.23. **License Plate Recognition** or **LPR** means hardware and software associated with either fixed or mobile license plate recognition for tracking vehicles in the Parking Facilities.

1.24. **Loop Detector** means an inductive electronic unit connected to an in-ground loop of wire or to another external sensing device used to detect vehicles. When the metal in a vehicle is detected by the Loop Detector, a signal is recorded by the Barrier Gate.

1.25. **Notice to Proceed** or **NTP** means a written authorization to proceed with a project, phase, or task, issued by the Contract Administrator.

1.26. **Point to Point Encryption** or **P2PE** means a standard established by the Payment Card Industry Security Standards Council to provide a payment security solution that instantaneously converts confidential payment card (credit and debit card) data and information into indecipherable code at the time the card is used, in order to prevent hacking and fraud.

1.27. **Parking Facilities** means all garages or parking lots at the Airport within which vehicles may be parked for the purpose of collecting parking revenue, including, but not limited to, the Palm Garage, Hibiscus Garage, Cypress Garage, Employee Parking Lot 1, Employee Parking Lot 2, and two (2) full size valet parking locations located at Terminals 1 and 4 upper-level curbsides.

1.28. **Parking Media** means any media used for entry or exit to/from the Parking Facilities, including, but not limited to, a ticket, Credit Card, Proximity Card, QR Code, license plate, or a SunPass transponder.

1.29. **Parking Operations Office** means the management location of the PARCS which provides user workstations for control of the PARCS devices.

1.30. **Payment Card Industry** or **PCI** means all the organizations which store, process and transmit cardholder data, most notably for debit cards and Credit Cards.

1.31. **Production Environment** means the live operating environment for the System.

1.32. **Products** means all Software, Equipment, Hosted Service, and Services provided or required to be provided by Provider, as further specified in **Exhibit A**.

1.33. **Proximity Card** means a contactless read-only card that can be read at short-range but without insertion into a card reading device that allows a cardholder to gain entry to the Parking Facilities.

1.34. **Purchasing Director** means County's Director of Purchasing.

1.35. **QR Code** means a type of matrix barcode or two-dimensional barcode that contains information about the item to which it is attached.

1.36. **Services** means all required installation, integration, programming, configuration, customization, operation, and enhancements of the Products, together with necessary and appropriate consulting, training, and project management services, and maintenance, to meet County's ongoing needs in connection with the Products, as further specified in the Statement of Work attached as **Exhibit A**, as well as any Optional Services procured under this Agreement.

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

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

1.39. **SunPass** means the electronic prepaid toll program operated by Florida's Turnpike Enterprise under the Florida Department of Transportation.

1.40. **Support and Maintenance** means the support and maintenance required for County to achieve and maintain optimal performance of the Products and the System, including as further described in **Exhibit D**.

1.41. **System** means the PARCS turnkey system provided by Provider pursuant to this Agreement as part of its Services hereunder, including all Products listed on **Exhibit A** and any other Products that Provider will make available to County and third-party users as part of its Services under this Agreement.

1.42. **Test Environment** means the Equipment identified in **Exhibit A**, Attachment 2, Equipment Schedule, which provides a permanent Test Environment, separate to the Production Environment, for prior testing of all configuration processes, patches, or updates to the System before deployment to the Production Environment.

1.43. **WebPARCS** means County's current PARCS system.

ARTICLE 2. EXHIBITS

Exhibit A **Statement of Work**
Exhibit B **Payment Schedule**
Exhibit C **Security Requirements**
Exhibit D **Support and Maintenance Minimum Standards**
Exhibit E **Minimum Insurance Coverages**
Exhibit F **Work Authorization Form**
Exhibit G **Service Level Agreement**
Exhibit H **CBE Subcontractor Schedule and Letters of Intent**
Exhibit I **PCI Responsibility Matrix**
Exhibit J **Nondiscrimination and Other Federal Requirements**
Exhibit K **Aviation Department Security Requirements**

ARTICLE 3. SCOPE OF SERVICES & TERMS OF USE

3.1. Scope of Services. Provider shall perform all work identified in this Agreement including, without limitation, the work specified in **Exhibit A** (the "Statement of Work"). The Statement of Work is a description of Provider'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 Provider impractical, illogical, or unconscionable.

3.2. Software and Subscriptions Rights.

3.2.1. Software License. Provider grants to County a perpetual, royalty-free, nonexclusive license to the Software, with no geographical limitations, for the number of users stated in **Exhibit A** (if none is stated, then an unlimited number of users), including to any embedded third-party software within the Software. This license is granted solely for County purposes, including on and off-site access, and for the benefit of and use by all agencies within County, including the offices of the County constitutional officers if elected by County. The Software rights granted to County in this Agreement shall not require or otherwise be contingent upon the continuance of Support and Maintenance.

3.2.2. Subscription Rights. Provider grants to County a royalty-free, nonexclusive right to use the Hosted Service for the duration of this Agreement, with no geographical limitations, for the number of users stated in **Exhibit A** (if none is stated, then for an unlimited number of users), including the right to use any third-party software or technology embedded in or otherwise required to operate or allow access to the Hosted Service. This right to use is granted solely for County purposes, including on- and off-site access, and for the benefit of and use by all agencies within the County, including the offices of the County constitutional officers if elected by County.

3.2.3. Authorized Users and Additional Licenses. Unless otherwise stated in **Exhibit A** (Statement of Work), County and any of its employees, agents, contractors, suppliers, and

other third parties authorized by County may concurrently operate and use the Products for County purposes. If additional licenses or users are requested by County, the Purchasing Director is authorized to execute a Work Authorization (in substantially the form of **Exhibit F**) to purchase additional licenses or users for the fee specified in **Exhibit B**.

3.2.4. Permitted Hardware and Environments. Unless otherwise stated in **Exhibit A**, County may install, use, and operate the Software, and access the Hosted Service, on any hardware. County may, at no additional cost: (a) install, use, and operate the Products on separate servers and in any and all development, test, failover, disaster recovery, and backup environments or configurations; (b) if required by reason of an emergency, disaster, or operational need, or for testing of recovery resources, temporarily use the Products on recovery resources, including recovery resources that may not be owned by County; (c) copy the Software for backup and archiving purposes for the purposes of support or maintenance by County or others hired by County to provide such support or maintenance; and (d) utilize a hosted environment, including without limitation through a third-party hosting provider, for any permitted uses of the Software.

3.2.5. Prohibited Uses. Except as otherwise provided in this Agreement or required under Florida law, County shall not reproduce, publish, or license the Software or Hosted Service to others. County shall not modify, reverse engineer, disassemble, or decompile the Software or the Hosted Service, or any portion thereof, except (a) to the extent expressly authorized in **Exhibit A**, in which event such authorized actions shall be deemed within the license grant of Section 3.2, or (b) to the extent permitted under any applicable open source license.

3.3. Hosting. All costs to County for the Hosted Service are included within the Subscription Fee and/or the Support and Maintenance Fee listed on the Payment Schedule (**Exhibit B**) and will be provided at no additional cost to County, unless otherwise expressly stated in **Exhibit B**. Provider, the Hosted Service, and the System shall comply for the duration of this Agreement with the Service Level Agreement set forth in **Exhibit G**, unless otherwise expressly approved in writing by County's Chief Information Officer or their designee.

3.4. Support and Maintenance. For so long as requested by County and for all Products other than the Hosted Service, Provider shall provide County with Support and Maintenance for the Products and the System as set forth in **Exhibit D**. Provider shall provide County with Support and Maintenance for the Hosted Service so long as County pays the Subscription Fee for the Hosted Service stated in **Exhibit B**. Support and Maintenance shall be invoiced and paid in accordance with the Payment Schedule set forth in **Exhibit B**, except that for the first year following Final Acceptance, all Support and Maintenance for Software and Equipment is included at no cost to County. County may elect to discontinue or recommence Support and Maintenance for some or all Products upon thirty (30) days prior written notice, and County shall only be obligated to pay for the time periods actually covered by Support and Maintenance at the rates stated in **Exhibit B**.

3.5. Updates, Upgrades, and Releases. For the duration of this Agreement, Provider shall promptly provide to County, with advance notice and at no additional cost, any and all software

and firmware updates (including error corrections, bug fixes, security updates, and patches), upgrades, and new releases to the Products, including all that Provider makes available at no additional cost to other licensees of the applicable Products or users of all or part of the System. All such updates, upgrades, and new releases shall remain the sole property of Provider and shall be deemed to be included within the scope of the licenses or subscriptions for Products granted under this Agreement. Installation or implementation of any such update, upgrade, or release in the County's environment requires prior written authorization by the Contract Administrator.

3.6. Compatibility. For the duration of this Agreement, Provider will ensure the continued compatibility of the Products with all major releases, updates, or upgrades of any third-party software used by County for access or operation of the System, including without limitation Active Directory (AD) and Geographic Information System Mapping (GIS). In the event Provider is not able to support any third-party software update, upgrade, or new release that changes major functionality and is not backwards compatible with the Products, Provider shall use all reasonable efforts to resolve such issues and to provide optimal functionality of the Software or the Hosted Service in accordance with this Agreement. If Provider is unable to provide continued optimal functionality of the Products in accordance with this Agreement due to any third-party software release, update, or upgrade, County shall be entitled to a refund of any Support and Maintenance Fees or Subscription Fee paid for the affected time period and affected Products and may, at County's sole election, terminate the Agreement upon written notice with no further obligation to Provider.

3.7. Documentation. Provider shall deliver copies of the Documentation to County concurrently with delivery of the Products, and thereafter shall promptly provide any updated Documentation as it becomes available during the term of this Agreement. Provider represents and warrants that the Documentation is sufficiently comprehensive and of sufficient quality to enable a competent user to operate the Products efficiently and in accordance with **Exhibit A**. County has the right to copy, reproduce, modify, and create derivative works utilizing the Documentation as County deems necessary provided such activities are solely for the purpose of use of the Products as permitted under this Agreement.

3.8. Optional Services. If any goods or services under this Agreement, or the quantity thereof, are identified as optional ("Optional Services"), County may select the type, amount, and timing of Optional Services pursuant to a work authorization ("Work Authorization") in substantially the form attached as **Exhibit F** executed by Provider and County pursuant to this section. Any Optional Services procured, when combined with the required goods or services under this Agreement, shall not result in a payment obligation exceeding the applicable maximum amount stated in Section 5.1. Notwithstanding anything to the contrary in this Agreement, Work Authorizations shall be executed on behalf of County as follows: (a) the Contract Administrator may execute Work Authorizations for which the total aggregate cost to County is less than $50,000.00; (b) the Purchasing Director may execute Work Authorizations for which the total aggregate cost to County is within the Purchasing Director's delegated authority; and (c) any Work Authorization above the Purchasing Director's delegated authority requires express

approval by the Board. Provider shall not commence work on any Work Authorization until receipt of a purchase order and issuance of a Notice to Proceed by the Contract Administrator**.**

ARTICLE 4. TERM AND TIME OF PERFORMANCE

4.1. Term. This Agreement begins on the date it is fully executed by the Parties ("Effective Date"). The initial term of the Agreement shall be for a period of five (5) years from the Effective Date ("Initial Term"), unless otherwise terminated as provided in this Agreement. The Initial Term, Extension Term(s), and any Additional Extension as defined in this article are collectively referred to as the "Term."

4.2. Extensions. County may extend this Agreement for up to five (5) additional one (1) year terms (each an "Extension Term") on the same terms and conditions stated in this Agreement by sending notice to Provider at least thirty (30) days prior to the expiration of the then-current term. The Purchasing Director is authorized to exercise any Extension Term(s), and notice of same to Provider only by electronic mail shall be effective and sufficient. If County extends this Agreement and such extension results in increased financial obligations to Provider, and Provider is able to demonstrate to County's satisfaction that the increased financial obligations were outside of Provider's control and impact its actual costs in providing Services under this Agreement, then the Parties agree to negotiate in good faith to agree upon an amendment to the rates set forth in **Exhibit B** for the Extension Term to mitigate the demonstrated impact to Provider's actual costs resulting specifically from increased financial obligations.

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 Term remains available and expiration of this Agreement would, as determined by the Purchasing Director, result in a gap in Services deemed necessary by County, then the Purchasing Director may extend this Agreement for period(s) not to exceed three (3) months in the aggregate ("Additional Extension") on the same rates, terms, and conditions as existed at the end of the then-current term. The Purchasing Director may exercise the Additional Extension by written notice to Provider at least thirty (30) days prior to the end of the then-current term stating the duration of the Additional Extension. The Additional Extension must be within the authority of the Purchasing Director or otherwise authorized by the Board.

4.4. 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 pursuant to Chapter 129 and, if applicable, Chapter 212, Florida Statutes.

4.5. Timetable. If Provider fails to achieve Final Acceptance within twenty-four (24) months after the Effective Date, County shall have the option to terminate the Agreement by written notice from its Contract Administrator, in which event all sums paid by County under this Agreement, if any, shall be reimbursed to County by Provider within fifteen (15) days. For purposes of this section, any delays caused by County prior to Final Acceptance shall extend the Final Acceptance deadline by the same number of days as the delay caused by County.

4.6. Time of the Essence. Time is of the essence for Provider's performance of the duties, obligations, and responsibilities required by this Agreement.

ARTICLE 5. COMPENSATION

5.1. Maximum Amounts. For all goods and Services provided under this Agreement, County will pay Provider up to a maximum amount as follows:

Services/Goods	Term	Not-To-Exceed Amount
Software License Fees and Subscription Fees	Initial Term	$405,075.00
Services and Support and Maintenance	Initial Term	$3,557,236.00
Support and Maintenance and Subscription Fees for Extension Terms	Extension Term(s)	$3,241,839.00
Equipment	Duration of Agreement	$2,270,850.00
Optional Services	Duration of Agreement	$25,000.00
TOTAL NOT TO EXCEED		$9,500,000.00

Payment shall be made only for Services actually performed and completed, and Equipment actually provided, repaired, or installed, pursuant to this Agreement, as set forth in **Exhibit B** (Payment Schedule), which amount shall be accepted by Provider as full compensation for all such Services. Provider acknowledges that the amounts set forth in this Agreement are the maximum amounts payable and constitute a limitation upon County's obligation to compensate Provider for goods and Services. These maximum amounts, however, do not constitute a limitation of any sort upon Provider's obligation to perform all Services.

5.2. Method of Billing and Payment.

5.2.1. Unless otherwise stated in **Exhibit B**, Provider must submit invoices no more often than once monthly, but only after the Services invoiced have been completed. Invoices are due within fifteen (15) days after the end of the month covered by the invoice, except that the final invoice must be received no later than sixty (60) days after expiration or earlier termination of this Agreement. Unless otherwise stated in **Exhibit B** or the applicable Work Authorization, any Optional Services shall be invoiced in accordance with the existing invoicing schedule for any like goods or services provided under this Agreement, including (if applicable) invoiced pro rata for the initial invoice period. Invoices shall describe the Services performed and, as applicable, the personnel, hours, tasks, or other details as requested by the Contract Administrator. Provider shall submit a Certification of Payments to Subcontractors and Suppliers in the form provided by County with each invoice that includes Services performed by a Subcontractor. The certification shall be accompanied by a copy of the notification sent to each unpaid

Subcontractor listed on the form, explaining the good cause why payment has not been made to that Subcontractor.

5.2.2. Invoices shall be in the amounts set forth in **Exhibit B** for the applicable Services, minus any agreed upon retainage as stated in **Exhibit B**. Retainage amounts shall only be invoiced upon completion of all Services, unless otherwise stated in **Exhibit B**.

5.2.3. County shall pay Provider within thirty (30) days after receipt of Provider's proper invoice, in accordance with the "Broward County Prompt Payment Ordinance," Section 1 51.6 of the Code. To be deemed proper, all invoices must: (a) comply with all applicable requirements set forth in this Agreement or the Code; and (b) must be submitted on the then-current County form and pursuant to instructions prescribed by the Contract Administrator. Payment may be withheld for failure of Provider to comply with a term, condition, or requirement of this Agreement.

5.2.4. Provider must pay Subcontractors and suppliers within fifteen (15) days after receipt of payment from County for such subcontracted work or supplies. Provider 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 after 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 Provider demonstrates to Contract Administrator's satisfaction that such failure to pay results from a bona fide dispute with the Subcontractor or supplier and, further, Provider promptly pays the applicable amount(s) to the Subcontractor or supplier upon resolution of the dispute. Provider shall include requirements substantially similar to those set forth in this subsection in its contracts with Subcontractors and suppliers.

5.3. Reimbursable Expenses. Provider shall not be reimbursed for any expenses it incurs unless expressly provided for in this Agreement. For reimbursement of any travel costs or travel-related expenses permitted under this Agreement, Provider agrees to comply with Section 112.061, Florida Statutes, except to the extent that **Exhibit B** expressly provides otherwise. County shall not be liable for any expenses that exceed those allowed by Section 112.061 or that were not approved in writing in advance by the Contract Administrator.

5.4. Subcontractors. Provider shall invoice Subcontractor fees only in the actual amount paid by Provider, without markup or other adjustment.

5.5. Withholding by County; Overcharges. Notwithstanding any provision of this Agreement to the contrary, County may withhold payment, in whole or in part, (a) in accordance with Applicable Law, or (b) to the extent necessary to protect itself from loss on account of (i) inadequate or defective work that has not been remedied or resolved in a manner satisfactory to the Contract Administrator, or (ii) Provider's failure to comply with any provision of this Agreement.

5.6. Fixed Pricing. Unless otherwise stated in **Exhibit B**, prices shall remain firm and fixed for the Term, including any extension terms. However, Provider may offer incentive or volume discounts to County at any time.

ARTICLE 6. DELIVERY, TESTING, AND ACCEPTANCE

6.1. Delivery. Unless otherwise stated in **Exhibit A**, Provider shall, within seven (7) days after the Effective Date, make the Software and the Hosted Service available electronically to County. All County license keys, usernames, and passwords shall be authenticated by Provider and perform according to **Exhibit A** (Statement of Work).

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

6.2.1. The testing period shall commence on the first business day after Provider informs County in writing that it has completed the Services required to be performed prior to testing and that the System is ready for testing, and shall continue for a period of up to thirty (30) days. During the testing period, County may notify Provider in writing of any error or defect in the System so that Provider may make any needed modifications or repairs. If Provider so elects in writing, testing will cease until Provider resubmits for Final Acceptance testing, at which time the testing period shall be reset to that of a first submission for testing.

6.2.2. County shall notify Provider in writing of its Final Acceptance or rejection of the System, or any part thereof, within fifteen (15) days after the end of the testing period, as same may be extended or reset. If County rejects the System, or any part thereof, County shall provide notice identifying the criteria for Final Acceptance that the System failed to meet. Following such notice, Provider shall have thirty (30) days to (a) modify, repair, or replace the System or any portion thereof, or (b) otherwise respond to County's notice. If Provider modifies, repairs, or replaces the System or portion thereof, the testing period shall re-commence consistent with the procedures set forth above in this Section 6.2.

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

ARTICLE 7. CONFIDENTIAL INFORMATION, PROPRIETARY RIGHTS, SECURITY REQUIREMENTS

7.1. Provider Confidential Information. Provider represents that the Software and the Hosted Service contain proprietary products and trade secrets of Provider. Accordingly, to the full extent permissible under Applicable Law, County agrees to treat intellectual property within the Software or the Hosted Service as confidential in accordance with this article. For any other material submitted to County, Provider must separately submit and conspicuously label as "RESTRICTED MATERIAL – DO NOT PRODUCE" any material (a) that Provider contends, constitutes, or contains its trade secrets under Chapter 688, Florida Statutes, or (b) for which Provider asserts a right to withhold from public disclosure as confidential or otherwise exempt from production under Florida public records laws (including Chapter 119, Florida Statutes) (collectively, "Restricted Material"). In addition, Provider must, simultaneous with the submission of any Restricted Material, provide a sworn affidavit from a person with personal knowledge attesting that the Restricted Material constitutes trade secrets or is otherwise exempt or confidential under Florida public records laws, including citing the applicable Florida statute and specifying the factual basis for each such claim. Upon request by County, Provider must promptly identify the specific applicable statutory section that protects any particular document. If a third party submits a request to County for records designated by Provider as Restricted Material or for trade secret material in the Software or the Hosted Service, County shall refrain from disclosing such material unless otherwise ordered by a court of competent jurisdiction, authorized in writing by Provider, or the claimed exemption is waived. Any failure by Provider to strictly comply with the requirements of this section shall constitute Provider's waiver of County's obligation to treat the records as Restricted Material. Provider must 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 nondisclosure of Restricted Material or materials relating to the Software or the Hosted Service in response to a third-party request.

7.2. County Confidential Information. All materials, data, transactions of all forms, financial information, documentation, inventions, designs, and methods that Provider obtains from County in connection with this Agreement, that are made or developed by Provider in the course of the performance of the Agreement, or in which County holds proprietary rights, constitute "County Confidential Information." All County-provided employee information, financial information, and personally identifiable information for individuals or entities interacting with County (including, without limitation, social security numbers, birth dates, banking and financial information, and other information deemed exempt or confidential under Applicable Law) also constitute "County Confidential Information."

7.2.1. County Confidential Information may not, without the prior written consent of County, or as otherwise required by Applicable Law, be used by Provider or its employees, agents, Subcontractors or suppliers for any purpose other than for the benefit of County pursuant to this Agreement. Neither Provider nor its employees, agents, Subcontractors, or suppliers may sell, transfer, publish, disclose, display, license, or otherwise make available to any other person or entity any County Confidential Information without the prior written consent of County.

7.2.2. Provider expressly agrees to be bound by and to defend, indemnify, and hold harmless County and its officers and employees from the breach of Applicable Law by Provider or its employees, agents, Subcontractors, or suppliers regarding the unlawful use or disclosure of County Confidential Information.

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

7.3. Maintenance of Confidential Information. Each Party shall advise its employees, agents, Subcontractors, and suppliers who receive or otherwise have access to the other Party's Confidential Information (as described in Section 7.1 or Section 7.2, as applicable) of their obligation to keep such information confidential, and shall promptly advise the other party in writing if it learns of any unauthorized use or disclosure of said Confidential Information. In addition, the Parties agree to cooperate fully and provide all reasonable assistance to ensure the confidentiality of the other Party's Confidential Information as described in this article.

7.4. County Proprietary Rights. Provider acknowledges and agrees that County retains all rights, title, and interest in and to all materials, data, documentation, and copies thereof furnished by County to Provider under this Agreement, including all copyright and other proprietary rights therein, which Provider as well as its employees, agents, Subcontractors, and suppliers may use only in connection with the performance of this Agreement.

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

7.6. Data and Privacy. Provider shall comply with all applicable data and privacy laws and regulations, including without limitation Section 501.171, Florida Statutes, and shall ensure that County data processed, transmitted, or stored by Provider or in the System is not accessed, transmitted, or stored outside the United States. Provider shall not sell, market, publicize, distribute, or otherwise make available to any third party any personal identification information (as defined by Sections 501.171, Section 817.568, or Section 817.5685, Florida Statutes, as amended) that Provider 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, Provider shall ensure that all hard drives or other storage devices and media that contained County data have been wiped in accordance with the then-current best industry practices, including without limitation DOD 5220.22-M, and that an appropriate data wipe certification is provided to the satisfaction of the Contract Administrator.

7.7. Security Requirements. Provider, the Products, and the System must meet or exceed all security requirements set forth in **Exhibit C** at all times throughout the duration of the Term, unless otherwise expressly approved in writing by the County's Chief Information Officer or their designee. Provider will cooperate with County and provide any and all information that County may reasonably request to determine appropriate security and network access restrictions and verify Provider compliance with County security requirements, including as stated in this section.

7.8. Custom Work Products. To the extent this Agreement (including the Statement of Work, any subsequent Work Authorization, any amendment, or the procurement documents relating to this Agreement) identifies deliverables that constitute custom work products that Provider is required to develop and furnish, the Parties agree that County shall own all rights, title, and interest in and to all such custom work products and that they shall be deemed to constitute "works made for hire" under the United States Copyright Act, 17 U.S.C. § 101. If, for any reason, any custom work product would not be considered a "work made for hire" under Applicable Law, Provider hereby exclusively and irrevocably sells, assigns, and transfers to County all of Provider's rights, title, and interest in and to such custom work product and in and to any copyright or copyright application(s) related thereto. Provider agrees that neither it nor its agents shall use or disclose any custom work product except for County's benefit as required in connection with Provider's performance under this Agreement, unless Provider has obtained County's prior written consent to such use or disclosure. "Custom work product" shall not include any software, copyrighted material, or other proprietary material developed by Provider or any third party prior to the Effective Date, but shall include any modification(s) thereof developed pursuant to this Agreement. To the full extent applicable, Provider shall provide County with the source code and object code for all custom work products upon Final Acceptance of the Software or System, or

within thirty (30) calendar days after written request by the Contract Administrator, whichever occurs first.

7.9. Injunctive Relief; Survival. The Parties represent and agree that neither damages nor any other legal remedy is adequate to remedy any breach of this article, and that the injured party shall therefore be entitled to injunctive relief to restrain or remedy any breach or threatened breach. The obligations under this article shall survive the termination of this Agreement or of any license granted under this Agreement.

ARTICLE 8. REPRESENTATIONS AND WARRANTIES

8.1. Ownership. Provider represents and warrants that it is the owner of all right, title, and interest in and to the Software and the Hosted Service or that it has the right to grant to County the rights and the licenses granted under this Agreement, and that Provider has not knowingly granted rights or licenses to any other person or entity that would restrict rights and licenses granted hereunder, except as may be expressly stated herein.

8.2. Limited Warranty. For the full term of this Agreement, Provider represents and warrants to County that the Products and System will perform substantially as described in the Documentation and in the Statement of Work (**Exhibit A**). This warranty does not cover any failure of the Products resulting from (a) use of the Products in a manner other than that for which they were intended; (b) any modification of the Products by County that is not authorized by Provider; or (c) County's provision of improperly formatted data to be processed through the System.

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

8.4. ADA Compliance. Provider represents and warrants that the Products and System are, and for the duration of the Agreement will remain, fully accessible and compliant with the Americans with Disabilities Act, 42 U.S.C. § 12101, Section 504 of the Rehabilitation Act of 1973, and all other Applicable Law, and that the Products and System meet or exceed the World Wide Web Consortium/Web Content Accessibility Guidelines (WCAG) 2.1 Level AA standard or any higher standard as may be adopted by the International Organization for Standardization. Upon request, Provider will provide County with any accessibility testing results and written documentation verifying accessibility, as well as promptly respond to and resolve accessibility complaints.

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

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

8.7. Solicitation Representations. Provider represents and warrants that all statements and representations made in Provider'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 Provider executes this Agreement, unless otherwise expressly disclosed in writing by Provider.

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

8.9. Truth-In-Negotiation Representation. Provider's compensation under this Agreement is based upon its representations to County, and Provider certifies that the wage rates, factual unit costs, and other information supplied to substantiate Provider's compensation, including without limitation those made by Provider during the negotiation of this Agreement, are accurate, complete, and current as of the date Provider executes this Agreement. Provider'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.

8.10. Public Entity Crime Act. Provider represents that it is familiar with the requirements and prohibitions under the Public Entity Crime Act, Section 287.133, Florida Statutes, and represents that its entry into this Agreement will not violate that Act. Provider further represents that there has been no determination that it committed a "public entity crime" as defined by Section 287.133, Florida Statutes, and that it has not been formally charged with committing an act defined as a "public entity crime" regardless of the amount of money involved or whether Provider has been placed on the convicted vendor list.

8.11. Discriminatory Vendor and Scrutinized Companies Lists; Countries of Concern. Provider 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 Sections 215.473 or 215.4725, Florida Statutes. Provider represents and certifies that it is not, and for the duration of the Term will not be, ineligible to contract with County on any of the grounds stated in Section 287.135, Florida Statutes. Provider represents that it is, and for the duration of the Term will remain, in compliance with Section 286.101, Florida Statutes.

8.12. Claims Against Provider. Provider 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 Provider, threatened against or affecting Provider, the outcome of which may (a) affect the validity or enforceability of this Agreement, (b) materially and adversely affect the authority or ability of Provider 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 Provider or on the ability of Provider to conduct its business as presently conducted or as proposed or contemplated to be conducted.

8.13. Verification of Employment Eligibility. Provider represents that Provider and each Subcontractor have registered with and use the E-Verify system maintained by the United States Department of Homeland Security to verify the work authorization status of all newly hired employees in compliance with the requirements of Section 448.095, Florida Statutes, and that entry into this Agreement will not violate that statute. If Provider violates this section, County may immediately terminate this Agreement for cause and Provider shall be liable for all costs incurred by County due to the termination.

8.14. Warranty of Performance. Provider 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 Services. Provider represents and warrants that the Services shall be performed in a skillful and respectful manner, and that the quality of all Services shall equal or exceed prevailing industry standards for the provision of such services.

8.15. Prohibited Telecommunications Equipment. Provider represents and certifies that Provider and all Subcontractors do not use any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, as such terms are used in 48 CFR §§ 52.204-24 through 52.204-26. Provider represents and certifies that Provider and all Subcontractors shall not provide or use such covered telecommunications equipment, system, or services during the Term.

8.16. Criminal History Screening Practices. If this Agreement is subject to the requirements of Section 26-125(d) of the Code, Provider represents and certifies that Provider will comply with Section 26-125(d) of the Code for the duration of the Term.

8.17. Construction Apprenticeship Program. If this Agreement is a construction contract as defined in Section 26-9 of the Code, Provider represents and certifies that it shall at all times comply with the requirements of the Construction Apprenticeship Program as set forth in Sections 26-8 through 26-11 of the Code.

8.18. Domestic Partnership Requirement. Unless this Agreement is exempt from the provisions of the "Broward County Domestic Partnership Act," Section 16½-157 of the Code ("Act"), Provider certifies and represents that it shall at all times comply with the provisions of the Act. The contract language referenced in the Act is deemed incorporated in this Agreement as though fully set forth in this section.

8.19. Breach of Representations. Provider acknowledges that County is materially relying on the representations, warranties, and certifications of Provider stated in this article, and County shall be entitled to exercise any or all of the following remedies if any such representation, warranty, or certification is untrue: (a) recovery of damages incurred; (b) termination of this Agreement without any further liability to Provider; (c) set off from any amounts due Provider the full amount of any damage incurred; and (d) debarment of Provider.

ARTICLE 9. INDEMNIFICATION AND LIMITATION OF LIABILITY

9.1. Indemnification. Provider shall indemnify, hold harmless, and defend County and all of County's current, past, and future officers, agents, 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 breach of this Agreement by Provider, or any intentional, reckless, or negligent act or omission of Provider, its officers, employees, or agents, arising from, relating to, or in connection with this Agreement (collectively, a "Claim"). If any Claim is brought against an Indemnified Party, Provider shall, upon written notice from County, defend each Indemnified Party with 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 Provider 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.

9.2. Infringement Remedy. If the Products or any portion thereof are finally adjudged to infringe, or in Provider's opinion are likely to become the subject of such a Claim, Provider shall, at County's option, either: (i) procure for County the right to continue using the Products; (ii) modify or replace the Products to make them noninfringing; or (iii) refund to County all fees paid under this Agreement. Provider shall have no liability regarding any infringement claim caused by any County modification of the Products not specifically authorized in writing by Provider.

9.3. Limitation of Liability. Neither Provider nor County shall be liable to the other party for any damages under this Agreement that exceed the largest of the following amounts: (a) $100,000; (b) twice the maximum compensation amount specified in Section 5.1; or (c) the amount of insurance Provider is required to provide under Article 10. Neither party shall be liable for the other party's special, indirect, punitive, or consequential damages (including damages resulting from lost data or records other than costs incurred in the recovery thereof), even if the party has been advised that such damages are possible, or for the other party's lost profits, lost revenue, or lost institutional operating savings. These limitations of liability shall not apply to (i) any Claim resulting from Provider's actual or alleged disclosure of County Confidential Information or resulting from an actual or alleged data breach in violation of Applicable Law, (ii) any Claim resulting from an actual or alleged infringement of any interest in any Product, or (iii) any indemnification obligation under this Agreement.

ARTICLE 10. INSURANCE

10.1. Throughout the Term, Provider shall, at its sole expense, maintain the minimum insurance coverages stated in **Exhibit E** in accordance with the terms and conditions of this article. Provider shall maintain insurance coverage against claims relating to any act or omission by Provider, 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.

10.2. Provider shall ensure that "Broward County" is listed and endorsed as an additional insured as stated in **Exhibit E** on all policies required under this article.

10.3. On or before the Effective Date or at least fifteen (15) days prior to commencement of Services, as may be requested by County, Provider shall provide County with a copy of all Certificates of Insurance or other documentation sufficient to demonstrate the insurance coverage required in this article. If and to the extent requested by County, Provider shall provide complete, certified copies of all required insurance policies and all required endorsements within thirty (30) days after County's request.

10.4. Provider shall ensure that all insurance coverages required by this article remain in full force and effect without any lapse in coverage throughout the Term and until all performance required by Provider has been completed, as determined by Contract Administrator. Provider 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).

10.5. All required insurance policies must be placed with insurers or surplus line carriers authorized to conduct business in the State of Florida with an A.M. Best rating of A- or better and a financial size category class VII or greater, unless otherwise approved by County's Risk Management Division in writing.

10.6. If Provider maintains broader coverage or higher limits than the insurance requirements stated in **Exhibit E**, County shall be entitled to all such broader coverages and higher limits. All required insurance coverages shall provide primary coverage and not require contribution from any County insurance, self-insurance or otherwise, which shall be in excess of and shall not contribute to the required insurance provided by Provider.

10.7. Provider shall declare in writing any self-insured retentions or deductibles over the limit(s) prescribed in **Exhibit E** and submit to County for approval at least fifteen (15) days prior to the Effective Date or commencement of Services. Provider shall be solely responsible for and shall pay any deductible or self-insured retention applicable to any claim against County. County may, at any time, require Provider 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. Provider agrees that any deductible or self-insured retention may be satisfied by either the named insured or County, if so elected by County, and Provider agrees to obtain same in endorsements to the required policies.

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

10.9. Provider 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 Provider under this article. Provider 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. Provider shall not permit any Subcontractor to provide Services unless and until all applicable requirements of this article are satisfied.

10.10. If Provider 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 Provider. If requested by County, Provider shall provide, within one (1) business day, evidence of each Subcontractor's compliance with this article.

10.11. 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 E**; 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, Provider must obtain and maintain "extended reporting" coverage that applies after termination or expiration of the Agreement for at least the duration stated in **Exhibit E**.

ARTICLE 11. TERMINATION

11.1. Termination for Cause. 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 be terminated for cause by County for reasons including, but not limited to, any of the following:

11.1.1. Provider'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;

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

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

Unless otherwise stated in this Agreement, if this Agreement was approved by Board action, termination for cause by County must be by action of the Board or the County Administrator; in any other instance, termination for cause may be by the County Administrator, the County representative expressly authorized under this Agreement, or the County representative (including any successor) who executed the Agreement on behalf of County. If County erroneously, improperly, or unjustifiably terminates this Agreement for cause, such termination shall be deemed a termination for convenience pursuant to Section 11.2 effective thirty (30) days after such notice was provided and Provider shall be eligible for the compensation provided in Section 11.2 as its sole remedy.

11.2. Termination for Convenience; Other Termination. This Agreement may also be terminated for convenience by the Board with at least thirty (30) days advance written notice to Provider. Provider acknowledges that it has received good, valuable, and sufficient consideration for County's right to terminate this Agreement for convenience including in the form of County's obligation to provide advance notice to Provider of such termination in accordance with this section. 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 this Agreement is terminated by County pursuant to this section, Provider 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, and County shall have no further obligation to pay Provider for Services under this Agreement.

11.3. 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.

11.4. In addition to any termination rights stated in this Agreement, County shall be entitled to seek any and all available contractual or other remedies available at law or in equity.

ARTICLE 12. EQUAL EMPLOYMENT OPPORTUNITY AND CBE COMPLIANCE

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

12.2. By January 1 of each year, Provider must submit, and cause each Subcontractor to submit, an Ownership Disclosure Form (or such other form or information designated by County), available at https://www.broward.org/econdev/Pages/forms.aspx, identifying the ownership of the entity and indicating whether the entity is majority-owned by persons fitting specified classifications.

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

12.4. Provider must meet or exceed the required CBE goal by utilizing the CBE firms listed in **Exhibit H** (or a CBE firm substituted for a listed firm, if permitted) for twenty-one and 30/100 percent (21.30%) of non-proprietary Equipment and Services (the "Commitment") for the scope of work and the percentage of work amounts identified on each Letter of Intent. Promptly upon execution of this Agreement by County, Provider shall enter into formal contracts with the CBE firms listed in **Exhibit H** and, upon request, shall provide copies of the contracts to the Contract Administrator and OESBD.

12.5. Each CBE firm utilized by Provider to meet the CBE goal must be certified by OESBD. Provider shall inform County immediately when a CBE firm is not able to perform or if Provider believes the CBE firm should be replaced for any other reason, so that OESBD may review and verify the good faith efforts of Provider to substitute the CBE firm with another CBE firm, as applicable. Whenever a CBE firm is terminated for any reason, Provider shall provide written notice to OESBD and, upon written approval of the Director of OESBD, shall substitute another

CBE firm in order to meet the CBE goal, unless otherwise provided in this Agreement or agreed in writing by the Parties. Such substitution shall not be required 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, Provider shall notify County, and OESBD may adjust the CBE goal by written notice to Provider. Provider shall not terminate a CBE firm for convenience without County's prior written consent, which consent shall not be unreasonably withheld.

12.6. The Parties stipulate that if Provider fails to meet the Commitment, the damages to County arising from such failure are not readily ascertainable at the time of contracting. If Provider fails to meet the Commitment and County determines, in the sole discretion of the OESBD Program Director, that Provider failed to make Good Faith Efforts (as defined in Section 1-81 of the Code) to meet the Commitment, Provider shall pay County liquidated damages in an amount equal to fifty percent (50%) of the actual dollar amount by which Provider failed to achieve the Commitment, up to a maximum amount of ten percent (10%) of the total contract amount excluding costs and reimbursable expenses. An example of this calculation is stated in Section 1-81.7 of the Code. As elected by County, such liquidated damages amount shall be either credited against any amounts due from County, or must be paid to County within thirty (30) days after written demand. These liquidated damages shall be County's sole contractual remedy for Provider's breach of the Commitment, but shall not affect the availability of administrative remedies under Section 1-81 of the Code. Provider acknowledges and agrees that the liquidated damages provided in this section are proportionate to an amount that might reasonably be expected to flow from a breach of the Commitment and are not a penalty. 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 Provider, shall not be deemed a failure by Provider to meet the Commitment.

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

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

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

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

ARTICLE 13. PAYMENT AND PERFORMANCE BOND

13.1. Within ninety (90) days after the Effective Date, Provider shall furnish County with an initial Payment and Performance Bond in a form acceptable to County, or an alternative form of security, which may be in the form of cash, money order, certified check, cashier's check, or an original irrevocable letter of credit (collectively "Security"), in an amount equal to Four Million Two Hundred Seventy-Three Thousand Eight Hundred Eighty-Five Dollars ($4,273,885.00) as security for the Services required of Provider during Agreement Year 1 through Agreement Year 3. On the first (1st) day of Agreement Year 4 the Security amount shall adjust as indicated below to include the total of the Subscription Fees and Support and Maintenance Fees for each respective Agreement Year as follows:

Agreement Year	Security Amount
4	$589,038.00
5	$723,109.00
6 (if extended)	$617,602.00
7 (if extended)	$632,530.00
8 (if extended)	$647,906.00
9 (if extended)	$663,744.00
10 (if extended)	$680,056.00

13.2. The Aviation Department, upon fourteen (14) calendar days' written notice to Provider, may require an increase in the amount of the Security to reflect any increases in the monies payable hereunder.

13.3. The Security required by this article must be executed by a surety company of recognized standing, authorized to do business in the State of Florida as surety, having a resident agent in the State of Florida, and having been in business with a record of successful continuous operation for at least the immediately preceding five (5) years.

ARTICLE 14. MISCELLANEOUS

14.1. Contract Administrator Authority. The Contract Administrator is authorized to coordinate and communicate with Provider to manage and supervise the performance of this Agreement. Provider acknowledges that the Contract Administrator has no authority to make changes that would increase, decrease, or otherwise materially modify the scope of services to be provided under this Agreement except as expressly set forth in this Agreement or, to the extent applicable, in the Broward County Procurement Code. Unless expressly stated otherwise in this Agreement or otherwise set forth in the Code or the Broward County Administrative Code, the Contract Administrator may exercise ministerial authority in connection with the day-to-day management of this Agreement. The Contract Administrator may also approve in writing minor modifications to the scope of Services that do not increase the total cost to County or waive any rights of County.

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

14.3. Public Records. Notwithstanding anything else in this Agreement, any action taken by County in compliance with, or in a good faith attempt to comply with, the requirements of Chapter 119, Florida Statutes, shall not constitute a breach of this Agreement. If Provider is acting on behalf of County as stated in Section 119.0701, Florida Statutes, Provider shall:

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

14.3.2. 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 Applicable Law;

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

14.3.4. Upon expiration of the Term or termination of this Agreement, transfer to County, at no cost, all public records in possession of Provider or keep and maintain public records required by County to perform the services. If Provider transfers the records to County,

Provider shall destroy any duplicate public records that are exempt or confidential and exempt. If Provider keeps and maintains the public records, Provider shall meet all requirements of Applicable Law 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.

14.4. If Provider receives a request for public records regarding this Agreement or the Services, Provider must immediately notify the Contract Administrator in writing and provide all requested records to County to enable County to timely respond to the public records request. County will respond to all such public records requests.

IF PROVIDER HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO PROVIDER'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS AGREEMENT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT (954) 359-6100, SNESBETH@BROWARD.ORG AND ALSO COPY CONTACTFLL@BROWARD.ORG, 320 TERMINAL DRIVE, SUITE 200, FORT LAUDERDALE, FLORIDA 33315.

14.5. Audit Rights and Retention of Records. County shall have the right to audit the books, records, and accounts of Provider and all Subcontractors that are related to this Agreement. Provider and all Subcontractors shall keep such books, records, and accounts as may be necessary 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, Provider and all Subcontractors shall make same available in written form at no cost to County. Provider shall provide County with reasonable access to Provider's facilities, and County shall be allowed to interview all current or former employees to discuss matters pertinent to the performance of this Agreement.

Provider and all 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. This article shall survive any dispute or litigation between the Parties, and Provider expressly acknowledges and agrees to be bound by this article throughout the course of any dispute or litigation with County. Any audit or inspection pursuant to this section may be performed by any County representative (including any outside representative engaged by County). Provider hereby grants County the right to conduct such audit or review at Provider's place of business, if deemed appropriate by County, with seventy-two (72) hours' advance notice. Provider shall make all such records and documents available electronically in common file formats or via remote access if, and to the extent, requested by County.

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 reveals overpricing or overcharges to County of any nature by Provider in excess of five percent (5%) of the total contract billings reviewed by County, in addition to making adjustments for the overcharges, Provider shall pay the reasonable cost of County's audit. 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 Provider.

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

14.6. Independent Contractor. Provider 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 Provider nor its agents shall act as officers, employees, or agents of County. Provider shall not have the right to bind County to any obligation not expressly undertaken by County under this Agreement.

14.7. 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 Applicable Law 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.

14.8. Sovereign Immunity. Except to the extent sovereign immunity may be deemed 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.

14.9. Third-Party Beneficiaries. Neither Provider 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.

14.10. Notice and Payment Address. Unless otherwise stated herein, for 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). Payments shall be made to the noticed address for Provider. Addresses may be changed by the applicable Party giving notice of such change in accordance with this section.

FOR COUNTY:

Broward County Administrator
Attn: Governmental Center East
115 South Andrews Avenue, Room 409
Fort Lauderdale, Florida 33301
Email address: mcepero@broward.org

with a copy to:

Broward County Director of Aviation
320 Terminal Drive, Suite 200
Fort Lauderdale, Florida 33315
Email address: mgale@broward.org

FOR PROVIDER:

Designa Access Corporation
Attn: John Curtiss, President and CEO
4401 South Pinemont Drive, Suite 200
Houston, Texas 77041
Email address: john.curtiss@designa.com

14.11. 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 approved subcontracting, neither this Agreement nor any right or interest in it may be assigned, transferred, subcontracted, or encumbered by Provider 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. County reserves the right to condition its approval of any assignment, transfer, encumbrance, or subcontract upon further due diligence and an additional fee paid to County to reasonably compensate it for the performance of any such due diligence.

14.12. Conflicts. Neither Provider nor its employees shall have or hold any continuing or frequently recurring employment or contractual relationship that is substantially antagonistic or incompatible with Provider's loyal and conscientious exercise of judgment and care related to its performance under this Agreement. During the Term, none of Provider's officers or employees shall serve as an expert witness against County in any legal or administrative proceeding in which they or Provider is not a party, unless compelled by legal process. Further, such persons shall not give sworn testimony or issue a report or writing as an expression of such person's 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 legal process. The limitations of this section shall not preclude Provider 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 Provider is permitted pursuant to this Agreement to utilize Subcontractors to perform any Services required by this Agreement, Provider shall require such Subcontractors, by written contract, to comply with the provisions of this section to the same extent as Provider.

14.13. 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. 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 shall not be deemed a waiver of any subsequent breach and shall not be construed to be a modification of this Agreement. To be effective, any waiver must be in writing signed by an authorized signatory of the Party granting the waiver.

14.14. Compliance with Laws. Provider, the Products, the System, the Services, and Support and Maintenance must comply with all Applicable Law, including, without limitation, the Americans with Disabilities Act, 42 U.S.C. § 12101, Section 504 of the Rehabilitation Act of 1973, and the requirements of any applicable grant agreements.

14.15. 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.

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

14.17. 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 any other gender, and the singular shall include the plural, and vice versa, unless the context otherwise requires. Terms such as "herein" 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 subsections thereof, 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 reference to approval by County shall require approval in writing, unless otherwise expressly stated.

14.18. 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 within an article or section of this Agreement, the article or section shall prevail and be given effect.

14.19. 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. **EACH PARTY HEREBY EXPRESSLY WAIVES ANY RIGHTS IT MAY HAVE TO A TRIAL BY JURY OF ANY CIVIL LITIGATION RELATED TO THIS AGREEMENT**.

14.20. Amendments. Unless expressly authorized herein, no modification, amendment, or alteration of any portion of this Agreement is effective unless contained in a written document executed with the same or similar formality as this Agreement and by duly authorized representatives of County and Provider.

14.21. Prior Agreements. This Agreement represents the final and complete understanding of the Parties regarding the subject matter of this Agreement and supersedes all prior and contemporaneous negotiations and discussions regarding same. All commitments, agreements, and understandings of the Parties concerning the subject matter of this Agreement are contained herein.

14.22. 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 Provider 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"), Provider 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 www.broward.org/Purchasing/Pages/StandardTerms.aspx. The County Administrator is authorized to execute a Business Associate Agreement on behalf of County. Where required, Provider shall handle and secure such PHI in compliance with HIPAA, HITECH, and related regulations and, if required by HIPAA, HITECH, or other Applicable Law, include in its "Notice of Privacy Practices" notice of Provider'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. Provider shall ensure that the requirements of this section are included in all agreements with Subcontractors.

14.23. Payable Interest.

14.23.1. Payment of Interest. Unless prohibited by Applicable Law, County shall not be liable for interest to Provider for any reason, whether as prejudgment interest or for any other purpose, and Provider waives, rejects, disclaims, and surrenders any and all entitlement to interest in connection with a dispute or claim arising from, related to, or in connection with this Agreement.

14.23.2. 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).

14.24. 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.

14.25. Counterparts and Multiple Originals. This Agreement may be executed in multiple originals, and may be executed in counterparts, whether signed physically or electronically, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement.

14.26. Use of County Name or Logo. Provider shall not use County's name or logo in marketing or publicity materials without prior written consent from the Contract Administrator.

14.27. Drug-Free Workplace. If required under Section 21.23(f), Broward County Administrative Code, or Section 287.087, Florida Statutes, Provider certifies that it has and will maintain a drug-free workplace program throughout the Term.

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

14.29. Polystyrene Food Service Articles. Provider shall not sell or provide for use on County property expanded polystyrene products or food service articles (e.g., Styrofoam), unencapsulated expanded polystyrene products, or single-use plastic straws or stirrers, as set forth in more detail in Section 27.173, Broward County Administrative Code.

14.30. Civil Rights – General. Provider shall comply with pertinent statutes, executive orders, and such rules as are promulgated to ensure that no person shall, on the grounds of race, creed, color, national origin, sex, age, or disability, be excluded from participating in any activity conducted with or benefiting from federal financial assistance.

14.31. Civil Rights – Title VII Assurances. Provider shall abide by and comply with the nondiscrimination requirements set forth in **Exhibit J**, to the extent same are applicable by law, rule, or regulation, or federal grant requirements.

14.32. Nondiscrimination. Neither Party to this Agreement shall discriminate on the basis of race, color, sex, religion, national origin, disability, age, marital status, political affiliation, sexual orientation, pregnancy, or gender identity and expression in the performance of this Agreement. Provider shall include the foregoing or similar language in its contracts with any Subcontractors,

except that any project assisted by the U.S. Department of Transportation funds shall comply with the nondiscrimination requirements in 49 C.F.R. Parts 23 and 26.

14.33. Federal Fair Labor Standards Act (Federal Minimum Wage). This Agreement incorporates by reference the provisions of 29 C.F.R. Part 201, the Federal Fair Labor Standards Act ("FLSA"), with the same force and effect as if fully restated herein. The FLSA sets minimum wage, overtime pay, recordkeeping, and child labor standards for full and part time workers. Provider must comply with the FLSA and has full responsibility to monitor compliance with the referenced statute and regulation. Provider must address any claims or disputes that arise from this requirement directly with the U.S. Department of Labor – Wage and Hour Division.

14.34. Occupational Safety and Health Act of 1970. This Agreement incorporates by reference the requirements of 29 C.F.R. Part 1910 with the same force and effect as if fully restated herein. Provider must provide a work environment that is free from recognized hazards that may cause death or serious physical harm to the employee. Provider retains full responsibility to monitor its compliance and its Subcontractors' compliance with the applicable requirements of the Occupational Safety and Health Act of 1970 (20 C.F.R. Part 1910). Provider must address any claims or disputes that pertain to a referenced requirement directly with the U.S. Department of Labor Occupational Safety and Health Administration.

14.35. Security Regulations. Provider certifies and represents that it will comply with the Airport Security Requirements attached hereto and incorporated herein as **Exhibit K**.

14.36. Airport Issued Identification Media, Public Area Business Purpose Media, and Emergency Response Training. All employees, agents, representatives, Providers, and Subcontractors of Provider shall obtain Airport Issued Identification Media or Public Area Business Purpose Media, and complete emergency response training, as required by Section 2-43 of the Code. Provider shall comply with the requirements of Section 2-43 of the Code, including the requirement that Provider compensate its employees, agents, representatives, contractors, and Subcontractors for time spent completing the emergency response training.

14.37. Retention of Records. If this project is subject to a Federal Department of Transportation grant, in addition to complying with Section 14.5 of this Agreement, Provider shall preserve all Agreement records for a period of five (5) years after the latter of final payment or the completion of all Services to be performed pursuant to this Agreement.

14.38. Entities of Foreign Concern. If Provider has access to personal identifying information from County, Provider represents and certifies (i) Provider is not owned by the government of a foreign country of concern; (ii) the government of a foreign country of concern does not have a controlling interest in Provider; and (iii) Provider is not organized under the laws of, and does not have its principal place of business in, a foreign country of concern. On or before the later of the Effective Date or the date that Provider or any Subcontractor has access to such personal identifying information, the entity shall submit to County executed affidavit(s) under penalty of perjury, in a form approved by County attesting that the entity does not meet any of the criteria in Section 283.138(2), Florida Statutes. Provider must provide County a copy of the applicable

affidavit(s) prior to requesting further payment for Services. Compliance with the requirements of this section is included in the requirements of a proper invoice for purposes of Section 5.2. Terms used in this section that are not otherwise defined in this Agreement shall have the meanings ascribed to such terms in Section 238.138, Florida Statutes.

(THE REMAINDER OF THIS PAGE 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 _____, 2023, and DESIGNA ACCESS CORPORATION, signing by and through its _____, duly authorized to execute same.

COUNTY

ATTEST:

By: _____
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
Aviation Office
320 Terminal Drive, Suite 200
Fort Lauderdale, Florida 33315
Telephone: (954) 359-6100

By Yesenia Alfonso Digitally signed by Yesenia Alfonso Date: 2023.08.31 13:59:00 -04'00'
Yesenia Alfonso (Date)
Assistant County Attorney

By Sharon V. Thorsen Digitally signed by Sharon V. Thorsen Date: 2023.08.31 14:56:12 -04'00'
Sharon V. Thorsen (Date)
Senior Assistant County Attorney

YA/ch
Designa Access Corp.
08/28/23
#1040605.1

TECHNOLOGY PRODUCTS AGREEMENT BETWEEN BROWARD COUNTY AND DESIGNA ACCESS CORPORATION FOR PARKING ACCESS AND REVENUE CONTROL EQUIPMENT AND MAINTENANCE FOR FORT LAUDERDALE-HOLLYWOOD INTERNATIONAL AIRPORT (RLI # PNC2119994R1)

PROVIDER

DESIGNA ACCESS CORPORATION

By: John Curtiss Digitally signed by John Curtiss Date: 2023.08.31 12:15:19 -05'00'
John Curtiss, President and CEO

_____
Print Name and Title

31st day of August, 2023

EXHIBIT A - STATEMENT OF WORK

Provider shall provide the following work under this Agreement:

1. **Project Outline**

Provider will provide County with the System, Software, Equipment, and Services required under this Agreement. The System will allow County to control, access, and collect parking revenues to increase the efficiency of the parking process by reducing transaction times, as it relates to controlled and measurable equipment actions, for customers and Airport Employees. Provider will perform all Services necessary to attain Final Acceptance. Provider will obtain all required permits, including, but not limited to, electrical, including low voltage, data installation and/or construction permits, and any other permits necessary for the installation of the System. Provider will install, configure, and maintain all application software and firmware required by the System. Provider must provide the complete installation of all Equipment and Software including site preparation, foundations, communication and power conduits and cables, and hard and soft connections.

2. **Services Description**

A. Software.

Provider will provide the Software listed in Attachment 1 to this Statement of Work ("SOW").

B. Equipment.

Provider will provide the Equipment listed in Attachment 2 to this SOW. All Equipment shall be factory finished with proper priming and powder coat finish to suit the environment in which it is to be installed. Final color shall be based on industry standard. All Equipment enclosures shall be properly gasketed and sealed to meet the ingress protection standards stated in the individual equipment data sheets provided by Provider on October 11, 2022.

The Equipment must be hardwired or wirelessly (as determined by County) networked via cellular network and connected to the System. Two-way communications shall be used to monitor equipment status, payments, and usage while also providing remote diagnostics and to change settings remotely (e.g., pricing or out of service notifications). Alternative wireless communication solutions may be considered at the sole discretion of County.

C. Interfaces/Integration.

Provider will ensure the System integrates and interfaces with County's existing third-party solutions as described below. Interfaces and integrations provided by Provider pursuant to this Agreement will be fully supported by Provider at no additional cost to County, and Provider will manage the maintenance of such interfaces and integrations. Provider shall configure the System such that County will have the ability to add, modify, or delete integrations or interfaces throughout the Term to ensure the System meets the needs of its users.

Provider will provide the interfaces detailed below, which must fully interface with all other County applications as identified by County and/or that are necessary for the full functionality of the System and achievement of the project's objectives, including, but not limited to, functionality necessary to batch uploads reflected in the table below and to conduct all Services required for full implementation of the System. County will assist Provider in identifying any additional interfaces needed to support County's business operations.

3rd Party Solution		
AVPMi	AVPMi is the valet parking system used at the Airport and must integrate with the System.	Allow for export of the valet parking system information for robust reporting.
Park Assist (PA)	Park Assist is the garage parking guidance system at the Airport and must integrate with the System.	Allow for export of parking occupancy information for robust reporting.
SunPass	SunPass toll system must integrate with the System.	Enable reading of Florida Department of Transportation toll passes and allow for import and export of information and communication for robust reporting.
Payment Solutions (Credit Card payment solutions; Google Pay; Apple Pay; and any other County approved payment solution application)	Payment Solutions integrations for contact and contactless payments for those solutions listed for the System and parking reservation system.	The System must have the ability to correlate diverse systems, including Credit Card, cash, parking reservation system, pay-by-phone, and remote-pay, including, but not limited to, Apple Pay, Google Pay, and any other County approved payment solution application, and must provide robust reporting functions for payment data.

3. **Project Approach**

A. Site Locations

Provider will perform Services at the following sites. Site names and site numbers may be used interchangeably throughout this SOW to refer to County sites.

Site 1 - Test Environment

Site 2 - Cypress Garage level 4 NW corner (4NW Communications Room/Server Location)

Site 3 - Hibiscus Garage level 1 behind the Parking Office (H2A2 Communications Room/Server Location

Site 4 - Parking Operations Office

Site 5 - Hibiscus Garage

Site 6 - Palm Garage

Site 7 - Cypress Garage

Site 8 - Employee Parking Lot 1

Site 9 - Employee Parking Lot 2

Site 10 - Valet Location at Terminal 1 upper-level curbside

Site 11 - Valet Location at Terminal 4 upper-level curbside

Site 12 - Production and Disaster Recovery Server Environments

4. **On-site Analysis**

Provider will perform a complete analysis of County's current operations. The results of this analysis will be used during the CDR (hereinafter defined) period to develop the transition plan for installation of the Equipment.

The analysis will include the twelve (12) County sites listed above. Provider will coordinate with the Aviation Department's Maintenance Division for a walk through of sites 1-12 to discuss intricate details of current and future equipment (as needed under Optional Services) of each site locations.

Provider will produce pre-built drawings of the conduits necessary for the Equipment and the size of the conduits, including any additional conduits required by the Aviation Department, and furnish and install all wiring required to make the System complete and operational pursuant to the itemized list of pricing for installation.

5. **Critical Design Review**

The Critical Design Review ("CDR") period is process by which the Parties jointly ensure all requirements as described in this SOW have been considered and all deliverables incorporated in the proposed design. The purpose of the CDR is to document and confirm the System's final design, including consistency with product specifications, for each configured item. The CDR process is an interactive process, including preliminary and interim critical design reviews to the extent necessary to present the final design for approval by County, including any and all necessary completed analyses, simulations, and test results. The final CDR must be submitted to and receive written approval of County prior to installation and implementation of the System.

6. **System functionality**

Provider must provide Software and Equipment to enable the System to provide appropriate parking controls for the Parking Facilities.

A. Key functional System requirements are as follows:

i. Include management of transient parking transactions.

ii. Process payments via Payment Card Industry ("PCI") approved terminals using a payment service provider approved by County who is certified by the PCI council as to compliance with PCI standards.

iii. Provide a P2PE validated payment solution.

iv. Process and manage vehicle and transaction counts as requested by County.

v. Include the ability to implement unblocked lists permitting the access of certain vehicles to the Parking Facilities.

vi. Include the ability to implement blocked lists to block certain vehicles from accessing the Parking Facilities.

vii. Include the ability to implement a pay-by phone payment solution as selected and approved by County.

viii. Interface with any County approved payment solution application, as stated in Section 2.C. of this SOW, Interfaces/Integration.

ix. Include robust reporting functions including cash flow yielding revenue analysis of the usage of the Parking Facilities as they relate to parking transactions and operations.

x. Be fully compliant with all applicable federal, state, and local security standards.

xi. Operate dependably within the environmental conditions indigenous to the Airport. Components located in a 24-hour climate-controlled office must be capable of normal performance in a business environment. Equipment must meet or exceed the specifications provided by Provider on October 11, 2022.

xii. Provide a fee calculation system, which must be capable of maintaining validation account numbers for the Parking Facilities while identifying active and/or inactive status.

xiii. Support the creation of a variety of validation codes.

xiv. Payments conducted within the System by Credit Card shall be PCI-DSS, Europay, Mastercard, and Visa (collectively referred to as "EMV") compliant. The payment system shall also stay compliant with future PCI-DSS changes, and Provider shall submit to County an updated Attestation of Compliance on an annual basis. Costs associated with changes to PCI-DSS compliance requirements specifically related to the System at the Airport shall be payable by County, after receipt of Provider's written request and County provides written approval. Credit card types accepted by PARCS shall include Visa, MasterCard, American Express, Discover, and all major E-wallet systems including Apple-Pay, and Google Wallet.

xv. Comply with County requirements that Credit Card readers read mag stripe products and integrate infrastructure for near field communication cards and EMV smart card with chip and pin technology.

xvi. Export all query results to multiple formats including, but not limited to, comma-separated value, Microsoft Excel©, and Adobe Acrobat (PDF).

xvii. Provide all detailed reports as described in Section 6.H of this SOW, System Reporting.

xviii. Provide remote management of entry/exit lane equipment including payment devices.

xix. Provide a parking reservation system ("Pre-Booking System") for all County sites.

xx. Provide a rewards system for frequent users at the Airport ("Loyalty System"), as agreed to by the Parties.

xxi. Provide a Test Environment and Production and Disaster Recovery Server Environments for testing of all configuration processes, patches, or updates to the System.

B. Entry Lane Functionality Description

Provider will design, configure, and install the System so that each entry lane provides the following functionality:

i. Customers will be granted entry through the use of a valid Parking Media.

ii. The Intercom System must provide customers the ability to communicate with the Parking Operations Office and for the Parking Operations Office to respond to the customer. The Parking Operations Office shall have the ability through the Intercom System to open the Barrier Gate.

iii. The Loop Detector must provide detection of vehicle presence essential to the Equipment operation and the Parking Facilities entry count totals. The Loop Detector must be fully self-tuning, have self-scanning vehicle detector sensors (arming and closing) installed at all entry lanes, and provide complete Parking Facilities entry count totals, regardless of the status of the Barrier Gate Arm. The Loop Detector must be integrated into the overall vehicle count control as part of the System and have sufficient speed and reliability to transmit accurate live data to the System.

iv. The Barrier Gate Arm must raise after a customer takes a ticket or presents a Parking Media for entry to the Parking Facilities, and lower once the vehicle has entered.

C. Exit Lane Functionality Description

Provider will design, configure, and install the System so that each exit lane provides the following functionality:

i. Customers must be permitted to exit by performing one (1) of the following actions:

a. Inserting an unpaid ticket and making payment at the applicable exit lane station with a Credit Card, printed QR Code, smartphone QR Code, or by a validation provided by the Parking Operations Office; or

b. Using any other valid Parking Media that has been first used at an entry lane.

ii. The Intercom System must provide customers the ability to communicate with the Parking Operations Office and for the Parking Operations Office to respond to the customer. The Parking Operations Office shall have the ability through the Intercom System to open the associated Barrier Gate.

iii. The Loop Detector must provide detection of vehicle presence essential to Equipment operation and Parking Facilities exit count totals. The Loop Detector must be fully self-tuning, self-scanning (arming and closing), installed at all exit lanes, and provide complete Parking Facilities exit count totals, regardless of the status of the Barrier Gate Arm. The In-Ground Loop Detector will be integrated into the overall vehicle count control as part of the System and will have sufficient speed and reliability to transmit accurate live data to the System.

iv. The Barrier Gate Arm must raise after a customer presents a valid Parking Media for exit at the exit station or completes the payment. The Barrier Gate Arm must lower once the vehicle has exited.

D. Fixed Lane License Plate Recognition Cameras Description

At Sites 1 and 5 - 9, Provider shall design, configure, install, and commission into operation a fixed lane LPR system ("LPR System"), which provides LPR cameras on all entry and exit lanes. The LPR System must provide the following functionality:

i. Maintain a license plate record for every vehicle that enters or exits the Parking Facilities;

ii. Record the license plate of the vehicle that enters or exits the Parking Facilities with a Parking Media against the respective transaction record;

iii. Recognize license plates on moving and stationary vehicles;

iv. Detect and recognize license plates of different states, fonts, and colors, including regular character and stacked character license plates;

v. Detect, recognize, and search for license plates in real-time and archived footage;

vi. Provide for automated matching of license plates against a watch list with real-time alerting;

vii. Provide tracking of vehicles across multiple Parking Facilities entry and exit lanes or across multiple Parking Facilities; and

viii. Provide for the storage of license plate records for a period of five (5) years.

E. Mobile License Plate Inventory

Provider will design, install, configure, and commission a Mobile License Plate Inventory ("MLPI") system ("MLPI System"). The MLPI System must provide the following functionality:

i. Provide LPR cameras mounted to County provided vehicles to capture license plates parked in the Parking Facilities. The MLPI data shall be used as a secondary look up for exit exception transactions to assist in the calculation of parking fees;

ii. Provide Equipment and Software modules to complete the overnight inventory process within a four (4) hour time window. This time window includes the inventory taking process, correction cycles, and generation of an updated current overnight inventory;

iii. The MLPI vehicle unit shall alert the parking operator of license plates that are not accurately read (below the agreed-upon confidence factor based on industry standards). The MLPI vehicle unit shall display the actual license plate image on the computer, show the license plate number captured by the camera, and allow the MLPI driver to input the correct license plate number into the computer;

iv. The MLPI computer shall upload the collected inventory data to the server each night;

v. MLPI computer synchronization shall be accomplished via a wireless connection;

vi. Record the beginning and ending dates/times for the inventory taking process for each unit and record on the daily event log each time that the uploading process begins;

vii. Allow for correction of mistakes made during inventory collection process. MLPI driver or MLPI personnel shall be able to delete any specific license plate entry;

viii. Provide changeable defaults for facility, section, and row. Inventory personnel shall not be required to enter facility, section, or row for each entry, but shall have the ability to change facility, section, and row defaults as appropriate during inventory process;

ix. Be route-specific but the MLPI System shall be easily modified and altered using a graphical user interface capability to reflect changed parking configurations; and

x. Detect, recognize, and search for license plates in real-time or archived footage.

F. Merchant Validation Feature

Provider will design, configure, and implement the System to provide a merchant validation feature, which will assist in performing the following tasks:

i. Print pre-paid parking validation label sheets on a color laser printer which can be distributed and applied to a customer's entry ticket;

ii. Process the pre-paid parking validation at the System's exit station according to County's programming preferences; and

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

G. Data Conversions

i. Provider must perform data conversions for all valid cardholder records from County's WebPARCS to the System and ensure the entire data set (or subset(s) as designated by County, if less than the entire data set) is fully and accurately converted.

ii. The data conversion must be performed by an import tool provided by the Provider using files generated from County's WebPARCs system. The format for data conversions will be determined after Provider has conducted the onsite analysis of County's current operations and during the CDR. Provider must test all data conversions to ensure completeness and accuracy of the converted data prior to County conducting Final Acceptance Testing.

iii. County will test the data conversions for accuracy at the Test Environment and during Final Acceptance Testing.

H. System Reporting

i. Provider must ensure the System provides real time reporting and a variety of canned reports that can integrate with the System and export to Excel, including, but not limited to, the following:

a. Analytical charts - Graphically summarizes statistical traffic and occupancy data by customer type.

b. Auditing reports - Reporting for all historical data of activity, duration, transactions, and revenue functions.

c. Company reports - Financial and revenue data about how companies and their employees use the parking facility.

d. Customer reports - Traffic usage data specific to customers plus financial and revenue information.

e. Duration reports - Reporting all historic data of entry and exit date and location information.

f. Entry and exit lane - Reporting for all functional and non-functional entry lanes and exit lanes and number of vehicles entering and exiting all lanes.

g. Occupancy and traffic reports - Statistical traffic and occupancy data including parking time counts, overflow area analysis, and demand level assessments.

h. Proximity Card and Courtesy Parking Card reports – Track and provide transaction information for employee access, usage, duration, and activity.

i. Revenue and transactions - Refined by facility, type of transaction, number of transactions, payment type, or event.

j. Revenue reports - Comprehensive financial and statistical data about the parking facility's revenue streams.

k. System event reports - Event log data on gate openings, garage station counters, and device alerts.

l. Ticket reports - Track and detail parking ticket usage to help protect a garage's revenue.

m. Ticket validation reports - Track and match parking ticket with the validation cost and duration.

n. Validation reports - Provide information into the operations of the validation programs that are in use.

o. Vehicle ID reports - Provide access to transaction logs and usage statistics.

i. Provider must ensure that the System provides detailed reporting on all accounting transactions, audit functions, and operations, including, but not limited to, the following information and reports:

a. Pre-programmed reports and customized ad-hoc reports, as requested by the Contract Administrator.

b. Automatically detect and report fault conditions through the management system. The System must perform a self-check on a real-time basis and provide notification in real-time for faulty conditions and equipment failure and maintenance.

c. Monitor and report status of all hardware, software, and communications links in real-time. Alerts must be definable and must be able to be sent to multiple devices designated by County (i.e., smartphones).

d. A robust alarm management system. Alarms with visual dashboard graphics and appropriate messages that notify County about all System and Equipment failures, and customer related issues must be provided and accessible on computer screens, laptops, tablets, and smart phones. County shall indicate which alarms require higher priority, and Provider must configure the alarms to County's preference.

e. Generate real-time alarms and status reports for maintenance needs, reporting by text messages, and/or e-mails in real-time to maintenance staff designated by County.

f. Track parking occupancy counts and display vacancy counts in the back-office software platform for the Parking Facilities, which are not installed with a Parking Guidance System. Vacancy counts must be displayed for the Parking Facilities with an installed Parking Guidance System through the existing parking count signage at the entrances to those facilities by the Parking Guidance System and in the back-office software platform of the Parking Guidance System.

g. Monthly Maintenance Reports in a County-approved format to designated personnel.

h. Document parking revenue and activity and generate revenue and activity reports.

i. Identify and produce reports that reflect public parking and employee parking separately.

j. Separate public parking data by category into transient and monthly/contract parking.

k. A detailed transaction report that can be accessed by a supervisor from a workstation to enable the examination of cashier transactions during and at the close of a cashier's shift.

l. All reports must query, filter, sort, transactions by date/time,

location, ticket identification, vehicle license plate number, field device unique identifier, parking fee, transaction type, validation type, or cashier, as may be applicable to the data captured for the particular transaction.

m. Capture, record, and report separately all exception transactions for the following use cases: unreadable, lost, previously used, or cancelled.

n. Provide Provider's standard reports including report descriptions, selectable data fields, and report layouts for all standard reports.

o. Provide a definition key for every report including a narrative description of what data each column and row represents and calculation formulas that define how all figures are obtained.

ii. Provider shall coordinate with County during the System design to address the specific reporting needs of County. The System shall allow grouping of reports by category to simplify choosing a report from a list. The System must provide reports that contain, at a minimum the following information:

a. Operating/cash book reporting.

b. Payment statistics.

c. Park check.

d. Value check settlements.

e. Time slot statistics.

f. Occupancy statistics.

g. Alarm statistics.

h. Credit card or courtesy card information.

i. Throughput statistics (including all transactions that are processed).

j. Manual pay stations shifts.

k. Midnight report.

l. Auditing.

m. Vehicle counts.

n. LPR.

o. Parking vouchers issued to personnel with a parking ticket for County business.

The System must generate the reports described in this section to allow County to review such reports within twenty-four (24) hours of County's request, have security protocols, and password protection to prevent unauthorized access and manipulation of data and reports, including individual transactions. The security measures must comply with all current PCI standards. All databases must be secured from unauthorized entry and tampering from either within or outside the System. The System must generate alerts of unauthorized access to the System.

County must have access to the raw data gathered by Provider to be extracted by County at any time for County's business purposes.

Provider must ensure the delivery of an export process to transfer raw data and/or complete a daily database export to allow County to generate executive reports.

All reports must be available online and on demand for County staff who have proper password access. The System must support the scheduling of reports to automatically run at a desired time or on a desired schedule. Users must be able to designate e-mail recipients for these reports to whom the reports will automatically be emailed. Only users with appropriate privileges shall schedule reports or view scheduled reports.

7. **Managerial Approach**

A. Project Personnel

Provider will ensure that the persons responsible for Provider's performance of the Services required pursuant to this SOW and, to the extent applicable, identified below (collectively "Key Personnel") are appropriately trained and experienced and have adequate time and resources to perform in accordance with the terms of this SOW. If Provider seeks or is required to make any change to the composition of the Key Personnel, Provider will provide County with thirty (30) days' advance notice regarding such changes and the management plan associated with such changes. If County reasonably requests in writing a replacement in Key Personnel, Provider shall use best efforts to promptly affect a suitable replacement no longer than thirty (30) days after such notice. County shall not be responsible for any additional costs associated with a change in Key Personnel.

Key Personnel shall be as follows:

Name	Title	Contact Tel.	Contact Email
John Curtiss	President and CEO	281-798-1483	john.curtiss@designa.com
Paul McIlvride	Program Manager	347-852-5550	paul.mcilvride@designa.com

Name	Title	Contact Tel.	Contact Email
Kayser Nazmee	Project Manager	832-986-6914	kayser.nazmee@designa.com
Brian McCabe	Installation Manager	404-578-4997	brian.mccabe@designa.com
Conn Townzen	Solution Architect	281-620-2428	conn.townzen@designa.com

Each of the Key Personnel will be on site during all Services activities for which they are directly responsible, providing coverage during Business hours, unless otherwise agreed in advance by the Contract Administrator.

The on-site resource personnel/technician will be on site during Business hours, unless otherwise agreed in advance by the Contract Administrator.

Project Manager (Day-to-day point of contact)
Kayser Nazmee is the project manager for Provider and will direct the installation and technical team. The project manager will be responsible for the entire project from the Effective Date through the completion of Final Acceptance. The project manager will report directly to the Contract Administrator.

Executive Level (Executive level single point of contact)
John Curtiss is the senior executive level and single point of contact for higher-level communications for Provider.

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

B. Reporting Schedule

i. Project Kickoff Meeting

After the Effective Date and the issuance of the Notice to Proceed, Provider and County will participate in an initial onsite kickoff meeting at the commencement of the Project. The kickoff meeting will be attended by the Provider's Program Manager, Project Manager, and County's Contract Administrator and Project Manager, and other individuals requested by the respective Project Managers. Provider must keep and provide County with the meeting minutes.

ii. Project Status Meeting

After the project kick-off meeting, Provider will coordinate and conduct remote status meetings on a weekly basis, or as otherwise agreed to between the Parties. These weekly meetings will continue up until one (1) week before the

commencement of Equipment installation. Provider must keep and provide County with the meeting minutes.

After Equipment installation commences, Provider will coordinate and conduct remote status meetings on a weekly basis, or as otherwise agreed to between the Parties. These meetings will continue until County issues written notice of Final Acceptance to Provider. Provider must keep and provide County with the meeting minutes.

iii. Project Status Reports

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

8. **Installation**

A. Equipment Removal and Disposal

i. As part of the Services, Provider will remove all existing equipment that is no longer usable or compatible with the System.

ii. The removal and disposal of the equipment will follow a process to be approved by County. Equipment will be removed at Sites 1-12, one (1) lane at a time, unless otherwise requested by County.

iii. Provider must minimize lane closures during the removal of old equipment to ensure minimal impact to Airport operations.

iv. During equipment removal, Provider will ensure the two (2) systems run simultaneously (i.e., WebPARCS and the System) following the processes reflected in the Transition Plan to minimize lane closure customer service impacts during removal of the old equipment.

B. Communications Equipment and Server Installation

i. As part of the Services, all communications equipment must be replaced, including Active and Passive Network Equipment, if requested by County.

ii. The permanent location of all required servers is Site 3.

iii. Provider will build and provide a communication network utilizing the current fiber infrastructure available at Sites 1- 12.

iv. Provider will logically segment the servers to ensure there is no connection to County network.

v. Provider will provide access to the servers to persons designated by County.

vi. As part of Provider's onsite analysis and CDR, Provider must identify user roles, the corresponding level of server access required per role, and Provider must, as part of its final configuration of the System, incorporate such roles and access levels.

vii. Provider is solely responsible for the security of the System, including providing and applying patches and updates, as may be required, to all equipment. Any patches, updates, or changes to the System must be approved in writing by the Contract Administrator prior to application or implementation.

viii. County shall not install, use, or operate the Products on servers other than those provided as part of the System by Provider or in any additional environments or configurations without written approval by Provider.

C. Project Activities and Phases

i. The project plan (which is a required written deliverable by Provider) must contain all project activities and phasing necessary to complete the project, including, but not limited to, the incorporation of environmental conditions, scheduling availability, and supply chain delays.

ii. Provider must complete the project, and achievement of Final Acceptance must occur, within twenty-four (24) months after the Effective Date.

9. **Testing**

A. Prior to FAT (hereinafter defined), the Parties shall develop a punch list of items that are incomplete, unresolved, or otherwise unsatisfactory to County. County will review and determine satisfactory resolution of each punch list item and provide Provider with written confirmation when all punch list items are resolved by Provider.

B. Final Acceptance Testing ("FAT")

i. FAT will be conducted jointly by County and Provider and shall test each Parking Facility's performance independently and as part of the entire System.

ii. FAT reviews the operation and status of equipment and system reports of the Parking Facilities.

iii. The System must run for thirty (30) days measured from the initial start-up date and continuing for thirty (30) consecutive twenty-four (24) hour periods with no Critical or Severe issues as defined in **Exhibit D**.

iv. FAT shall be performed for the System for each Parking Facility only after all lane tests in the Parking Facilities have been successfully completed.

v. Only routine maintenance procedures, as defined in Provider's Preventative Maintenance Manual and according to industry standards, shall be permitted during FAT. All other maintenance procedures shall be approved in writing by County before they are performed; the failure to obtain prior written approval from County shall constitute a failure of FAT, resulting in a mandatory restart.

vi. Provider must submit necessary documentation to demonstrate the System as built is consistent with and reflects the County's approved CDR. Required documentation and all hands-on use of the System shall demonstrate to County that the System meets one hundred percent (100%) of the requirements of this SOW.

vii. Provider shall submit FAT criteria that includes the requirements stated in this section and the Deliverables section. FAT scripts are intended to outline procedures for monitoring the overall performance of the System and include test procedures for individual lanes or components.

viii. The performance criteria for successful completion of FAT shall include:

a. The System must be operationally available one hundred percent (100%) of the time during the thirty (30) day test period; and

b. If any single component fails during the thirty (30) day test, testing must halt and start over upon replacement or correction of the problem.

ix. The Contract Administrator will provide written Final Acceptance upon successful completion of the following FAT criteria and any other criteria required by the Contract Administrator:

No.	Deliverable	Final Acceptance Test Criteria	Pass/Fail
1.	Server and database function	County to confirm the server and database functions in accordance with System Functionality.	
2.	Validation	County to confirm the validation, QR Code, and barcode scanner functions properly.	
3.	Payment tenders	County to confirm the payment tenders are accepted.	
4.	System reporting functions	County to confirm the System provides accurate System reporting.	
5.	Proximity Card readers	County to confirm the proximity reader functions properly.	
6.	Loop Detector(s)	County to confirm the Loop Detector(s) functions	

No.	Deliverable	Final Acceptance Test Criteria	Pass/Fail
		properly.	
7.	Double stroke red X/green arrow sign	County to confirm the red X green arrow sign functions properly.	
8.	Barrier gate arms	County to confirm the Barrier Gate Arms function properly.	
9.	Barcodes, QR Codes, scanner functionality	County to confirm the Equipment successfully accepts and processes barcodes, QR Codes, and scanner scans.	
10.	Intercom System	County to confirm the Intercom System functions properly.	
11.	Verify ability to integrate with third-party pay by phone vendor	County to confirm ability to integrate with third-party pay by phone application in the future based on P2PE Certification.	
12.	License Plate Recognition and inventory system	County to confirm the License Plate Recognition and Inventory system functions and reports accurate data.	
13.	Data Conversions	County to confirm data converted from WebPARCS to the System during the installation process. Data must be historically accurate and complete.	
14.	SunPass	County to confirm SunPass installation is operational and accurately reporting.	
15.	Preventative Maintenance Manual	Twenty (20) business days before the commencement of operations, Provider will submit to County for approval a Preventative Maintenance Manual.	
16.	P2PE Certification	Prior to commencement of lane testing, Provider will provide an updated P2PE Certification.	
17.	Test Environment	County to confirm the Test Environment functions properly.	
18.	Pre-Booking System	County to confirm the Pre-Booking System functions properly.	
19.	Production and Disaster Recovery Server Environments	County to confirm the Production and Disaster Recovery Server Environments functions properly.	

10. **Training**

A. Provider must provide comprehensive training for County staff and/or third-party personnel identified by County prior to any Equipment being placed into revenue service.

B. Training must be in accordance with the training plan that has been reviewed and

approved in writing by County ("Approved Training Plan").

C. Following Final Acceptance, Provider must provide onsite training sessions for County staff and/or third-party personnel identified by County, consisting of a minimum of ten (10) training hours annually. Each class will run a minimum of two (2) hours. Training hours shall be allocated as desired by County and will adhere to the Approved Training Plan. Each training session will be conducted at a designated County location between Monday through Friday during the hours of 8:30 am to 5:00 pm, or after hours, as requested by County. Each training session will be tailored to specific tasks to provide training using the Test Environment and/or fully functioning Equipment.

D. Provider must provide training attendees with a hard copy of all training materials. Provider must provide with an electronic and hard copy version of all training materials.

E. Until Final Acceptance, Provider must provide continuous training on an as-needed basis at no additional cost to County.

11. **Software and Maintenance**

A. Provider must provide Support and Maintenance services to County for the Software and Equipment in accordance with **Exhibit D**.

B. On the date that one (1) complete lane of all required Equipment is installed by Provider, approved in writing by County, and placed In Revenue Service at the Airport, Provider must provide County with one (1) full-time dedicated on-site resource personnel at the Airport to provide services to County during regular business hours for the Term. County may request, with at least sixty (60) days' notice by the Director of Purchasing, that the number of on-site resource personnel(s) be modified. In such event, the rates established in **Exhibit B** shall apply on a pro rata basis. The on-site resource personnel will serve as the primary responder to any issues with the Software or Equipment during Business hours of the Airport. There shall be no additional charge to County, other than the Support and Maintenance fees in **Exhibit B**, for any services provided by the on-site resource personnel during Business hours, including, but not limited to, repairing damaged Equipment and replacing Equipment that is under warranty, excluding any additional parts needed that are not under warranty.

C. Within sixty (60) days after the Effective Date and periodically thereafter, Provider must review and provide to the Contract Administrator any proposed updates or other modifications to the Software and Equipment included under Attachment 1 and Attachment 2 of this SOW to ensure the Software and Equipment being maintained by the Provider under this Agreement remains accurately reflected. Upon written approval by the Contract Administrator, the updated or modified Software and Equipment schedule will be deemed incorporated in this Agreement.

12. **Written Deliverables**

No.		
1	Project Plan	Within fifteen (15) business days after the NTP, Provider will submit an initial project plan, using Microsoft® Project, or other project management software approved by the Aviation Department. The project plan shall outline tasks for all services for each site. The project plan shall include at a minimum: 1. Timeframe for installation of any new network infrastructure and testing. 2. Timeframe for installation of new data servers and testing. 3. Timeframe for installation of new Credit Card processing and connection to clearing house with testing. 4. Timeframe for coordination for the removal of existing Equipment. 5. Timeframe for installation of Equipment. 6. Timeframe for integration and development of other Services required per this SOW.
2	Minutes of Project Kick-off Meeting	Within three (3) business days after the Project kick-off meeting, Provider will submit minutes of the meeting to County.
3	Minutes of Project Status Meetings	Within three (3) business days after each weekly Project status meetings, Provider will submit minutes of the meeting to County.
4	Project Status	On the first business day of each month, Provider will submit a Project status report to County. The Report will provide an update of what has been installed with a two (2) week look ahead of Project activities.
5	CDR Review Plan	Within twenty (20) business days after the NTP, Provider shall submit a CDR review plan that includes, but is not limited to, the time, place, and length of the review, review format, overall description of review, goals of the review, agenda items and topics, recommended participants, and the role/responsibilities of County in the review.
6	System Description	Within twenty (20) business days after the completion of the CDR period, Provider shall submit a detailed description of the System and its components to County.
7	Solution Architecture	Within twenty (20) business days after the completion of the CDR period, Provider shall submit a detailed description of the

		System server architecture, network logical and physical, server and network hardware requirements and network port density and bandwidth requirements to County.
8	Transition Plan	Within twenty (20) business days after the completion of the CDR period, Provider shall submit a detailed transition plan which will include a lane by lane and deployment schedule to be approved by County based on the priority of County's parking needs and operation as determined during the CDR period. The transition plan will address installation procedures to ensure operational disruptions during equipment replacement are kept to a minimum. The transition plan will be used to: 1. Minimize lane closures during installation of new equipment. 2. Prepare a work plan to schedule and minimize installation work around peak season hours of operation, holidays, and weekends and to schedule around airline flight banks. 3. Focus equipment installation activities to occur during non-business hours when possible. 4. Ensure the implementation of all electrical and communication infrastructure before work in entry or exit lanes occurs, where possible. 5. Phase equipment implementation so that one (1) entry is installed with one (1) exit.
9	Spare Parts Price List	Prior to commencement of FAT, Provider will provide an itemized spare parts price list to County.
10	P2PE Certification	Prior to commencement of lane testing, Provider will provide an updated P2PE Certification to County.
11	System and Equipment Acceptance Test Plan	Fifteen (15) business days before the commencement of lane testing, Provider will submit a FAT plan to County for prior written approval.
12	Training Plan	Twenty (20) business days before the commencement of any training, Provider will submit a training plan to County for prior written approval.
13	Preventative Maintenance Manual	Twenty (20) business days before the commencement of operations, Provider will submit a Preventative Maintenance Manual to County for prior written approval.

13. **Transition & Disentanglement Services, Optional Services, Additional Software/Licenses:**

A. Transition & Disentanglement Services

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

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

B. Additional Software, Equipment, and Services

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

i. Additional training sessions (for advanced training topics).

ii. Additional sites, including new parking garages, additional surface lots, or valet stations if needed. Such additional sites must be readily able to be added to the configuration of the System.

iii. Additional products, including, but not limited to, software licenses or subscriptions, firmware, equipment, modules, and/or support and maintenance.

iv. Professional services (such as consulting, professional services, or other hourly services as requested by County).

v. County-specific project requirements, documentation, and deliverables that are not specifically identified in this **Exhibit A** and are not directly associated with tasks required for Provider resources to deploy the System.

vi. Maintenance and support services associated with the Park Assist Parking Guidance System installed at Sites 5, 6, and 7.

vii. The System to be reconfigured to allow for a ticket-less and gate-less method of entry.

(THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK.)

ATTACHMENT 1 – SOFTWARE

1. Software is licensed in accordance with Section 3.2.1 of the Agreement, Software License and subject to the following:

A. Server access is limited to ten (10) concurrent users for administration.

B. Application users are unlimited through the provided ParkingHQ Control Center software.

2. Subscriptions are provided in accordance with Section 3.2.2 Subscription Rights of the Agreement, and subject to the following:

A. Server access is limited to ten (10) concurrent users for administration.

B. Application users are unlimited through the provided ParkingHQ Control Center software.

3. Additional user licenses may be purchased as follows:

A. Server access for administration may be purchased at the then current published rates for Microsoft Client Access Licenses as may be advertised from time to time.

B. User access to the WinOperate application for PARCS configuration may be purchased for One Thousand Six Hundred Seventy Dollars ($1,670.00) per additional user.

Software and Subscriptions:

Software Suite, Version & Module	Quantity	Type of License	Purpose, Functionality & Expected Operation of Software
PARCS Application Software/ Version 23.3	3	Enterprise	PARCS core application.
LPR and MLPI Software Interface/ Version 23.3	3	Enterprise	Interface to LPR Cameras.
Online Booking System Interface/ Version 23.3	3	Enterprise	API for 3rd party Pre-booking.
Parking HQ Control Center/ Version 23.3	3	Enterprise	PARCS User interface.
WinOperate/ Version 23.3	3	Enterprise	PARCS configuration.
ParkingHQ Control Parker/ Version 23.3	3	Enterprise	Employee of other Contract Parker Management.

Software Suite, Version & Module	Quantity	Type of License	Purpose, Functionality & Expected Operation of Software
ParkingHQ Loyalty/ Version 23.3	3	Enterprise	Loyalty System.
ParkingHQ Pre-booking/ Version 23.3	3	Enterprise	Pre-Booking System.
Valet Software/ Version 23.3	1	Enterprise	Valet operations.
On-Line Validation System Software/ Version 23.3	3	Enterprise	On-line Validations.
Server operating system. Windows Server® 2019 Datacenter, 16CORE, FI, No MED, UnLTD VMs, NO CALs, Multi Language Server	3	Datacenter	Production, Disaster and Test Environments. Server operating system
Server Database application MS SLC+ SQLSVRSTDCORE 2019. Microsoft SQL 2019 Standard Core 2019	3	Standard Core	Production, Disaster Recovery and Test Environments Database application.
Server Database application. Microsoft SQL 2019 Standard License	3	Standard	Production, Disaster Recovery and Test Environments Database application. Microsoft SQL Server 2019 Standard license - 1 license
Client Access Licenses	3	User	Server user access. 5-pack of Windows Server 2019 Remote Desktop Services, Device
SunPass integration	1	3rd party integration	Integration to SunPass. To be integrated in the Test Environment

Third-Party Software provided by Provider	Quantity & Type of License	Purpose, Functionality & Expected Operation of Software
Commend Virtuosis Intercom Software	3 x Enterprise	Application software for the operation of the Intercom system
ADVAM Credit Card Payment Processing System	1 x Enterprise	CLOUD hosted application for the processing of all Credit Card transactions

ATTACHMENT 2 – EQUIPMENT SCHEDULE

County shall provide the following Equipment:

Quantity	Equipment	Comments
Parking Facilities		
GARAGE ENTRIES		
Entry Lane Equipment**/ENT 01**		
1	SunPass Reader	Reuse existing
1	SunPass Sign	Reuse existing
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Entry Lane Equipment**/ ENT 02**		
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Entry Lane Equipment**/ ENT 03**		
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Entry Lane Equipment**/ ENT 06**		
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Entry Lane Equipment**/ ENT 08**		
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Entry Lane Equipment**/ ENT 09**		
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware

Quantity	Equipment	Comments
Parking Facilities – (Continued)		
GARAGE ENTRIES – (Continued)		
Entry Lane Equipment **/ ENT 10**		
1	SunPass Reader	Reuse existing
1	SunPass Sign	Reuse existing
1	Proximity Reader – Allow Valet entry	Reuse existing
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Entry Lane Equipment**/ ENT 11**		
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Entry Lane Equipment **/ ENT 12**		
1	SunPass Reader	Reuse existing
1	SunPass Sign	Reuse existing
Entry Lane Equipment **/ ENT 13**		
1	SunPass Reader	Reuse existing
1	SunPass Sign	Reuse existing
Entry Lane Equipment **/ ENT 14**		
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
MAIN EXIT PLAZA		
Exit Lane Equipment/ **EXIT 01**		
1	Proximity Reader – Allow Valet vehicles to exit	Reuse existing
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Exit Lane Equipment/ **EXIT 02**		
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware

Quantity	Equipment	Comments
Parking Facilities – (Continued)		
MAIN EXIT PLAZA – (Continued)		
Exit Lane Equipment/ **EXIT 03**		
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Exit Lane Equipment/ **EXIT 04**		
1	SunPass Reader	Reuse existing
1	SunPass Sign	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Exit Lane Equipment/ **EXIT 05**		
1	SunPass Reader	Reuse existing
1	SunPass Sign	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Exit Lane Equipment/ **EXIT 06**		
1	SunPass Reader	Reuse existing
1	SunPass Sign	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Exit Lane Equipment/ **EXIT 07**		
1	SunPass Reader	Reuse existing
1	SunPass Sign	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Exit Lane Equipment/ **EXIT 08**		
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Exit Lane Equipment/ **EXIT 09**		
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Exit Lane Equipment/ **EXIT 10**		
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware

Quantity	Equipment	Comments
Parking Facilities – (Continued)		
MAIN EXIT PLAZA – (Continued)		
Exit Lane Equipment/ **EXIT 11**		
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Exit Lane Equipment/ **EXIT 12**		
1	SunPass Reader	Reuse existing
1	SunPass Sign	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
CYPRESS GARAGE EXITS		
Exit Lane Equipment/ **LEVEL 6 EXPRESS EXIT**		
1	SunPass Reader	Reuse existing
1	SunPass Sign	Reuse existing
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Exit Lane Equipment/ **LEVEL 6 BOOTH**		
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Exit Lane Equipment/ **LEVEL 7 EXPRESS EXIT**		
1	SunPass Reader	Reuse existing
1	SunPass Sign	Reuse existing
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Exit Lane Equipment/ **LEVEL 7 BOOTH**		
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Exit Lane Equipment/ **LEVEL 8 EXPRESS EXIT**		
1	SunPass Reader	Reuse existing
1	SunPass Sign	Reuse existing
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware

Quantity	Equipment	Comments
Parking Facilities – (Continued)		
CYPRESS GARAGE EXITS – (Continued)		
Exit Lane Equipment/ **LEVEL 8 BOOTH**		
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Exit Lane Equipment/ **LEVEL 9 EXPRESS EXIT**		
1	SunPass Reader	Reuse existing
1	SunPass Sign	Reuse existing
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Exit Lane Equipment/ **LEVEL 9 BOOTH**		
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
EMPLOYEE LOT ENTRIES		
Entry lane Equipment/ **ENT 26**		
1	Proximity Reader	Reuse existing
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Entry lane Equipment/ **ENT 27**		
1	Proximity Reader	Reuse existing
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Entry lane Equipment/ **ENT 30**		
1	Proximity Reader	Reuse existing
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware

Quantity	Equipment	Comments
Parking Facilities – (Continued)		
EMPLOYEE LOT ENTRIES – (Continued)		
Entry lane Equipment/ **ENT 31**		
1	Proximity Reader	Reuse existing
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Entry lane Equipment/ **ENT 32**		
1	Proximity Reader	Reuse existing
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
BUS ENTRIES		
Entry lane Equipment/ **ENT28**		
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Entry lane Equipment/ **ENT29**		
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Entry lane Equipment/ **ENT33**		
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
EMPLOYEE LOT EXITS		
Exit Lane Equipment/ **Exit 68**		
1	Proximity Reader	Reuse existing
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Exit Lane Equipment/ **Exit 69**		
1	Proximity Reader	Reuse existing
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware

Quantity	Equipment	Comments
Parking Facilities – (Continued)		
EMPLOYEE LOT EXITS – (Continued)		
Exit Lane Equipment/ **Exit 70**		
1	Proximity Reader	Reuse existing
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Exit Lane Equipment/ **Exit 72**		
1	Proximity Reader	Reuse existing
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Exit Lane Equipment/ **Exit 73**		
1	Proximity Reader	Reuse existing
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Exit Lane Equipment/ **Exit 74**		
1	Proximity Reader	Reuse existing
1	UPS	Reuse existing
1	Barrier Gate	Reuse existing with modification to controller for DESIGNA firmware
Valet Operations		
Valet Equipment/ **Terminal 1**		
-	Valet handheld	Valet units to be provided by AVPM
Valet Equipment/ **Terminal 2**		
-	Valet handheld	No Valet in this Terminal
Valet Equipment/ **Terminal 3**		
-	Valet handheld	No Valet in this Terminal
Valet Equipment/ **Terminal 4**		
-	Valet handheld	Valet units to be provided by AVPM

Provider shall provide the following Equipment:

Quantity	Equipment	Model No.	Comments
Centralized PARCS Components			
PRODUCTION ENVIRONMENT			
1	PARCS Application Server	R7515	Dell PowerEdge Server Motherboard, with 2 x 1Gb Onboard LOM (BCM5720)MLK2. Hyper-V cluster for the PARCS Production environment
1	KVM Console	B020-U08-19-K	Tripp Lite 8-Port Console KVM Switch w/ 19" LCD & 8 PS2/USB Combo Cables
1	UPS	DLRT5KRMXLT	Dell SmartUPS 5000VA 208V - Rack/Tower
1	Server Rack rails	09D83	Dell Ready Rails 2U Static Rails for 2/4-Post Racks and ReadyRails Sliding Rails Without Cable Management Arm, CK
DISASTER RECOVERY ENVIRONMENT			
1	PARCS Application Server	R7515	Dell PowerEdge R7515 Server Motherboard, with 2 x 1Gb Onboard LOM (BCM5720)MLK2. Hyper-V cluster for the PARCS Production environment
1	KVM Console	B020-U08-19-K	Tripp Lite 8-Port Console KVM Switch w/ 19" LCD & 8 PS2/USB Combo Cables
1	UPS	DLRT5KRMXLT	Dell SmartUPS 5000VA 208V - Rack/Tower
1	Server Rack rails	09D83	Dell Ready Rails 2U Static Rails for 2/4-Post Racks and ReadyRails Sliding Rails Without Cable Management Arm, CK
1	Intercom Server	S3	Commend Server

Quantity	Equipment	Model No.	Comments
Parking Operations Office			
1	PARCS Workstation	Dell 5400 All-in-one Optiplex	As requested, Supervisor's Office (3), Manager's Office (2), Audit Office (2), Assistant Manager's Office (1) and Employee Lot (2)
1	Central Cashier Terminal	POS600	Parking Management Office
3	Intercom Base Stations ID5	ID5	Parking Management Office

Quantity	Equipment	Model No.	Comments
Parking Facilities			
GARAGE ENTRIES			
Entry Lane Equipment/ **ENT 01**			
1	Ticket Dispenser	Connect Lane 600 in Full	New including basic device, Pinhole Camera, Intercom, QR code reader, and Contact and Contactless Credit Card Reader
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Entry Lane Equipment/ **ENT 02**			
1	Ticket Dispenser	Connect Lane 600 in Full	New including basic device, Pinhole Camera, Intercom, QR code reader, and Contact and Contactless Credit Card Reader
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Entry Lane Equipment / **ENT 03**			
1	Ticket Dispenser	Connect Lane 600 in Full	New including basic device, Pinhole Camera, Intercom, QR code reader, and Contact and Contactless Credit Card Reader
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New

Quantity	Equipment	Model No.	Comments
Parking Facilities – (Continued)			
GARAGE ENTRIES – (Continued)			
Entry Lane Equipment/ **ENT 06**			
1	Ticket Dispenser	Connect Lane 600 in Full	New including basic device, Pinhole Camera, Intercom, QR code reader, and Contact and Contactless Credit Card Reader
1	LPR Camera 1	Nanopak	New

Quantity	Equipment	Model No.	Comments
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Entry Lane Equipment/ **ENT 08**			
1	Ticket Dispenser	Connect Lane 600 in Full	New including basic device, Pinhole Camera, Intercom, QR code reader, and Contact and Contactless Credit Card Reader
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Entry Lane Equipment/ **ENT 09**			
1	Ticket Dispenser	Connect Lane 600 in Full	New including basic device, Pinhole Camera, Intercom, QR code reader, and Contact and Contactless Credit Card Reader
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Entry Lane Equipment / **ENT 10**			
1	Ticket Dispenser	Connect Lane 600 in Full	New including basic device, Pinhole Camera, Intercom, QR code reader, and Contact and Contactless Credit Card Reader
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New

Quantity	Equipment	Model No.	Comments
Parking Facilities – (Continued)			
GARAGE ENTRIES – (Continued)			
Entry Lane Equipment / **ENT 11**			
1	Ticket Dispenser	Connect Lane 600 in Full	New including basic device, Pinhole Camera, Intercom, QR code reader, and Contact and Contactless Credit Card

Quantity	Equipment	Model No.	Comments
			Reader
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Entry Lane Equipment / **ENT 12**			
1	Ticket Dispenser	Connect Lane 600 in Full	New including basic device, Pinhole Camera, Intercom, QR code reader, and Contact and Contactless Credit Card Reader
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Entry Lane Equipment / **ENT 13**			
1	Ticket Dispenser	Connect Lane 600 in Full	New including basic device, Pinhole Camera, Intercom, QR code reader, and Contact and Contactless Credit Card Reader
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Entry Lane Equipment **/ ENT 14**			
1	Ticket Dispenser	Connect Lane 600 in Full	New including basic device, Pinhole Camera, Intercom, QR code reader, and Contact and Contactless Credit Card Reader
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New

Quantity	Equipment	Model No.	Comments
Parking Facilities – (Continued)			
GARAGE ENTRIES – (Continued)			
MAIN EXIT PLAZA			
Exit Lane Equipment/ ***EXIT 01***			
1	Exit Ticket Reader -	Connect Lane 600 Slim Out	New including basic device, Pinhole Camera, Intercom, QR code reader, Contact and Contactless Credit Card Reader and Receipt Printer
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Exit Lane Equipment/ ***EXIT 02***			
1	Exit Ticket Reader	Connect Lane 600 Slim Out	New including basic device, Pinhole Camera, Intercom, QR code reader, Contact and Contactless Credit Card Reader and Receipt Printer
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
1	Cashier Equipment	Connect POS600	New including Cashier Workstation, 17” TFT monitor, keyboard, QR code reader, Contact and Contactless Credit Card Reader, Receipt Printer, Customer Fee Display, Cash Drawer and Intercom Base Station

Quantity	Equipment	Model No.	Comments
Parking Facilities – (Continued)			
MAIN EXIT PLAZA – (Continued)			
Exit Lane Equipment/ ***EXIT 03***			
1	Exit Ticket Reader	Connect Lane 600 Slim Out	New including basic device, Pinhole Camera, Intercom, QR code reader, Contact and Contactless Credit Card Reader and Receipt Printer
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New

Quantity	Equipment	Model No.	Comments
1	Closing loop	DESIGNA N loop	New
1	Cashier Equipment	Connect POS600	New including Cashier Workstation, 17" TFT monitor, keyboard, QR code reader, Contact and Contactless Credit Card Reader, Receipt Printer, Customer Fee Display, Cash Drawer and Intercom Base Station
Exit Lane Equipment/ ***EXIT 04***			
1	Exit Ticket Reader	Connect Lane 600 Slim Out	New including basic device, Pinhole Camera, Intercom, QR code reader, Contact and Contactless Credit Card Reader and Receipt Printer
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Exit Lane Equipment/ ***EXIT 05***			
1	Exit Ticket Reader	Connect Lane 600 Out Full	New including basic device, Pinhole Camera, Intercom, QR code reader, Contact and Contactless Credit Card Reader and Receipt Printer
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New

Quantity	Equipment	Model No.	Comments
Parking Facilities – (Continued)			
MAIN EXIT PLAZA – (Continued)			
Exit Lane Equipment/ ***EXIT 06***			
1	Exit Ticket Reader	Connect Lane 600 Slim Out	New including basic device, Pinhole Camera, Intercom, QR code reader, Contact and Contactless Credit Card Reader and Receipt Printer
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Exit Lane Equipment/ ***EXIT 07***			
1	Exit Ticket Reader	Connect Lane 600 Slim Out	New including basic device, Pinhole Camera, Intercom, QR code reader, Contact and Contactless Credit Card Reader and Receipt Printer
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Exit Lane Equipment/ ***EXIT 08***			
1	Exit Ticket Reader	Connect Lane 600 Slim Out	New including basic device, Pinhole Camera, Intercom, QR code reader, Contact and Contactless Credit Card Reader and Receipt Printer
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Exit Lane Equipment/ ***EXIT 09***			
1	Exit Ticket Reader	Connect Lane 600 Slim Out	New including basic device, Pinhole Camera, Intercom, QR code reader, Contact and Contactless Credit Card Reader and Receipt Printer
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New

1	Cashier Equipment	Connect POS600	New including Cashier Workstation, 17" TFT monitor, keyboard, QR code reader, Contact and Contactless Credit Card Reader, Receipt Printer, Customer Fee Display, Cash Drawer and Intercom Base Station

Quantity	Equipment	Model No.	Comments
Parking Facilities – (Continued)			
MAIN EXIT PLAZA – (Continued)			
Exit Lane Equipment/ ***EXIT 10***			
1	Exit Ticket Reader	Connect Lane 600 Slim Out	New including basic device, Pinhole Camera, Intercom, QR code reader, Contact and Contactless Credit Card Reader and Receipt Printer
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Exit Lane Equipment/ ***EXIT 11***			
1	Exit Ticket Reader	Connect Lane 600 Slim Out	New including basic device, Pinhole Camera, Intercom, QR code reader, Contact and Contactless Credit Card Reader and Receipt Printer
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Exit Lane Equipment/ ***EXIT 12***			
1	Exit Ticket Reader	Connect Lane 600 Slim Out	New including basic device, Pinhole Camera, Intercom, QR code reader, Contact and Contactless Credit Card Reader and Receipt Printer
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New

Quantity	Equipment	Model No.	Comments
Parking Facilities – (Continued)			
CYPRESS GARAGE EXITS			
Exit Lane Equipment/ **LEVEL 6 EXPRESS EXIT**			
1	Exit Ticket Reader	Connect Lane 600 Slim Out	New including basic device, Pinhole Camera, Intercom, QR code reader, Contact and Contactless Credit Card Reader and Receipt Printer
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Exit Lane Equipment/ **LEVEL 6 BOOTH EXIT**			
1	Exit Ticket Reader	Connect Lane 600 Slim Out	New including basic device, Pinhole Camera, Intercom, QR code reader, Contact and Contactless Credit Card Reader and Receipt Printer
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Exit Lane Equipment/ **LEVEL 7 EXPRESS EXIT**			
1	Exit Ticket Reader	Connect Lane 600 Slim Out	New including basic device, Pinhole Camera, Intercom, QR code reader, Contact and Contactless Credit Card Reader and Receipt Printer
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New

Quantity	Equipment	Model No.	Comments
Parking Facilities – (Continued)			
CYPRESS GARAGE EXITS – (Continued)			
Exit Lane Equipment/ **LEVEL 7 BOOTH EXIT**			
1	Exit Ticket Reader	Connect Lane 600 Slim Out	New including basic device, Pinhole Camera, Intercom, QR code reader, Contact and Contactless Credit Card Reader and Receipt Printer
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Exit Lane Equipment/ **LEVEL 8 EXPRESS EXIT**			
1	Exit Ticket Reader	Connect Lane 600 Slim Out	New including basic device, Pinhole Camera, Intercom, QR code reader, Contact and Contactless Credit Card

Quantity	Equipment	Model No.	Comments
			Reader and Receipt Printer
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Exit Lane Equipment/ **LEVEL 8 BOOTH EXIT**			
1	Exit Ticket Reader	Connect Lane 600 Slim Out	New including basic device, Pinhole Camera, Intercom, QR code reader, Contact and Contactless Credit Card Reader and Receipt Printer
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Exit Lane Equipment/ **LEVEL 9 EXPRESS EXIT**			
1	Exit Ticket Reader	Connect Lane 600 Slim Out	New including basic device, Pinhole Camera, Intercom, QR code reader, Contact and Contactless Credit Card Reader and Receipt Printer
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Parking Facilities – (Continued)			
CYPRESS GARAGE EXITS – (Continued)			
Exit Lane Equipment/ **LEVEL 9 BOOTH EXIT**			
1	Exit Ticket Reader	Connect Lane 600 Slim Out	New including basic device, Pinhole Camera, Intercom, QR code reader, Contact and Contactless Credit Card Reader and Receipt Printer
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Quantity	**Equipment**	**Model No.**	**Comments**
EMPLOYEE LOT ENTRIES			
Entry Lane Equipment/ **ENT26**			
1	Card Reader	Connect Lane 600 Lite In	For logic control of the HID Proximity Reader. Includes pedestal with Intercom
1	LPR Camera 1	Nanopak	New including Camera and pole as not currently installed
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Entry Lane Equipment**/ ENT27**			
1	Card Reader	Connect Lane 600 Lite In	For logic control of the HID Proximity der. Includes pedestal with Intercom

Quantity	Equipment	Model No.	Comments
1	LPR Camera 1	Nanopak	New including Camera and pole as not currently installed
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Entry Lane Equipment**/ ENT30**			
1	Card Reader - Lane 600 In Lite	Connect Lane 600 Lite In	For logic control of the HID Proximity Reader. Includes pedestal with Intercom
1	LPR Camera 1	Nanopak	New including Camera and pole as not currently installed
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Entry Lane Equipment**/ ENT31**			
1	Card Reader	Connect Lane 600 Lite In	For logic control of the HID Proximity Reader. Includes pedestal with Intercom
1	LPR Camera 1	Nanopak	New including Camera and pole as not currently installed
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Entry Lane Equipment**/ ENT32**			
1	Card Reader	Connect Lane 600 Lite In	For logic control of the HID Proximity Reader. Includes pedestal with Intercom
1	LPR Camera 1	Nanopak	New including Camera and pole as not currently installed
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
BUS LANE EQUIPMENT			
Entry Lane Equipment/ **ENT28**			
1	Card Reader	Connect Lane 600 Lite In	New for logic control of the Transcore Reader. Includes pedestal with Intercom
1	Transcore Reader	E3	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Entry Lane Equipment/ **ENT29**			
1	Card Reader	Connect Lane 600 Lite In	New for logic control of the Transcore Reader. Includes pedestal with Intercom
1	Transcore Reader	E3	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
ENT33			
1	Card Reader	Connect Lane 600	New for logic control of the Transcore

Quantity	Equipment	Model No.	Comments
		Lit In	Reader. Includes pedestal with Intercom
1	Transcore Reader	E3	New
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
EMPLOYEE LOT EXITS			
Exit Lane Equipment/ **EXIT 68**			
1	Card Reader	Connect Lane 600 Slim Out	For logic control of the HID Proximity Reader. Includes pedestal with Intercom
	LPR Camera 1	Nanopak	New including Camera and pole as not currently installed
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Exit Lane Equipment/ **EXIT 69**			
1	Card Reader	Connect Lane 600 Slim Out	For logic control of the HID Proximity Reader. Includes pedestal with Intercom
1	LPR Camera 1	Nanopak	New including Camera and pole as not currently installed
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Exit Lane Equipment/ **EXIT 70**			
	Card Reader	Connect Lane 600 Slim Out	For logic control of the HID Proximity Reader. Includes pedestal with Intercom
	LPR Camera 1	Nanopak	New including Camera and pole as not currently installed
	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Exit Lane Equipment/ **EXIT 72**			
1	Card Reader	Connect Lane 600 Slim Out	For logic control of the HID Proximity Reader. Includes pedestal with Intercom
1	LPR Camera 1	Nanopak	New including Camera and pole as not currently installed
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
Exit Lane Equipment/ **EXIT 73**			
1	Card Reader	Connect Lane 600 Slim Out	For logic control of the HID Proximity Reader. Includes pedestal with Intercom
1	LPR Camera 1	Nanopak	New including Camera and pole as not currently installed
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New

Quantity	Equipment	Model No.	Comments
Exit Lane Equipment/ **EXIT 74**			
1	Card Reader	Connect Lane 600 Slim Out	For logic control of the HID Proximity Reader. Includes pedestal with Intercom
1	LPR Camera 1	Nanopak	New including Camera and pole as not currently installed
1	Arming loop	DESIGNA V loop	New
1	Closing loop	DESIGNA N loop	New
BUS LANE EQUIPMENT			
Exit Main Plaza			
	Card Reader	Connect Lane 600 Lite out	For logic control of the Transcore Reader. Includes pedestal with Intercom
	Transcore Reader	E3	New
1	Arming Loop	DESIGNA V loop	New
	Closing Loops	DESIGNA N loop	New
HIBISCUS LEVEL 2 HELIX CONTROL			
4	Arming loop	DESIGNA N loop	New, final number to be agreed to by the Parties
4	Barrier Gate	Gate M	New, final number to be agreed to by the Parties
4	Closing loop	DESIGNA N loop	New, final number to be agreed to by the Parties
MOBILE LPI			
Mobile License Plate Inventory Systems			
1	Handheld	12.9” iPad PRO	New
1	Mobile LPI	Picopak	New including Vehicle mounted Cameras, in Vehicle tablet and all associated hardware
TEST ENVIRONMENT			
1	PARCS Application Server	R6515	PowerEdge Server Motherboard, with 2 x 1Gb Onboard LOM (BCM5720)MLK2
1	UPS	DLRT5KRMXLT	Dell SmartUPS 5000VA 208V - Rack/Tower
1	Server Rack rails	09D83	Dell Ready Rails 2U Static Rails for 2/4-Post Racks and ReadyRails Sliding Rails Without Cable Management Arm, CK
1	Intercom Server	S3	Commend Server
Entry Lane Equipment/ **ENTTEST**			
1	Ticket Dispenser	Connect Lane 600 In Full	New including basic device, Pinhole Camera, Intercom, QR code reader, and Contact/Contactless Credit Card Reader

Quantity	Equipment	Model No.	Comments
1	SunPass Reader	E5	New
1	SunPass Sign	SignalTech 5211	New
1	LPR Camera 1	Nanopak	New
1	Arming loop	DESIGNA V loop	New
1	Barrier Gate	Gate M	New
1	Closing loop	DESIGNA N loop	New
1	UPS	Micro 400	New

Quantity	Equipment	Model No.	Comments
Exit Lane Equipment/ **EXTTEST**			
1	Exit Ticket Reader	Lane 600 Slim Out	New including basic device, intercom, QR code reader, Contact and Contactless Credit Card Readers and Receipt Printer
1	LPR Camera 1	Nanopak	New
1	UPS	Micro 400	New
1	SunPass Reader	E5	New
1	Arming loop	DESIGNA V loop	New
1	Barrier Gate	Gate M	New
1	Closing loop	DESIGNA N loop	New
Employee Entry Lane Equipment/ **ENTEMP**			
1	Card Reader	Connect Lane 600 Lite In	New for logic control of the Transcore Reader. Includes pedestal with Intercom
1	Transcore Reader	E3	Supplied with CR120PLUS
1	LPR Camera 1	Nanopak	New including Camera and pole as not currently installed
1	UPS	Micro 400	New
1	Arming loop	DESIGNA V loop	New
1	Barrier Gate	Gate M	New
1	Closing loop	DESIGNA N loop	New
Employee Exit Lane Equipment/ **EXTEMP**			
1	Card Reader	Connect Lane 600 Slim Out	New for logic control of the Transcore Reader. Includes pedestal with Intercom
1	Transcore Reader	E3	Supplied with CR120 PLUS
1	LPR Camera 1	Nanopak	New including Camera and pole as not currently installed
1	UPS	Micro 400	New
1	Arming loop	DESIGNA V loop	New

Quantity	Equipment	Model No.	Comments
1	Barrier Gate	Gate M	New
1	Closing loop	DESIGNA N loop	New
Cashier Equipment/ **CASHTEST**			
1	Cashier equipment	Connect POS600	New including Cashier Workstation, 17" TFT monitor, keyboard, QR code reader, Contact and Contactless Credit Card Reader, Receipt Printer, Customer Fee Display, Cash Drawer and Intercom Base Station
Quantity	**Equipment**	**Model No.**	**Comments**
1	Intercom Base Station	Commend ID5	New, as required for Intercom control
Valet			
1	Handheld	iPhone 13	New
MLPI			
1	Handheld	12.9" iPad PRO	New
Networking			
60	, 8 x 1GBASE-T, L2+ Managed Industrial Switch (Rugged - Low Voltage) Switch	FS.com IE3110-8TF	New
9	16-Port Gigabit Ethernet L2+ (Rugged) Switch	FS.com IE31110-16TF	New
15	20 x 10Gb SFP+, L3 Core and Distribution Switch	FS.com SS860-20SQ	New
84	10GBASE-LRM SFP+ 1310nm 2km DOM Duplex LC SMF Optical Transceiver Module for FS	SFP-10GER-55	New
1	Ancillary Equipment to	To be confirmed by the Parties	New

Quantity	Equipment	Model No.	Comments
	be confirmed by the Parties		
SPARE PARTS			
2	Ticket Dispenser	Connect Lane 600 Full In	New
2	Ticket Reader	Connect Lane 600 Slim Out	New
1	Card Reader	Connect Lane 600 Lite In	New
Quantity	**Equipment**	**Model No.**	**Comments**
1	Card Reader	Connect Lane 600 Slim Out	New
2	Barrier Gate	Gate M	New
2	LPR Camera 1	Nanopak	New

Provider shall be responsible for maintaining, organizing, storing, and managing an appropriate spare parts inventory. The spare parts inventory, shall include, but not be limited to, sufficient inventory to enable Provider to respond to support requirements within the Required Response Times.

(THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK.)

EXHIBIT B - PAYMENT SCHEDULE

The rates specified below shall be in effect for the entire Term, 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**.

Completion Payments:

Provider shall invoice County for the following amounts upon Provider's completion and County's written notice of acceptance of the applicable completion task below:

Completion Task/Invoicing	Completion Amount	Retention Amount	Completion Payment	Acceptance Criteria
On completion of Critical Design Review	$400,000.00	$20,000.00	$380,000.00	On County's written acceptance of Critical Design Review deliverables as per Section 12 of **Exhibit A**. Deliverables Number 6, 7, 8, and 9 and County's written acceptance of all functional specifications for sub-systems.
On establishment of the Test Environment	$272,294.00	$13,615.00	$258,679.00	On County's written acceptance of system functionality requirements as per Section 6 of **Exhibit A**, System functionality.
On establishment of Production and Disaster Recovery Server Environments	$288,783.00	$14,439.00	$274,344.00	Upon installing and operating properly, as determined by the County.
On acceptance of SunPass system integration	$431,530.00	$21,577.00	$409,953.00	Upon County's written acceptance of SunPass integration per Section 9 of **Exhibit A**, testing No. 14.
On acceptance of the Pre-Booking System	$125,000.00	$6,250.00	$118,750.00	Upon installing in the Test environment and County's written acceptance of the System functionality requirements.

Completion Task/Invoicing	Completion Amount	Retention Amount	Completion Payment	Acceptance Criteria
On acceptance of the employee parking system in the Test Environment	$145,000.00	$7,250.00	$137,750.00	Upon installing in the Test environment and County's written acceptance of the System functionality requirements.
On acceptance of the Loyalty System, as agreed to by the Parties	$80,000.00	$4,000.00	$76,000.00	Upon installing in the Test environment and County's written acceptance of the System functionality requirements.
On completion of the Reporting requirements	$260,000.00	$13,000.00	$247,000.00	Upon installing in the Test environment and County's written acceptance of the System functionality requirements in Section 6(H)(ii) of **Exhibit A**.
PARCS	$572,530.00	$28,627.00	$543,903.00	Upon installing and integrating PARCS network components to the System.
Equipment	$1,450,792.00	$72,540.00	$1,378,252.00	Upon delivery of the Equipment to each site not included in other milestones and County's written acceptance of such Equipment.
Build and deploy each lane	$736,331.00	$36,817.00	$699,514.00	On commencement of In Revenue Service and go-live of each lane.
Retention			$241,301.00	On satisfactory resolution of all punch list items prior to Final Acceptance, as determined by County.
Final Acceptance (5% of remaining capital investment)	$38,745.00	$1,938.00	$36,807.00	Per Final Acceptance criteria (**Exhibit A**, Section 9, Testing).

Spare Parts prices will be in accordance with Provider's then current list price as published from time to time.

Software/Subscription Fees

Software Description	License Term	Invoicing	Fees
Operating Systems Software License Fee	Perpetual	At County's written Acceptance of the Test Environment	$45,075.00
Subscription Fees	Annual	Monthly in arrears commencing upon In Revenue Service	$10,000.00/monthly (total $120,000.00 annually)
Training	Hourly	N/A	Unlimited hours included until Final Acceptance at no cost

Support and Maintenance Services Fees

Specific Support and Maintenance Services	Unit or Term	Invoicing	Annual Fee
Support and Maintenance	Prior to Final Acceptance, and Year 1 and Year 2 after Final Acceptance	N/A	No Cost
Support and Maintenance	Year 3 after Final Acceptance	Monthly in arrears	$334,800.00
Support and Maintenance	Year 4 after Final Acceptance	Monthly in arrears	$469,038.00
Support and Maintenance	Year 5 after Final Acceptance	Monthly in arrears	$603,109.00
Support and Maintenance	Year 6 after Final Acceptance (if extended)	Monthly in arrears	$497,602.00
Support and Maintenance	Year 7 after Final Acceptance (if extended)	Monthly in arrears	$512,530.00

Specific Support and Maintenance Services	Unit or Term	Invoicing	Annual Fee
Support and Maintenance	Year 8 after Final Acceptance (if extended)	Monthly in arrears	$527,906.00
Support and Maintenance	Year 9 after Final Acceptance (if extended)	Monthly in arrears	$543,744.00
Support and Maintenance	Year 10 after Final Acceptance (if extended)	Monthly in arrears	$560,056.00

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

Optional Services, Additional Software/Licenses, or Other Rates for Services or Labor, as requested by County:

Description	Unit/Term	Fee
Subscription Fee for additional front-end on-line devices added after Final Acceptance	Per device per month	$120.00
Technical Support excluded from the Agreement and not requiring attendance on site during Business hours	Fifteen (15) minutes	$35.00
Technical support excluded from the Agreement and not requiring attendance on site outside of Business hours	Fifteen (15) minutes	$70.00
On-site service by technician excluded from the Agreement during Business hours	Hourly	$175.00
On-site service by technician excluded from the Agreement outside of Business hours	Hourly	$340.00
Rate changes are included in the Support and Maintenance amounts; however, less than five (5) days' notice to Provider will incur this late notice penalty	Hourly	$260.00

The following rates will apply for Provider's designated specialists during Business hours. If specialist labor is required by County outside of Business hours, the rates below shall be increased by a multiplier of two (2). The following rates will be escalated by three (3) percent per annum on the Final Acceptance anniversary date of each year.

Description	Unit/Term	Fee
Project Manager	Hourly	$290.00/hour
Professional Engineer	Hourly	$260.00/hour
Electrical Engineer	Hourly	$260.00/hour
Network Engineer	Hourly	$260.00/hour
Security Specialist	Hourly	$340.00/hour
PCI Specialist	Hourly	$340.00/hour
Licensed Electrician	Hourly	$180.00/hour
Field Technician	Hourly	$170.00/hour
Systems Design Engineer	Hourly	$280.00/hour
Computer Programmer/Analyst	Hourly	$240.00/hour
Business Analyst	Hourly	$260.00/hour
Application Specialist/Trainer – Cost for Additional Training	Hourly	$260.00/hour
Web Application Programmer	Hourly	$260.00/hour
System Integration Specialist	Hourly	$290.00/hour
Database Administrator	Hourly	$290.00/hour
Contract/Agreement Administrator	Hourly	$380.00/hour

(THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK.)

EXHIBIT C - SECURITY REQUIREMENTS

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

Data and Privacy. Provider shall comply with all applicable data and privacy laws and regulations, including without limitation the Florida Information Protection Act of 2014, Florida Statutes Section 501.171, and shall ensure that County data processed, transmitted, or stored in the System is not accessed, transmitted, or stored outside the continental United States. Provider may not sell, market, publicize, distribute, or otherwise make available to any third party any personal identification information (as defined by Florida Statutes Section 817.568 or Section 817.5685) that Provider may receive or otherwise have access to in connection with this Agreement, unless expressly authorized in advance by County. If and to the extent requested by County, Provider shall ensure that all hard drives or other storage devices and media that contained County data have been wiped in accordance with the then-current best industry practices, including without limitation DOD 5220.22-M, and that an appropriate data wipe certification is provided to the satisfaction of the Contract Administrator.

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

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

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

Equipment Leased or Purchased from Provider. Provider shall ensure that physical security features to prevent tampering are included in any Equipment provided under this Agreement. Provider shall ensure, at a minimum, industry-standard security measures are followed during the manufacture of the Equipment provided under this Agreement. Any Equipment provided under this Agreement shall not contain any embedded remote control features unless approved

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

Payment Card Industry (PCI) Compliance. If and to the extent the Provider Platform accepts, transmits or stores any credit cardholder data County or is reasonably determined by County to potentially impact the security of County's cardholder data environment ("CDE"), the following provisions shall apply: Provider shall comply with the most recent version of the Security Standards Council's Payment Card Industry ("PCI") Data Security Standard ("DSS"). Prior to the Effective Date, after any significant change to the CDE, and annually Provider shall provide to County: A copy of their Annual PCI DSS Attestation of Compliance ("AOC"); A written acknowledgement of responsibility for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of County, or to the extent that the service provider could impact the security of County's cardholder data environment; and a PCI DSS responsibility matrix that outlines the exact PCI DSS Controls are the responsibility of the service provider and which controls the service provider shares responsibility with County. Provider shall follow the VISA Cardholder Information Security Program ("CISP") payment Application Best Practices and Audit Procedures and maintain current validation. If Provider subcontracts or in any way outsources the CDE processing, or provides an API which redirects or transmits County Data to a payment gateway, Provider is responsible for maintaining PCI compliance for their API and providing the AOC for the Subcontractor or payment gateway to County. Mobile payment application providers must follow industry best practices such as VISA Cardholder Information Security Program ("CISP") or OWASP for secure coding and transmission of payment card data. Provider agrees that it is responsible for the security of County's cardholder data that it possesses, including the functions relating to storing, processing, and transmitting of the cardholder data. Provider will immediately notify County if it learns that it is no longer PCI DSS compliant and will immediately provide County the steps being taken to remediate the noncompliant status. In no event should Provider's notification to County be later than seven (7) calendar days after Provider learns it is no longer PCI DSS complaint. Provider shall enforce automatic disconnect of sessions for remote access technologies after a specific period of inactivity with regard to connectivity into County infrastructure. (PCI 12.3.8) Provider shall activate remote access from vendors and business partners into County network only when needed by vendors and partners, with immediate deactivation after use. (PCI 12.3.9) Provider shall implement encryption and two-factor authentication for securing remote access

(non-console access) from outside the network into County's environment with access to any stored Credit Card data. (PCI 8.3) Provider shall maintain a file integrity monitoring program to ensure critical file system changes are monitored and approved with respect to County Data. (PCI 10.5.5) All inbound and outbound connections to County's CDE must use Transport Layer Security (TLS) 1.2 or current industry equivalent (whichever is higher).

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

(THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK.)

EXHIBIT D - SUPPORT AND MAINTENANCE MINIMUM STANDARDS

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

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

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

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

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

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

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

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

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

Failure to Meet Required Response Times. If Provider fails to meet the Required Response Times, County may offset against any sums due to Provider by Five Hundred Dollars ($500.00) for each Event that Provider failed to meet the Required Response Time, which amount the Parties agree is a fair and reasonable approximation of County's negative financial impact caused by the delay in Provider's response.

Down Time Maintenance Credit. If a Severe or Critical Event is not resolved or reduced to Minor or Minimal priority level within two (2) business hours after notice to Provider, Provider will refund to County five percent (5%) of the monthly fee (or monthly pro rata equivalent, if the fee is other than monthly) for Support and Maintenance for each additional business hour that the Event remains unresolved or at the Severe or Critical priority level, unless the Contract Administrator determines, in his or her sole discretion, that Provider utilized best efforts to implement and is actively pursuing an appropriate plan for prompt resolution. Such refunds will be paid within ten (10) days or, at County's option, may be credited against future sums due to Provider. This refund shall be in addition to any other remedy that is available in the event of a breach of the Agreement.

EXHIBIT E - MINIMUM INSURANCE REQUIREMENTS

Broward County Board of County Commissioners

Bid PNC2119994R1

Minimum Insurance Requirements for Parking Access and Revenue Control System

the following are deemed appropriate for minimum insurance requirements for this project and will be required of the selected firm and be incorporated in the final agreement. Any deviation or change shall be approved in writing byRisk Management.

TYPE OF INSURANCE 1. ALL COI's be submitted on an ACCORD 25 form 2. ALL deductibles are vendors responsibility 3. Self-Insurance and SIR's are not approved	Limits on Liability in Thousands of Dollars		
		Each Occurrence	**Aggregate**
GENERAL LIABILITY [x] Commercial General Liability [x] Premises–Operations [ ] Explosion & Collapse Hazard [ ] Underground Hazard [x] Products/Completed Operations Hazard [x] Contractual Insurance [x] Broad Form Property Damage [x] Independent Contractors [x] Personal Injury [x] mobile equipment [x]garage keepers	Bodily Injury		
	Property Damage		
	Bodily Injury and Property Damage Combined	**$ 2 Mil**	**$ 5 Mil**
	Personal Injury		
AUTO LIABILITY [x] ComprehensiveForm [x] Owned [x] Hired [x] Non-owned [X] Any Auto If applicable	Bodily Injury (each person)		Broward County reserves the right to review and revise any insurance requirements at the time of contract renewal, not limited to the limits, coverages and endorsements based on insurance market conditions and/or changes in the scope of services.
	Bodily Injury (each accident)		
	Property Damage		
	Bodily Injury and Property Damage Combined	**$300 K non airside** **$5 Mil airside**	
[x] PROPERTY INSURANCE **Waiver of subrogation**	**Full replacement value of all equipment on site**		
[X] SOFTWARE/TECH E&O		**$5 Mil**	**$5 Mil**
[x]CYBER INSURANCE		**$5 Mil**	**$5 Mil**
[x] WORKER'S COMPENSATION AND EMPLOYER'S LIABILITY (NOTE *) WC required no State exemptions accepted	[x] STATUTORY dollar limitation		
		(each accident)	**$1 Mil**
Contractor responsible for all tools, materials, equipment, machinery, etc., until completion and acceptance by County. **NO DEDUCTIBLE SHALL BE GREATER THAN TEN THOUSAND DOLLARS ($10,000.00)** **"claims made" basis must remain in force for two (2) years after the termination of this contract**			
Description of Operations/Locations/Vehicles Certificate must show on general liability and excess liability **Additional Insured: Broward County.** Also when applicable certificate should show Certificate Must be Signed and All applicable Deductibles shown. **INSURED is RESPONSIBLE FOR ALL DEDUCTIBLES UNLESS OTHERWISE STATED. Indicate bid number, RLI, RFP, and project manager on COI.**			

NOTE * - If the Company is exempt from Workers' Compensation Coverage, please provide a letter on company letterhead or a copy of the State's exemption which documents this status and attaché to the Certificate of Insurance for approval. If any operations are to be undertaken on or about navigable waters, coverage must be included for U.S. Longshoremen & Harbor Workers' Act/ & Jones Act **CANCELLATION: Thirty (30) Day written notice of cancellation required to the Certificate Holder:**

Name & Address of Certificate Holder
Broward County
2200 SW 45th Street, Suite 101
Fort Lauderdale, FL 33301 RE: Parking

Tracy Meyer

Digitally signed by Tracy Meyer
DN: dc=local, dc=fll-airport, ou=FLLUSERS, cn=Tracy Meyer
Date: 2019.12.17 11:55:56 -05'00'

Aviation Department
Risk Manager itsForm.03 Revised certificateofinsrevised2005.DOC COI

EXHIBIT F - WORK AUTHORIZATION

Agreement Title: _____
Agreement Date: _____
Contract Number: _____
Work Authorization No. _____
Provider: _____

This Work Authorization is between Broward County and Provider pursuant to the Agreement. Provider affirms that the representations and warranties in the Agreement are true and correct as of the date this Work Authorization is executed by Provider. In the event of any inconsistency between this Work Authorization and the Agreement, the provisions of the Agreement shall govern and control.

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

Services to be provided:

[COMPOSE SIMPLE SUMMARY]

See Exhibit A for additional detail.

The applicable not-to-exceed amount stated in the Agreement for the work at issue is: $[_____].

The total fee for goods and services under this Work Authorization is: $[_____] ("Total Fee").

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

(*Signatures appear on the following page.*)

IN WITNESS WHEREOF, the Parties hereto have made and executed this Work Authorization, effective as of the date the last party signs this Work Authorization.

County

_____ _____

Project Manager Date Contractor Administrator Date

Approved as to form by the
Office of the Broward County Attorney

_____

Board or Designee Date

_____

Yesenia Alfonso (Date)
Assistant County Attorney

Provider [Name of Provider]

WITNESSES

_____

Signed Date

_____ _____

Signature Print/Type Name

_____ _____

Print/Type Name Title

_____

Signature

_____

Print/Type Name

ATTEST

_____

Signed Date

_____

(Print/Type Name of Secretary)

CORPORATE SEAL

EXHIBIT G - SERVICE LEVEL AGREEMENT

In connection with all Services provided to County under the applicable contract (the "Agreement"), Provider shall, at no additional cost to County, meet or exceed the requirements set forth in this Service Level Agreement ("SLA") for the duration of the Agreement. The standards set forth herein are intended to reflect the current industry best practices for the Provider Platform provided by Provider under this Agreement. If and to the extent industry best practices evolve to impose higher standards than set forth herein, this SLA shall be deemed to impose the new, higher standards upon Provider. Provider shall promptly notify County in writing of any material change to its compliance with these standards. Any approval required by County under this SLA may be issued in writing by the Contract Administrator or the Broward County Chief Information Officer ("CIO").

Sections 1-5 of this SLA apply to all aspects of the Provider Platform. In addition, Sections 6 and 7 of this SLA apply to any Software as a Service ("SaaS") or web hosting services provided to County under the Provider Platform.

1. **Definitions**

1.1. "Provider Platform" means any and all SaaS or web hosting to be provided by Provider under the Agreement, including any system or other solution that stores, hosts, or transmits County Data. Provider shall maintain the same standards set forth herein for its data centers and facilities that store or host County Data.

1.2. "County Data" means the data and information (including text, pictures, sound, graphics, video and other medium) relating to County or its employees or agents, or made available or provided by County or its agents to Provider, 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 Provider's services, whether or not electronically retained, and regardless of the retention media.

1.3. Any other capitalized terms not defined herein refer to those terms as defined in the Agreement, if so defined; if not defined in the Agreement, any other capitalized terms shall have their plain language meaning as used in the applicable context**.**

2. **Security**

2.1. **General**

2.1.1. Provider will ensure that County can authenticate all access by username/password or two-factor authentication. Upon request, Provider shall restrict access to County Data to a specific source static IP address.

2.1.2. Provider shall ensure that separation of duties and least privilege access are enforced for privileged or administrative access to County Data and the Provider Platform.

2.1.3. Provider's procedures for the following must be documented and made available upon request by County, including:

2.1.3.1. Evaluating security alerts and vulnerabilities;
2.1.3.2. Installing security patches and service packs;
2.1.3.3. Intrusion detection, incident response, and incident escalation/investigation;
2.1.3.4. Access and authorization procedures and resetting access controls (e.g., password policy);
2.1.3.5. Risk analysis and assessment procedures;
2.1.3.6. User access and termination procedures;
2.1.3.7. Security log review;
2.1.3.8. Physical facility access controls; and
2.1.3.9. Change control procedures.

2.1.4. Provider shall ensure that its service providers, subcontractors, and any third parties, including any data hosting providers, performing any services related to this Agreement shall comply with all terms and conditions specified in this SLA unless County, in writing, excuses specific compliance with any such term or condition. Provider shall provide County with a list of any such service providers, subcontractors or other third parties on an annual basis, upon County's request, and promptly upon a material change in the composition of such entities.

2.1.5. If new or unanticipated threats or hazards to the Provider Platform are discovered by either County or Provider, or if existing safeguards have ceased to function properly, the discovering party shall immediately bring the situation to the attention of the other party.

2.1.6. When technically feasible, for all software used, furnished, or supported under the Agreement, Provider shall review such software to find and remediate security vulnerabilities during initial implementation and upon any significant modifications and updates to same.

2.1.7. Provider must mitigate critical or high-risk vulnerabilities (as defined by Common Vulnerability and Exposures scoring system) to the Provider Platform within 30 days after patch release. If Provider is unable to apply a patch to remedy the vulnerability, Provider must promptly notify County of proposed mitigation steps to be taken and develop and implement an appropriate timeline for resolution.

2.2. **Controls**

2.2.1. Prior to the Effective Date of the Agreement, and at least once annually and upon request for the duration of this Agreement, Provider shall provide County with a copy of a current unqualified System and Organization Controls (SOC) 2 Type II, Report for Provider's Organization or application, as well as any

third party that provide hosting, SaaS, or data storage services for the Provider Platform, inclusive of all five Trust Service Principles (Security, Availability, Processing Integrity, Confidentiality, and Privacy), unless County's Chief Information Officer in his or her sole discretion approves other documentation of appropriate security controls implemented by Provider. If the audit opinion in the SOC 2, Type II report is qualified in any way, Provider shall provide sufficient documentation to demonstrate remediation of the issue(s) to the satisfaction of County's Chief Information Officer.

2.2.2. Provider shall maintain industry best practices for data privacy, security, and recovery measures, including, but not limited to, disaster recovery programs, physical facilities security, server firewalls, virus scanning software, current security patches, user authentication, and intrusion detection and prevention. Upon request by County, Provider shall provide documentation of such procedures and practices to County.

2.2.3. Provider shall utilize industry standard security measures to safeguard against unauthorized access to the Provider Platform.

2.2.4. Provider shall utilize antivirus protection software, updated and currently supported operating systems, firmware, third party and open source application patches, and firewalls to protect against unauthorized access to the Provider Platform.

2.2.5. Provider shall conduct penetration testing internally and externally at least annually and after any significant infrastructure or application upgrade or modification to the Provider Platform.

2.3. **Network Architecture/Security**

2.3.1. Provider shall protect any Internet interfaces or web services provided under this Agreement using a security certificate from a certification authority ("CA") that meets or exceeds the CA/Browser Forum's latest Secure Sockets Layer ("SSL") baseline requirements and network and certificate systems security requirements.

2.3.2. Provider will support encryption using at a minimum Advanced Encryption Standard 256-bit encryption keys ("AES-256") or current industry security standards, whichever is higher, for the connection between any user or County network to the Provider Platform.

2.4. **Physical Architecture/Security**

2.4.1. Provider shall ensure the facilities that house the network infrastructure for the Provider Platform are physically secure against threats such as

unauthorized access and natural and environmental hazards, and entry controls are in place to limit and monitor physical access to the Provider Platform.

2.4.2. Provider shall ensure adequate background checks are routinely performed on any personnel with access to County Data. Provider shall not knowingly allow convicted felons or other persons deemed by Provider to be a security risk to access County Data. Provider shall provide privacy and information security training to its employees upon hire and at least once annually.

2.5. **Incident Response**

2.5.1. If any unauthorized party is successful in accessing any information technology component related to the Provider Platform, including but not limited to servers or fail-over servers where County Data exists or is stored, Provider shall report to County within twenty-four (24) hours after Provider becoming aware of such breach. Provider shall provide County with a detailed incident report within five (5) days after the breach, unless a longer time period is approved in writing by the CIO, including remedial measures instituted and any law enforcement involvement. Provider shall fully cooperate with County on incident response, forensics, and investigations that involve the Provider's infrastructure relating to any County Data or County applications. Provider shall not release County Data without the advance written consent of County.

2.5.2. Prior to the Effective Date of this Agreement, Provider shall provide County with the names and contact information for a security point of contact and a backup security point of contact to assist County with security incidents.

2.5.3. Upon request by County, Provider shall deliver to County in electronic form the website application activity such as logs of visits and user logins and logoffs by or on behalf of County on the Provider Platform.

2.5.4. In the event the Provider Platform has been compromised, Provider shall promptly notify County of the security breach. County may, at its sole discretion, terminate all access to the Provider Platform.

2.6. **County Data**

2.6.1. Provider shall maintain controls that ensure logical separation of County Data from non-County data. Provider agrees to provide at a minimum Advanced Encryption Standard 256-bit encryption ("AES-256") or current industry security standards (or whichever is higher) for all County Data that includes any social security numbers, bank account numbers, username with passwords or security questions, cardholder data, or any other protected data such as Protected Health Information ("PHI") and Personally Identifiable Information ("PII"), and any other data as may be directed by County, and on all copies of such data stored,

transmitted, or processed, at no additional charge to County, and shall classify such data internally at its highest confidentiality level. Provider shall also ensure that the encryption key(s) are not stored with the encrypted data and are secured by a Hardware Security Module ("HSM"). Provider shall immediately notify County of any compromise of any encryption key. Provider shall provide a copy of County's encryption key(s) at County's request. Provider shall prohibit the use of unencrypted protocols such as FTP and Telnet for the data identified in this paragraph.

2.6.2. Upon termination or expiration of this Agreement or end of serviceable life of any media used in connection with this Agreement, and upon written notification from County that the applicable County Data is currently maintained by County or otherwise securely stored, Provider shall, at County's option, (a) securely destroy all media (including media used for backups) containing any County Data on all decommissioned hard drives or storage media to National Institute of Standards and Technology ("NIST") standards and provide to County a signed certificate of destruction within ten (10) business days, or (b) return to County all County Data and provide a signed certification within two (2) business days thereafter documenting that no County Data is retained by Provider in any format or media.

2.6.3. County Data is the property solely of County and may not be reproduced or used by Provider with the prior written consent of County. Provider and its Subcontractors will not publish, transmit, release, sell, or disclose any County Data to any third party without County's prior written consent.

2.6.4. County shall have the right to use the Products and Services to provide public access to County Data as County deems appropriate or as otherwise required by law.

2.6.5. In the event of any impermissible disclosure, loss, or destruction of County Data caused in whole or in part by any action or omission of Provider, Provider must immediately notify County and take all reasonable and necessary steps to mitigate any potential harm, further disclosure, loss, and destruction.

2.6.6. County shall have sole control over County Data unless otherwise expressly stated in the Agreement and required for Provider to provide the Services required under the Agreement.

2.6.7. Provider shall not supplement, modify, or alter any deliverable previously accepted by County or any County Data (other than modifications strictly necessary to upload County Data to the Contactor Platform) without County's prior written consent.

3. **Compliance**

3.1. Provider shall cooperate and provide any information requested by County relating to compliance and regulatory requirements, and will, upon request:

3.1.1. Provide a letter attesting that the Provider performed vulnerability scans of authenticated and unauthenticated operating systems/networks, web applications, database applications, and the Provider Platform;

3.1.2. Permit County or its Providers to conduct automated and manual scans and penetration ("Pen") tests at mutually agreed upon times;

3.1.3. Provide Provider's architecture documents, information security policies and procedures (redacted, if necessary), and general network security controls documentation such as firewalls, Intrusion Detection System ("IDS"); and

3.1.4. Permit County to conduct a physical inspection of Provider's facilities but only to the extent such inspection is related to the security of and access to County Data or the Provider Platform.

3.2. Provider shall provide County with the ability to generate account reports consisting of the account holder's name and application access rights.

3.3. Provider shall provide County with the ability to generate account management reports showing new users, access rights changes, and account termination with the associated time stamp information.

3.4. Provider shall provide County with the ability to generate time-stamped user and administrator access (login/logout) and a list of activities performed by administrators, privileged users, or third-party Providers while using the System.

3.5. Upon request by County, Provider shall promptly provide County with access to time-stamped data transfer logs (including the account, a description of the data transferred and its size, and the user and account names for forensic purposes), time-stamped application and platform environment change control logs, and time-stamped data backup logs indicating the backup type (e.g., full, incremental, etc.).

3.6. Upon County's request, Provider shall make available to County proof of Provider's compliance with all applicable federal, state, and local laws, codes, ordinances, rules, and regulations in performing under this Agreement, including but not limited to: HIPAA compliance; Provider's latest compliance reports (e.g., PCI Compliance report, SSAE 16 report, International Organization for Standardization 27001 (ISO 27001) certification); and any other proof of compliance as may be required from time to time.

4. **Infrastructure Management**

Provider shall ensure that an unlimited number of transactions may be processed to the County production database. Subject to County approval, Provider may recommend that non-routine reports and queries be limited to certain timeframes, quantities or other specifications if Provider determines that such reports and queries cause degradation to response times affecting performance levels established in this SLA. Provider shall routinely apply upgrades, new releases, and enhancements to the Provider Platform as they become available and shall ensure that these changes will not adversely affect the Provider Platform or County Data. A development and test system, which shall mirror the production system, shall be made available for use by County for testing or training purposes, including without limitation, for County's testing of application upgrades and fixes prior to installation in the Production Environment. County may control data that is populated on the demonstration and training system by requesting that Provider perform any or all of the following: periodically refresh data from production; perform an ad-hoc refresh of data from production; not refresh data from production until further notice from County; or refresh data on an ad hoc basis with training data supplied by County.

5. **Transition/Disentanglement**

5.1. Provider will complete the transition of any terminated Services or Support and Maintenance to County and any replacement provider(s) that County designates (collectively, the "Transferee"), without causing any unnecessary interruption of, or adverse impact on, the Services, County Data, or the ongoing business operation of County ("Disentanglement"). Provider will work in good faith (including, upon request, with the Transferee) at no additional cost to County to develop an orderly Disentanglement plan that documents the tasks required to accomplish an orderly transition with minimal business interruption or expense for County. Upon request by County, Provider shall cooperate, take any necessary additional action, and perform such additional tasks that County may reasonably request to ensure timely and orderly Disentanglement, which shall be provided at the rate(s) specified in the Agreement or, if no applicable rate is specified, at a reasonable additional fee upon written approval by County. Specifically, and without limiting the foregoing, Provider shall:

5.1.1. Promptly provide the Transferee with all nonproprietary information needed to perform the Disentanglement, including, without limitation, data conversions, interface specifications, data about related professional services, and complete documentation of all relevant software and equipment configurations;

5.1.2. Promptly and orderly conclude all work in progress or provide documentation of work in progress to Transferee, as County may direct;

5.1.3. Not, without County's prior written consent, transfer, reassign, or otherwise redeploy any of Provider's personnel during the Disentanglement period to the extent such action would impede performance of Provider's obligations under the Agreement;

5.1.4. If applicable, with reasonable prior written notice to County, remove its assets and equipment from County facilities;

5.1.5. If County requests, and to the extent permitted under the applicable agreements, assign to the Transferee (or use its best efforts to obtain consent to such assignment where required) all contracts including third-party licenses and maintenance and support agreements, used by Provider exclusively in connection with the Services or Support and Maintenance. Provider shall perform all of its obligations under such contracts at all times prior to the date of assignment, and Provider shall reimburse County for any losses resulting from any failure to perform any such obligations;

5.1.6. Deliver to Transferee all current, nonproprietary documentation and data related to County-owned assets and infrastructure. After confirming in writing with County that the applicable County Data is received intact or otherwise securely stored by County, Provider shall securely erase all County Data, including on any hard drives and backup media, in accordance with NIST standards. Upon written consent from County, Provider may retain one copy of documentation to the extent required for Provider's archival purposes or warranty support; and

5.1.7. To the extent requested by County, provide County a list with current valuation based on net book value of any Provider-owned tangible assets required to make the Provider Platform available to County. County shall have the right to acquire any or all such assets for net book value. If County elects to acquire such assets for the net book value, Provider shall use best efforts to ensure that any and all related warranties will transfer along with those assets.

6. Network Architecture/Security

6.1. Network Architecture

6.1.1. The Provider Platform shall be protected behind a layer of firewalls.

6.1.2. At County's request, Provider shall submit a network architecture diagram of County's stored and transmitted data, including the location of the data center and details of connectivity for all third parties who have access to County Data. Any network security changes implemented by Provider must not compromise the security of County Data. Provider shall ensure that all database servers are protected behind a second set of internal firewalls.

6.1.3. Provider shall restrict inbound and outbound traffic to County's network to "deny all, permit by exception" configuration.

6.1.4. Provider's wireless networks connected to the Provider Platform shall at a minimum, be configured for Wi-Fi Protected Access 2 (WPA2)-Enterprise using

Advanced Encryption Standard (AES) and Protected Extensible Authentication Protocol (PEAP), or current industry security standards (whichever is higher) to secure and protect County data.

6.2. Physical Architecture/Security. Provider shall connect its hosting site for the Provider Platform through at least two (2) independent Internet Service Providers ("ISPs") with different Internet points of presence.

6.3. **Disaster Recovery**

6.3.1. Provider shall maintain a disaster recovery plan for the Provider Platform with mirrored sites geographically separated by at least 250 miles, with a Recovery Time Objective ("RTO") of a maximum of eight (8) hours and a Recovery Point Objective ("RPO") of a maximum of four (4) hours from the incident.

6.3.2. Provider shall conduct a disaster recovery test of the hosted or SaaS system that is utilized by or comprises the Provider Platform on at least an annual basis, and shall notify County at least ten (10) days in advance of each such test. In addition, Provider shall conduct a disaster recovery test specific to County, including testing County Data and the Provider Platform, in coordination with County at least once per year; the timing and duration of County-specific test is subject to the approval of County.

6.4. **County Data**. Provider shall make any County Data available to County upon request within one (1) business day and in any format reasonably requested by County, including, without limitation, Extensible Markup Language ("XML") and Structured Query Language ("SQL"), or in another format as may be mutually agreed by County and Provider.

7. **Service Availability**

7.1. **System Availability**

7.1.1. Provider guarantees that the Network Uptime (as defined herein) will be 99.99% of Prime Time (defined as County business days from 7 a.m. – 7 p.m. Eastern Time) and 98.00% of non-Prime Time for each calendar month during the term of the Agreement, excluding Scheduled Maintenance as defined herein (collectively, the "Network Uptime Guarantee"). Network Uptime is the time that the Provider Platform and System are functioning optimally and fully operational, and requires proper functioning of all network infrastructure, including routers, switches, and cabling, affecting a user's ability to reliably transmit or receive data; Network Downtime is the remainder of time that is not included in Network Uptime, and is measured from the time the trouble ticket is opened to the time the Provider Platform and System are fully restored. As long as the System is available over the Internet to at least two other comparable non-County

customers (i.e., the System is functioning properly and there are no technical issues with Provider or the Provider Platform), any inability on the part of County to access the System as a result of a general Internet outage will not be counted toward Network Downtime. System unavailability for the purpose of building redundancy or other recovery systems that is approved by County in advance shall not be charged as downtime in computing the Network Downtime. Provider Platform or System unavailability due to Provider's equipment failure constitutes Network Downtime.

7.1.2. Provider will refund to County five percent (5%) of the monthly fees (or monthly pro rata equivalent, if recurring fees under the Agreement are charged other than monthly) under the Agreement for each thirty (30) minutes of Network Downtime in excess of that permitted under the Network Uptime Guarantee (up to 100% of County's monthly or pro rata fee), measured on a calendar month basis. Such refunds will be paid within ten (10) days after the applicable monthly report or, at County's option, may be credited against amounts due under any unpaid invoice or future invoice. If the Agreement provides for other credit or compensation due to County for an event that also constitutes Network Downtime, the greater of the two amounts shall apply.

7.1.3. Normal availability of the Provider Platform and System shall be twenty-four (24) hours per day, seven (7) days per week. Planned downtime (i.e., taking the System offline such that it is not accessible to County) ("Scheduled Maintenance") shall occur during non-Prime Time and with at least five (5) business days' advance written notice to County. Provider may conduct Scheduled Maintenance at other times without advance notice only with written consent from County, which consent will not be unreasonably withheld. During non-Prime Time, Provider may perform routine maintenance operations that do not require the Provider Platform or System to be taken offline but may have immaterial effects on performance and response time without any notice to County. Such immaterial degradation in performance and response time shall not be deemed Network Downtime. All changes that are expected to take more than four (4) hours to implement or are likely to impact user workflow require County's prior written approval, which will not be unreasonably withheld.

7.1.4. By the tenth day of each calendar month, Provider shall provide County a report detailing Provider's performance under this SLA for the prior calendar month. To the extent the performance fails to meet the Network Uptime Guarantee, the report shall calculate: the total number of minutes of uptime for each of Prime Time and non-Prime Time; the total number of minutes for each of Prime Time and non-Prime Time minus any applicable Scheduled Maintenance, respectively; and the percentage of uptime versus total time minus Scheduled Maintenance for each (e.g., monthly minutes of non-Prime Time network uptime / (Total minutes of non-Prime Time – Minutes of Scheduled Maintenance) = __%).

7.2. **Infrastructure Management**

7.2.1. During Prime Time, Provider shall ensure packet loss of less than one percent (1%) and less than sixty (60) milliseconds domestic latency within the Provider Platform. Provider shall maintain sufficient bandwidth to the Provider Platform and ensure the server processing time (or CPU processing capacity) to provide millisecond response times from the server. County and Provider recognize that end user response times are dependent on intermittent ISP network connectivity, and in the case of County's users, dependent on County's internal network health.

7.2.2. To the extent the Provider Platform provides or supports public access to users in Broward County or through County's web pages, the Provider Platform shall support up to 500,000 site hits per calendar day and capture the number of site hits by page for performance to standards reporting.

7.2.3. Provider will retain all County-related database records regardless of number or size.

7.2.4. To the extent the Provider Platform includes an ad-hoc reporting tool or standard reports, Provider agrees to provide unlimited access to such functionality to County. Provider agrees to support an unlimited number of queries and reports against County Data. County agrees that Provider may put reasonable size limits on queries and reports to maintain System performance, provided such limits do not materially impact County's regular business operations.

7.2.5. Provider shall conduct full, encrypted backups (including System and user data) weekly and shall conduct incremental, encrypted backups daily. Encrypted backups will be written to a backup device with sufficient capacity to handle the data. Provider shall maintain a complete current set of encrypted backups for County's System, including County Data, at a remote, off-site "hardened" facility from which data can be retrieved within one (1) business day at any point in time. Full System restoration performed as a recovery procedure after a natural disaster is included as part of the required performance by Provider under this Agreement. Upon County's request, Provider shall also provide restoration of individual file(s).

7.3. **Performance Monitoring and Hosting Capacity Increases**

7.3.1. If requested by County, Provider shall provide standard reporting metrics of the Provider Platform to County on a monthly basis which shall include: traffic patterns by user and by time; server load, including central processing unit load, virtual memory, disk and input/output channel utilization; transmission control protocol load for each server allocated in part or in full to County System; and system errors in the System, database, operating system, and each server allocated in part or in full to the System.

7.3.2. In the event County anticipates an increase in transaction volume or seeks to expand capacity beyond the limitations, if any, provided under the Agreement, Provider will provide timeline and cost estimates to upgrade existing servers or deploy additional servers dedicated to County's System within fifteen (15) calendar days after written notice by County.

(THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK.)

EXHIBIT H - CBE SUBCONTRACTOR SCHEDULE AND LETTERS OF INTENT

BROWARD COUNTY FLORIDA
OFFICE OF ECONOMIC AND SMALL BUSINESS DEVELOPMENT

LETTER OF INTENT

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

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

Solicitation No.: PNC2119994R1

Project Title: Parking Access and Revenue Control Equipment and Maintenance

Bidder/Offeror Name: DESIGNA Access Corporation

Address: 4401 S Pinemont Drive. Suite 200 City: Houston State: TX Zip: 77041

Authorized Representative: Paul McIlvride Phone: 347 852 5550

CBE Firm/Supplier Name: AUM Construction Inc.

Address: 6011 Rodman Street, Suite 208 City: Hollywood State: FL Zip: 33023

Authorized Representative: Humberto Ortiz Phone: 954 251 2455

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
Installation and Maintenance Services	238210,811320	$ 1,084,092.00	21.30 %
			%
			%

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

CBE Firm/Supplier Authorized Representative

Signature: Humberto C Ortiz Digitally signed by Humberto C Ortiz DN: c=US, o=aum construction inc, dnQualifier=A01410C000000178A1F0D93B00003F23, cn=Humberto C Ortiz Date: 2023.08.30 16:25:34 -04'00' Title: President Date: 08/30/2023

Bidder/Offeror Authorized Representative

Signature: Paul H McIlvride Digitally signed by Paul H McIlvride Date: 2023.08.30 12:45:56 -05'00' Title: SVP Sales & Marketing Date: 08/30/2023

---

[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 I - PCI RESPONSIBILITY MATRIX

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				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
1.1.6	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	X				
1.1.7	Requirement to review firewall and router rule sets at least every six months	X				
1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. 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	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	between the wireless environment and the cardholder data environment.					
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	X				
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	X				
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	X				
1.3.3	Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	X				
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	X				
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				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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 address space instead of registered addresses.	X				
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:	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	• 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.					
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 Protocol (SNMP) community strings, etc.).	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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 technologies are in use, implement only one primary function per virtual system component.	X				
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	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	documented, in use, and known to all affected parties.					
2.6	Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.	X				
3.1	Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: 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				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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 secu*rely. Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	X				
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*	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	To minimize risk, store only these data elements as needed for business.					
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. Note: This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.		X			
3.4	Render PAN unreadable anywhere it is stored (including on portable digital media, backup	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	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.					

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
3.4.1	If disk encryption is used (rather than file or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts. *Note: This requirement applies in addition to all other PCI DSS encryption and key-management requirements.*	X				
3.5	Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse: *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				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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 other SCDs used for key management	X				
3.5.2	Restrict access to cryptographic keys to the fewest number of custodians necessary.	X				
3.5.3	Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • 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	X				
	• 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*	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	stored in one of these forms.					
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 including NIST, which can be found at http://csrc.nist.gov.*	X				
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				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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				
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	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	responsibilities.					
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 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).*	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	• *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				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
5.4	Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	X				
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*	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.					
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				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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 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	X				

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

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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 version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.	X				
6.5.1	Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
6.6	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • 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.	X				
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				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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 necessary to perform job responsibilities.	X				
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				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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				
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				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
8.1.7	Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	X				
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 passwords/phrases) unreadable during transmission and storage on all system components.	X				
8.2.2	Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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	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 methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi- factor authentication*	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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 critical functions. • Shared and generic user IDs are not used to	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	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				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
8.7	All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through 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).	X				
8.8	Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	X				
9.1	Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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 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.	X				
9.1.3	Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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				
9.4.x	Implement procedures to identify and authorize visitors. Procedures should include the following:	X				
9.4.1	Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.	X				
9.4.2	Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
9.4.3	Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	X				
9.4.4	A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. 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 media, including the following:	X				
9.6.1	Classify media so the sensitivity of the data can be determined.	X				
9.6.2	Send the media by secured courier or other delivery method that can be accurately	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	tracked.					
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				
9.8.2	Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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 sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.		X			
9.9.1	Maintain an up-to-date list of devices. The list should include the following: • 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		X			

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	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.					
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 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).		X			

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
9.10	Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.	X				
10.1	Implement audit trails to link all access to system components to each individual user.	X				
10.2	Implement automated audit trails for all system components to reconstruct the following events:	X				
10.2.1	All individual user accesses to cardholder data	X				
10.2.2	All actions taken by any individual with root or administrative privileges	X				
10.2.3	Access to all audit trails	X				
10.2.4	Invalid logical access attempts	X				
10.2.5	Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	X				
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				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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 server or media that is difficult to alter.	X				
10.5.4	Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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 organization's policies and risk management strategy, as determined by the organization's annual risk	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	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:	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	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 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				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
11.1	Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.	X				
11.1.1	Maintain an inventory of authorized wireless access points including a documented business justification.	X				
11.1.2	Implement incident response procedures in the event unauthorized wireless access points are detected.	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.		X			

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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			

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	• 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					

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	place					
11.3.1	Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).		X			
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			

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
11.3.4.1	Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.	X				
11.4	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.		X			
11.5	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the 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			X			

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.					
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 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.		X			
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			

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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			

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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			

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
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 management responsibilities:		X			
12.5.1	Establish, document, and distribute security policies and procedures.		X			
12.5.2	Monitor and analyze security alerts and information, and distribute to appropriate personnel.		X			
12.5.3	Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.		X			
12.5.4	Administer user accounts, including additions, deletions, and modifications.		X			
12.5.5	Monitor and control all access to data.		X			

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
12.6	Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.		X			Applies to all sub-numbered requirements
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.) Note: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.		X			
12.8	Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data,	X				

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

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	entity.					
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			Applies to all sub-numbered requirements

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
12.10.1	Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: • 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.		X			
12.10.2	Test the plan at least annually.		X			
12.10.3	Designate specific personnel to be available on a 24/7 basis to respond to alerts.		X			
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		X			

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	systems.					
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 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		X			
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	X				

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	PCI DSS compliance program					
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				
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 J – NONDISCRIMINATION AND OTHER FEDERAL REQUIREMENTS

A. Title VI List of Pertinent Nondiscrimination Acts and Authorities. During the performance of this Agreement, Provider, for itself, its assignees, and successors in interest, agrees as follows:

1. *Compliance with Regulations:* Provider (hereinafter includes Subcontractors) will comply with the **Title VI List of Pertinent Nondiscrimination Acts and Authorities** ("Nondiscrimination Acts and Authorities"), as they may be amended from time to time, which are herein incorporated by reference and made a part of this Agreement, and which include, but are not limited to, the following:

a. Title VI of the Civil Rights Act of 1964 (42 U.S.C. § 2000d *et seq*., 78 Stat. 252) (prohibits discrimination on the basis of race, color, national origin);

b. 49 C.F.R. Part 21 (Nondiscrimination in Federally-assisted programs of the Department of Transportation—Effectuation of Title VI of the Civil Rights Act of 1964);

c. The Uniform Relocation Assistance and Real Property Acquisition Policies Act of 1970, (42 U.S.C. § 4601) (prohibits unfair treatment of persons displaced or whose property has been acquired because of Federal or Federal-aid programs and projects);

d. Section 504 of the Rehabilitation Act of 1973 (29 U.S.C. § 794 et seq.), as amended (prohibits discrimination on the basis of disability); and 49 C.F.R. Part 27;

e. The Age Discrimination Act of 1975, as amended (42 U.S.C. § 6101 et seq.) (prohibits discrimination on the basis of age);

f. Airport and Airway Improvement Act of 1982 (49 U.S.C. § 47123), as amended (prohibits discrimination based on race, creed, color, national origin, or sex);

g. The Civil Rights Restoration Act of 1987 (P.L. 100-209) (broadened the scope, coverage and applicability of Title VI of the Civil Rights Act of 1964, the Age Discrimination Act of 1975 and Section 504 of the Rehabilitation Act of 1973, by expanding the definition of the terms "programs or activities" to include all of the programs or activities of the Federal-aid recipients, subrecipients and Providers, whether such programs or activities are Federally funded or not);

h. Titles II and III of the Americans with Disabilities Act of 1990, which prohibit discrimination on the basis of disability in the operation of public entities, public and private transportation systems, places of public accommodation, and certain testing entities (42 U.S.C. §§ 12131 – 12189) as implemented by U.S. Department of Transportation regulations at 49 C.F.R. Parts 37 and 38;

i. The Federal Aviation Administration's Nondiscrimination statute (49 U.S.C. § 47123) (prohibits discrimination on the basis of race, color, national origin, and sex);

j. Executive Order 12898, Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations, which ensures nondiscrimination against minority populations by discouraging programs, policies, and activities with disproportionately high and adverse human health or environmental effects on minority and low-income populations;

k. Executive Order 13166, Improving Access to Services for Persons with Limited English Proficiency, and resulting agency guidance, national origin discrimination includes discrimination because of limited English proficiency (LEP). To ensure compliance with Title VI, you must take reasonable steps to ensure that LEP persons have meaningful access to your programs (70 Fed. Reg. at 74087 to 74100); and

l. Title IX of the Education Amendments of 1972, as amended, which prohibits you from discriminating because of sex in education programs or activities (20 U.S.C. § 1681 et seq).

2. *Nondiscrimination:* Provider, with regard to the work performed by it during the Agreement, will not discriminate on the grounds of race, color, or national origin in the selection and retention of Subcontractors, including procurements of materials and leases of equipment. Provider will not participate directly or indirectly in the discrimination prohibited by the Nondiscrimination Acts and Authorities, including employment practices when the Agreement covers any activity, project, or program set forth in Appendix B of 49 C.F.R. Part 21.

3. *Solicitations for Subcontracts, Including Procurements of Materials and Equipment:* In all solicitations, either by competitive bidding or negotiation made by Provider for work to be performed under a subcontract, including procurements of materials, or leases of equipment, each potential subcontractor or supplier will be notified by Provider of Provider's obligations under this Agreement and the Nondiscrimination Acts and Authorities on the grounds of race, color, or national origin.

4. *Information and Reports:* Provider will provide all information and reports required by the Nondiscrimination Acts and Authorities, and directives issued pursuant thereto, and will permit access to its books, records, accounts, other sources of information, and its facilities as may be determined by the sponsor or the Federal Aviation Administration to be pertinent to ascertain compliance with such Nondiscrimination Acts and Authorities and instructions. Where any information required of Provider is in the exclusive possession of another who fails or refuses to furnish the information, Provider will so certify to the sponsor or the Federal Aviation Administration, as appropriate, and will set forth what efforts it has made to obtain the information.

5. *Sanctions for Noncompliance:* In the event of Provider's noncompliance with the nondiscrimination provisions of this Agreement, the sponsor will impose such contract sanctions as it or the Federal Aviation Administration may determine to be appropriate, including, but not limited to:

a. Withholding payments under the Agreement until Provider complies; and/or

b. Cancelling, terminating, or suspending the Agreement, in whole or in part.

6. *Incorporation of Provisions:* Provider will include the provisions of paragraphs one through six in every subcontract, including procurements of materials and leases of equipment, unless exempt by the Nondiscrimination Acts and Authorities, and directives issued pursuant thereto. Provider will take action with respect to any subcontract or procurement as the sponsor or the Federal Aviation Administration may direct as a means of enforcing such provisions including sanctions for noncompliance. Provided, that if Provider becomes involved in, or is threatened with litigation by a Subcontractor or supplier because of such direction, Provider may request the sponsor to enter into any litigation to protect the interests of the sponsor. In addition, Provider may request the United States to enter into the litigation to protect the interests of the United States.

B. Nondiscrimination - 14 C.F.R. Part 152 Requirements. During the performance of this Agreement, Provider, for itself, its assignees, and successors in interest, agrees as follows:

1. Provider agrees to undertake an affirmative action program as required by 14 C.F.R. Part 152, Subpart E, to insure that no person shall on the grounds of race, color, religion, gender, national origin, age, marital status, political affiliation, familial status, physical or mental disability, or sexual orientation be excluded from participation in any employment, contracting, or leasing activities covered in 14 C.F.R. Part 152, Subpart E. Provider agrees that no person shall be excluded on these grounds from participating in or receiving the services or benefits of any program or activity covered by this Subpart. Provider agrees that it will require its covered suborganizations to provide assurances to Provider that they similarly will undertake affirmative action programs and that they will require assurances from their suborganizations as required by 14 C.F.R. Part 152, Subpart E, to the same effect.

2. Provider agrees to comply with any affirmative action plan or steps for equal employment opportunity required by 14 C.F.R. Part 152, Subpart E, as part of the affirmative action program, and by any federal, state, County or local agency or court, including those resulting from a conciliation agreement, a consent decree, court order or similar mechanism. Provider agrees that state or County affirmative action plans will be used in lieu of any affirmative action plan or steps required by 14 C.F.R. Part 152, Subpart E, only when they fully meet the standards set forth in 14 C.F.R. 152.409. Provider agrees to obtain a similar assurance from its covered organizations, and to cause them to

require a similar assurance of their covered suborganizations, as required by 14 C.F.R. Part 152, Subpart E.

3. If required by 14 C.F.R. Part 152, Provider shall prepare and keep on file for review by the FAA Office of Civil Rights an affirmative action plan developed in accordance with the standards in Part 152. Provider shall similarly require each of its covered suborganizations (if required under Part 152) to prepare and to keep on file for review by the FAA Office of Civil Rights, an affirmative action plan developed in accordance with the standards in Part 152.

4. If Provider is not subject to an affirmative action plan, regulatory goals and timetables, or other mechanism providing for short and long-range goals for equal employment opportunity under Part 152, then Provider shall nevertheless make good faith efforts to recruit and hire minorities and women for its aviation workforce as vacancies occur, by taking any affirmative action steps required by Part 152. Provider shall similarly require such affirmative action steps of any of its covered suborganizations, as required under Part 152.

5. Provider shall keep on file, for the period set forth in Part 152, reports (other than those submitted to the FAA), records, and affirmative action plans, if applicable, that will enable the FAA Office of Civil Rights to ascertain if there has been and is compliance with this subpart, and Provider shall require its covered suborganizations to keep similar records as applicable.

6. Provider shall, if required by Part 152, annually submit to County the reports required by Section 152.415 and Provider shall cause each of its covered suborganizations that are covered by Part 152 to annually submit the reports required by Section 152.415 to Provider who shall, in turn, submit same to County for transmittal to the FAA.

(THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK.)

EXHIBIT K – AVIATION DEPARTMENT SECURITY REQUIREMENTS

Airport Security Program and Aviation Regulations.

Provider shall observe all security requirements and other requirements of the Federal Aviation Regulations applicable to Provider, including, but not limited to, all regulations of the United States Department of Transportation, the Federal Aviation Administration, and the Transportation Security Administration. Provider shall comply with County's Airport Security Program and the Air Operations Area ("AOA") Vehicle Access Program, and any amendments thereto, and with such other rules and regulations as may be reasonably prescribed by County, including any regulations pertaining to emergency training, and shall take such steps as may be necessary or directed by County to ensure that Subcontractor, employees, invitees, and guests of Provider observe these requirements. If required by the Aviation Department, Provider shall conduct background checks of its employees in accordance with applicable Federal Regulations. If as a result of the acts or omissions of Provider, its Subcontractors, employees, invitees, or guests, County incurs any fines and/or penalties imposed by any governmental agency, including, but not limited to, the United States Department of Transportation, the Federal Aviation Administration, or the Transportation Security Administration, or any expense in enforcing any Federal regulations, including, but not limited to, airport security regulations, or the rules or regulations of County, and/or any expense in enforcing County's Airport Security Program, then Provider shall pay and/or reimburse to County all such costs and expenses, including all costs of administrative proceedings, court costs, and attorney's fees and all costs incurred by County in enforcing this provision. Provider shall rectify any security deficiency or other deficiency as may be determined as such by County or the United States Department of Transportation, Federal Aviation Administration, the Transportation Security Administration, or any other Federal agency with jurisdiction. In the event Provider fails to remedy any such deficiency, County may do so at the sole cost and expense of Provider. County reserves the right to take whatever action is necessary to rectify any security deficiency or other deficiency.

(a) Access to Security Identification Display Areas and Identification Media. Provider shall be responsible for requesting the Aviation Department to issue Airport Issued Identification Media to all employees including those who are authorized access to Security Identification Display Areas ("SIDA") on the Airport, as designated in the Airport Security Program. In addition, Provider shall be responsible for the immediate reporting of all lost or stolen Airport Issued Identification Media and the immediate return of the media of Provider's personnel transferred from the Airport, or terminated from the employ of Provider, or upon termination of this Agreement. Before an Airport Issued Identification Media is issued to an employee, Provider shall comply with the requirements of applicable Federal regulations with regard to fingerprinting for criminal history record checks and security threat assessments, and shall require that each employee complete security training programs conducted by the Aviation Department. Provider shall pay or cause to be paid to the Aviation Department such charges as may be established from time to time for lost or stolen Airport Issued Identification Media and those not returned to the Aviation Department in accordance with these provisions. The Aviation Department shall have the right to require Provider to conduct background investigations and to furnish certain data on such

employees before the issuance of Airport Issued Identification Media, which data may include the fingerprinting of employee applicants for such media.

(b) Operation of Vehicles on the AOA: Before Provider shall permit any employee of Provider or of any Subcontractor to operate a motor vehicle of any kind or type on the AOA (and unless escorted by an Aviation Department approved escort), Provider shall ensure that all such vehicle operators possess current, valid, and appropriate Florida driver's licenses. In addition, any motor vehicles and equipment of Provider or of any Subcontractor operating on the AOA must have an appropriate vehicle identification permit issued by the Aviation Department, which identification must be displayed as required by the Aviation Department.

(c) Consent to Search/Inspection: Provider's vehicles, cargo, goods, and other personal property are subject to being inspected and searched when attempting to enter or leave and while on the AOA. Provider and its Subcontractor shall not authorize any employee or other person to enter the AOA unless and until such employee or other person has executed a written consent-to-search/inspection form acceptable to the Aviation Department. The foregoing requirements are for the protection of users of the Airport and are intended to reduce incidents of cargo tampering, aircraft sabotage, thefts and other unlawful activities at the Airport. For this reason, persons not executing such consent-to-search/inspection form shall not be employed by Provider or by any Subcontractor at the Airport in any position requiring access to the AOA or allowed entry to the AOA by Provider or by any Subcontractor.

(d) If any of Provider's employees, or the employees of any of its Subcontractors, are required in the course of the work to be performed under this Agreement to access or otherwise be in contact with Sensitive Security Information ("SSI") as defined and construed under Federal law, that individual will be required to execute a Sensitive Security Information Non-Disclosure Agreement promulgated by the Aviation Department.

(e) The provisions of this exhibit shall survive the expiration or any other termination of this Agreement.

(THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK.)