

# MEMORANDUM

Agenda Item No. 8(P)(1)


**TO:** Honorable Chairman Oliver G. Gilbert, III  
and Members, Board of County Commissioners

**DATE:** March 19, 2024

**FROM:** Geri Bonzon-Keenan  
County Attorney

**SUBJECT:** Resolution approving award of Contract No. RFP-02194 to Securus Technologies, LLC for the purchase of a Detainee Electronic Communication and Media Solution for the Miami-Dade Corrections and Rehabilitation Department in a total amount not to exceed \$10,000,000.00 for the initial five-year term and one, five-year option to renew, should the County elect to purchase optional services; and authorizing the County Mayor to execute same for and on behalf of Miami-Dade County, and to exercise all provisions of the contract, including any renewal, cancellation, or extensions, pursuant to section 2-8.1 of the Code and Implementing Order 3-38

The accompanying resolution was prepared by the Strategic Procurement Department and placed on the agenda at the request of Prime Sponsor Commissioner Kionne L. McGhee.

  
\_\_\_\_\_  
Geri Bonzon-Keenan  
County Attorney

GBK/ks

MDC001

# Memorandum



**Date:** March 19, 2024

**To:** Honorable Chairman Oliver G. Gilbert, III  
and Members, Board of County Commissioners

**From:** Daniella Levine Cava *Daniella Levine Cava*  
Mayor

**Subject:** Recommendation for Approval to Award Detainee Electronic Communication and Media Solution

---

## **Summary**

This item is recommending award of a competitive contract for the provision of a communication and media solution, inclusive of tablets and kiosks, on behalf of the Miami-Dade Corrections and Rehabilitation Department (MDCR), to be used by detainees in Miami-Dade County correctional facilities. Tablets and kiosks will facilitate communication with family, friends, and legal representatives and provide access to an increased array of educational courses and material to prepare them for a successful re-entry into society, as well as offering various forms of entertainment media to keep detainees occupied in safe and positive activities to increase facility safety for detainees and staff.

The scope of services for this enterprise-wide solution will provide for detainee kiosks, infrastructure and related equipment, software, and services, at no cost to the County, except for options offered by the contractor, for the benefit of the County. Detainees will be charged a nominal fee for communication offered via tablets and kiosks for phone calls, video calls, and outgoing electronic messages that exceed the free communication amounts offered through the tablets. Additionally, there will be optional fees for entertainment media, i.e., music, movies, books/magazines, and games. The services offered at no charge to rule abiding detainees include up to 90 minutes of phone calls per day; two hours of video visitation per week; five outgoing electronic messages per week; unlimited receipt of electronic personal and privileged mail, and unlimited phone calls with their Attorneys.

One of the goals of the project is to transition the agency from a paper-based format to a modernized digital environment that will provide: a) uninterrupted access to all detainee service requests such as medical, legal, faith based, etc.; b) a positive impact on the environment through a reduction of paper usage; and c) less physical property to safeguard, search, and transport, reducing fire hazards in the facilities.; Additionally, it is anticipated that the engagement of detainees in new technology to positively occupy their time while incarcerated will also lead to a reduction in institutional violence, providing a more positive environment for rehabilitation and a reduction in recidivism through increased programs, education, training, possible job placement and overall improvement in the conditions of confinement within Miami Dade County facilities.

## **Recommendation**

It is recommended that the Board of County Commissioners (Board) approve a competitive contract award, Contract No. RFP-02194, Detainee Electronic Communication and Media Solution to Securus Technologies, LLC (Securus), for MDCR in the cumulative amount of \$10,000,000 for a five-year contract with one, five-year option to renew, should the County elect to purchase optional services from Securus. There is no existing nor any prior contract for the provision of the recommended enterprise-wide solution.

## **Background**

A Request for Proposals (RFP) was issued under full and open competition on April 6, 2022, and the solicitation closed on May 26, 2022. Three proposals were received on the closing date and were forwarded to the County Attorney's Office (CAO) for review on June 2, 2022. The CAO issued a legal opinion dated August 23, 2022, and deemed two proposals non-responsive. The kick-off meeting was

held and evaluation meetings were conducted between June and September 2022. Negotiations commenced in November 2022 and concluded in August 2023. A total of 11 negotiation and internal strategy meetings with staff and the recommended proposer were held to reach consensus on the final contract terms including, but not limited to, scope of work, delivery of services, and terms for payment.

The RFP was issued to obtain a solution to help bridge the gap between incarcerated citizens and the community. This includes removing the financial burden on many of the families of incarcerated individuals by providing significant amounts of daily phone time, video visits, and other services at zero cost to the detainee, their families, or the County, as studies have shown that the success rate of returning citizens from incarceration are significantly higher when they maintain connections to the community. As such, the County will not collect commissions from revenues generated through the resulting contract to further this goal. This will alleviate many families, friends, and loved ones, already facing disproportionate amounts of financial inequity in marginalized communities, from having to subsidize county operations and strengthen their community connections, while ensuring that the County achieve the lowest possible rates on all services.

The terms of the resultant contract were extensively negotiated, resulting in favorable provisions for the County and incarcerated citizens. In addition to the no-cost provisions, the contract includes four value added contract options to be evaluated by the County, that may provide benefit for the County as follows:

1. Guarded Exchange Monitoring Services (Telephone) - Telephone Monitoring and Reporting at \$.02 per minute for the monitoring of five percent of the total call volume at \$400,000 per year.
2. Guarded Exchange Monitoring Services (Video Visitation) - Telephone Monitoring and Reporting at \$.02 per minute for monitoring of five percent of the total call volume at \$400,000 per year.
3. Word Alert and iPRO - Full investigative suite of both applications at \$150,000 per year.
4. Behavioral Reward Program - This program will enable detainees to earn credits to purchase premium items based on a behavior award system and the completion of educational material, as structured in the plan, at \$50,000 per year.

**Scope**

The scope of this item is countywide in nature.

**Fiscal Impact/Funding Source**

There are no costs to the County during the initial five-year term or the one, five-year option to renew term. Should the County elect to purchase the optional services, the fiscal impact would be up to \$5,000,000 for the initial term, and should the County choose to exercise, at its sole discretion, the option to renew term and continue purchasing optional services, the cumulative value would be up to \$10,000,000.

Department	Allocation	Funding Source	Contract Manager
MDCR	\$10,000,000	General Fund/Inmate Welfare Fund	Christopher Moreno
<b>Total</b>	<b>\$10,000,000</b>		

**Track Record/Monitor**

Vanessa Stroman of the Strategic Procurement Department (SPD) is the Procurement Contracting Manager.

**Delegated Authority**

If this item is approved, the County Mayor or County Mayor's designee will have the authority to execute the agreement and exercise all provisions of the contract, including any cancellation, renewal, or extensions, pursuant to Section 2-8.1 of the County Code and Implementing Order 3-38.

**Vendor Recommended for Award**

A Request for Proposals was issued under full and open competition, and three proposals were received in response to the solicitation. Pursuant to Resolution No. R-477-18, the sole responsive proposer is recommended in accordance with the method of award per the solicitation and is non-local. There were no local vendors identified by SPD during market research. The Office of Small Business Development identified three certified Small Business Enterprise (SBE) firms with the associated commodity codes; however, none of the firms had the ability to meet project requirements.

Vendor	Principal Address	Local Address	Number of Employee Residents	Principal
			1) Miami-Dade 2) Percentage*	
Securus Technologies, LLC	1800 NW 69 Avenue Suite 201 Plantation, FL	None	0	Daniel Boron
			0%	

\*Provided pursuant to Resolution No. R-1011-15. Percentage of employee residents is the percentage of vendor's employees who reside in Miami-Dade County as compared to the vendor's total workforce.

**Vendors Not Recommended for Award**

Vendor	Local Address	Reason for Not Recommending
Global Tel*Link Corporation d/b/a ViaPath Technologies	No	Deemed non-responsive by the CAO for failing to propose in accordance with the terms of the RFP (opinion attached)
Veterans Technology Systems, LLC	No	

**Due Diligence**

Pursuant to Resolution No. R-187-12, due diligence was conducted in accordance with SPD's Procurement Guidelines to determine vendor responsibility, including verifying corporate status and that there are no performance and compliance issues through various vendor responsibility lists and a keyword internet search. The lists that were referenced included convicted vendors, debarred vendors, delinquent contractors, suspended vendors, and federal excluded parties. There were no adverse findings relating to vendor responsibility.

**Applicability of Ordinances and Contract Measures**

- The two percent User Access Program does not apply.
- The SBE Selection Factor and Local Preference were included in the solicitation.
- The Living Wage Ordinance does not apply.

Attachment



James Reyes  
 Chief of Public Safety

**Date:** August 23, 2022

**To:** Brian Webster  
Procurement Contracting Officer 2  
Internal Services Department

**From:** Oren Rosenthal  
Assistant County Attorney

**Subject:** RFP-02194, Detainee Communications and Media Solution

---

You have asked this office if the proposals submitted by Veterans Technology Systems (“Veterans”), Global Tel\*Link Corporation d/b/a ViaPath Technologies (“ViaPath”), and Securus Technologies, LLC (“Securus”) can be considered responsive to the above Request for Proposals (“RFP”) for the provision of detainee communications and media solutions at County detention facilities at no cost to Miami-Dade County (“County”). For the reasons set forth below, we conclude that Veterans and ViaPath’s proposals are not responsive to the RFP and may not be awarded this solicitation as a competitive contract award. Securus, on the other hand, is responsive and is eligible for award.

## FACTS

We rely on the information provided in your e-mail dated June 2, 2022 to the County Attorney’s Office, subsequent conversations and e-mails received by the administration, the relevant provisions of the RFP and the various proposal documents referenced in your request. If any of the underlying facts change or additional analysis is requested, please let us know and we will provide an updated opinion.

The County issued the RFP on April 6, 2022, to solicit proposals for a contract with MDCR to provide in-custody detainees with an electronic communication and media solution through tablets, mobile kiosks, and stationary kiosks that utilize touchscreen as the primary input device. The Contractor was required to provide all required equipment, hardware, software licenses, implementation, interface development, configuration, training, hosting, and maintenance and support services, throughout the duration of the awarded contract. Critically, the RFP made clear that the equipment and services be provided at no cost to the County. *See*, Attachment A, Scope of Services, Section 3.0 (“Purpose Contractor shall provide all detainee kiosks, infrastructure and related equipment, software, and services at no cost to the County.”); Price Proposal Form (indicating all services to be provided at “no charge”).

The County received three proposals in response to the RFP prior to the closing date. Upon your review of the proposals, you report the following issues regarding the proposals:

- Veterans omitted the Proposal Price Schedule from their submission and did not prepare a proposal response in accordance with Section 5.0 of the RFP document.
- ViaPath included as part of their price proposal the following statements: “[a]ssumes a monthly revenue guarantee of \$375,000 gross contract revenue is met from all services contained in Table B1-B4 and Table C. Should revenue in any given month be less than the defined monthly guarantee, a reimbursement for the difference from the County will

be required” and “[i]f mail volume exceeds 3 pieces per inmate per month, Miami-Dade would be charged \$2.25 per piece of mail above that threshold. Scanned mail will be delivered to the tablet/kiosk.” These statements were inserted in the narrative assumption section next to the price proposal that indicated “no charge” for these services.

- Securus included as part of their price proposal the following statement: “To support the volume of free minutes, and to include all of the additional technology required, Securus respectfully requests that MDCR engage the renewal term years after year one. Securus is willing to be flexible to meet all of the stated requirements, but due to the upfront capital costs, and limited amount of revenue generated initially, these renewal years are necessary to make the agreement self sustaining.”

## DISCUSSION

As a general rule a bid will be found not responsive if it materially differs from the proposals requested by the solicitation. The determination of whether a proposal’s variance from the solicitation is minor or material is fact specific and may differ from proposal to proposal. Florida courts have used a two part test to determine if a specific noncompliance in a proposal would constitute a substantial and, thus, nonwaivable issue: (1) whether the effect of the waiver would be to deprive the County of the assurance that the contract would be entered into, performed and guaranteed according to its specific requirements; and (2) whether it would adversely affect competitive bidding by placing a proposer in a position of advantage over other proposers. *See, e.g., Robinson Elec. Co., Inc. v. Dade County*, 417 So. 2d 1032, 1034 (Fla. 3d DCA 1982).

Although Veterans’ submitted a proposal submittal form and some portions of the requested proposal, Veterans failed to submit any pricing and otherwise submit a proposal in accordance with terms of the RFP. Such a deviation deprives the County of any assurance that the proposal will result in a contract that will be entered into, performed, and guaranteed in accordance with the RFP’s requirements. This is particularly true here, where the price proposal form required all proposers to: (1) confirm that the provision of the services requested by the RFP must be provided at “no charge” and; (2) propose pricing for services to inmates that will be considered and assigned points in the RFP evaluation. Veterans’ failure to include that commitment and any pricing information in its proposal renders the proposal not responsive.

ViaPath’s offer to the County similarly deprives the County with the assurance that the proposal will result in a contract in accordance with the material terms of the RFP and, if permitted, would allow ViaPath a significant advantage over other proposers. By requiring all proposals to agree to provide the equipment and services requested in the RFP at “no cost to the County,” the County is shifting all risk associated with providing the equipment and services to the proposer with the compensation to be derived wholly from non-County sources. Notwithstanding this essential element of the Solicitation, ViaPath’s explicitly states that “a reimbursement ... from the County will be **required**” (emphasis added) if a minimum monthly revenue guarantee from inmates is not realized. Although contained in a section reserved for assumptions, this condition is not worded as an assumption underlying their proposal but rather as an express repudiation of the fixed price of no charge to the County required in the solicitation. ViaPath could have, but did not, phrase this statement as a request to negotiate on this issue. Rather, the wording used by ViaPath intentionally conditions its “no cost” proposal on the acceptance of this criteria, which clearly establishes a cost that is not permissible by the express terms of the Solicitation and not available to other proposers who proposed in accordance with the document.

Allowing a proposer to differ from this requirement after proposal submittal would provide a huge advantage over any other proposer or any potential proposer and is a material deviation from the specifications of the RFP. *See, e.g., Matter of: Billsmart Sols., LLC*, B-413272.4, 2017 WL 4804008, \*11 (Comp. Gen. Oct. 23, 2017) (“A proposal that takes exception to a solicitation's material terms and conditions must be considered unacceptable for award. ... Where a solicitation requests offers on a fixed-price basis, an offer that is conditional and not firm cannot be considered for award.”).

Securus’ proposal, on the other hand, does not present such a material deviation because it does not contain a similar rejection of the Solicitation. Rather than condition its proposal on a specific act by the County, Securus merely “respectfully requests that MDCR engage the renewal term years after year one” and informs the County of the financial hardship it may experience should the County end the awarded contract before the term and any extensions thereto. Such a request is not a conditional proposal but merely provides the requested information to allow the County to evaluate the assumptions underlying the proposal and potential issues that may arise with the contract. Such evaluation may be considered in the course of the County’s responsibility review of the vendor but it does not render the proposal non-responsive.

Accordingly, for the reasons stated above, Veterans and ViaPath’s proposals are not responsive to the RFP and may not be awarded. Securus is responsive and is eligible for award.



---

Oren Rosenthal



**MEMORANDUM**  
(Revised)

**TO:** Honorable Chairman Oliver G. Gilbert, III  
and Members, Board of County Commissioners

**DATE:** March 19, 2024

**FROM:**   
Gen Bonzon-Keenan  
County Attorney

**SUBJECT:** Agenda Item No. 8(P)(1)

Please note any items checked.

- "3-Day Rule" for committees applicable if raised
- 6 weeks required between first reading and public hearing
- 4 weeks notification to municipal officials required prior to public hearing
- Decreases revenues or increases expenditures without balancing budget
- Budget required
- Statement of fiscal impact required
- Statement of social equity required
- Ordinance creating a new board requires detailed County Mayor's report for public hearing
- No committee review
- Applicable legislation requires more than a majority vote (i.e., 2/3's present \_\_\_\_, 2/3 membership \_\_\_\_, 3/5's \_\_\_\_, unanimous \_\_\_\_, CDMP 7 vote requirement per 2-116.1(3)(h) or (4)(c) \_\_\_\_, CDMP 2/3 vote requirement per 2-116.1(3)(h) or (4)(c) \_\_\_\_, or CDMP 9 vote requirement per 2-116.1(4)(c)(2) \_\_\_\_ ) to approve
- Current information regarding funding source, index code and available balance, and available capacity (if debt is contemplated) required

Approved \_\_\_\_\_ Mayor  
Veto \_\_\_\_\_  
Override \_\_\_\_\_

Agenda Item No. 8(P)(1)  
3-19-24

RESOLUTION NO. \_\_\_\_\_

RESOLUTION APPROVING AWARD OF CONTRACT NO. RFP-02194 TO SECURUS TECHNOLOGIES, LLC FOR THE PURCHASE OF A DETAINEE ELECTRONIC COMMUNICATION AND MEDIA SOLUTION FOR THE MIAMI-DADE CORRECTIONS AND REHABILITATION DEPARTMENT IN A TOTAL AMOUNT NOT TO EXCEED \$10,000,000.00 FOR THE INITIAL FIVE-YEAR TERM AND ONE, FIVE-YEAR OPTION TO RENEW, SHOULD THE COUNTY ELECT TO PURCHASE OPTIONAL SERVICES; AND AUTHORIZING THE COUNTY MAYOR OR COUNTY MAYOR'S DESIGNEE TO EXECUTE SAME FOR AND ON BEHALF OF MIAMI-DADE COUNTY, AND TO EXERCISE ALL PROVISIONS OF THE CONTRACT, INCLUDING ANY RENEWAL, CANCELLATION, OR EXTENSIONS, PURSUANT TO SECTION 2-8.1 OF THE CODE OF MIAMI-DADE COUNTY, FLORIDA AND IMPLEMENTING ORDER 3-38

**WHEREAS**, this Board desires to accomplish the purposes outlined in the accompanying memorandum, a copy of which is incorporated herein by reference,

**NOW, THEREFORE, BE IT RESOLVED BY THE BOARD OF COUNTY COMMISSIONERS OF MIAMI-DADE COUNTY, FLORIDA**, that:

**Section 1.** This Board approves award of Contract No. RFP-02194 to Securus Technologies, LLC, in substantially the form attached and made a part hereof, for the purchase of a Detainee Electronic Communication and Media Solution for the Miami-Dade Corrections and Rehabilitation Department in a total amount not to exceed \$10,000,000.00 for the initial five-year term and one, five-year option to renew, should the County elect to purchase optional services.

**Section 2.** This Board authorizes the County Mayor or County Mayor's designee to exercise all provisions of the contract, including any renewal, cancellation, or extensions, pursuant to section 2-8.1 of the Code of Miami-Dade County, Florida and Implementing Order 3-38.

The foregoing resolution was offered by Commissioner ,  
who moved its adoption. The motion was seconded by Commissioner  
and upon being put to a vote, the vote was as follows:

Oliver G. Gilbert, III, Chairman	
Anthony Rodríguez, Vice Chairman	
Marleine Bastien	Juan Carlos Bermudez
Kevin Marino Cabrera	Sen. René García
Roberto J. Gonzalez	Keon Hardemon
Danielle Cohen Higgins	Eileen Higgins
Kionne L. McGhee	Raquel A. Regalado
Micky Steinberg	

The Chairperson thereupon declared this resolution duly passed and adopted this 19<sup>th</sup> day of March, 2024. This resolution shall become effective upon the earlier of (1) 10 days after the date of its adoption unless vetoed by the County Mayor, and if vetoed, shall become effective only upon an override by this Board, or (2) approval by the County Mayor of this resolution and the filing of this approval with the Clerk of the Board.

MIAMI-DADE COUNTY, FLORIDA  
BY ITS BOARD OF  
COUNTY COMMISSIONERS

JUAN FERNANDEZ-BARQUIN, CLERK

By: \_\_\_\_\_  
Deputy Clerk

Approved by County Attorney as  
to form and legal sufficiency.



Angela F. Benjamin

DETAINEE COMMUNICATIONS AND MEDIA SOLUTION  
CONTRACT NO. RFP-02194

THIS AGREEMENT for the provision of specified detainee communication and media services, made and entered into as of this \_\_\_\_\_ day of \_\_\_\_\_, 2023 by and between Securus Technologies, LLC, a corporation organized and existing under the laws of the State of Delaware, having its principal office at 4000 International Parkway, Carrollton TX 75007 (the "Contractor"), and Miami-Dade County, a political subdivision of the State of Florida, having its principal office at 111 NW 1st Street, Miami, Florida 33128 (the "County") (collectively, the "Parties").

WITNESSETH:

WHEREAS, the Contractor has offered to provide a Detainee Communications and Media Solution ("Solution"), on an exclusive basis to the extent set forth in Article 17(g) below, that shall conform to the Scope of Works ("Attachment A"), Miami-Dade County's Request for Proposal (RFP) No. 02194 and all associated addenda and attachments, and the requirements of this Agreement; and

WHEREAS, the Contractor has submitted a written proposal dated May 26, 2022 (the "Contractor's Proposal") which is incorporated herein by reference; and

WHEREAS, the County desires to procure from the Contractor such Detainee Communications and Media Solution for the County, in accordance with the terms and conditions of this Agreement;

## Table of Contents

ARTICLE 1	DEFINITIONS .....	4
ARTICLE 2	ORDER OF PRECEDENCE .....	4
ARTICLE 3	RULES OF INTERPRETATION.....	4
ARTICLE 4	NATURE OF THE AGREEMENT.....	5
ARTICLE 5	CONTRACT TERM.....	5
ARTICLE 6	EXTENSION OF TIME .....	6
ARTICLE 7	EXTENSION OF TIME NOT CUMULATIVE.....	7
ARTICLE 8	FORCE MAJEURE .....	7
ARTICLE 9	EXCUSABLE DELAY .....	7
ARTICLE 10	EXTRA WORK.....	8
ARTICLE 11	CHANGE ORDER BASIS FOR PAYMENT .....	8
ARTICLE 12	NOTICE REQUIREMENTS.....	8
ARTICLE 13	FINANCIAL STRUCTURE.....	9
ARTICLE 14	SOLUTION AVAILABILITY .....	10
ARTICLE 15	PAYMENT FOR SERVICES/AMOUNT OBLIGATED .....	10
ARTICLE 16	INDEMNIFICATION AND INSURANCE .....	10
ARTICLE 17	MANNER OF PERFORMANCE .....	12
ARTICLE 18	SOCIAL/FAIR LABOR STANDARDS .....	12
ARTICLE 19	SUSTAINABLE PROCUREMENT PRACTICES .....	12
ARTICLE 20	EMPLOYEES OF THE CONTRACTOR .....	13
ARTICLE 21	INDEPENDENT CONTRACTOR RELATIONSHIP .....	13
ARTICLE 22	DISPUTE RESOLUTION PROCEDURE .....	13
ARTICLE 23	MUTUAL OBLIGATIONS .....	14
ARTICLE 24	QUALITY ASSURANCE/QUALITY ASSURANCE RECORD KEEPING .....	14
ARTICLE 25	AUDITS.....	14
ARTICLE 26	SUBSTITUTION OF PERSONNEL.....	14
ARTICLE 27	CONSENT OF THE COUNTY REQUIRED FOR ASSIGNMENT .....	14
ARTICLE 28	SUBCONTRACTUAL RELATIONS.....	14
ARTICLE 29	ASSUMPTION, PARAMETERS, PROJECTIONS, ESTIMATES AND EXPLANATIONS.....	15
ARTICLE 30	SEVERABILITY .....	15
ARTICLE 31	TERMINATION AND SUSPENSION OF WORK.....	15
ARTICLE 32	EVENT OF DEFAULT .....	16
ARTICLE 33	NOTICE OF DEFAULT - OPPORTUNITY TO CURE.....	17
ARTICLE 34	REMEDIES IN THE EVENT OF DEFAULT .....	17
ARTICLE 35	EQUIPMENT .....	17
ARTICLE 36	GRANT OF LICENSE .....	18
ARTICLE 37	DELIVERY .....	18
ARTICLE 38	MAINTENANCE AND TECHNICAL SUPPORT SERVICES.....	18

ARTICLE 39 PROTECTION OF SOFTWARE..... 18

ARTICLE 40 SOFTWARE MODIFICATIONS ..... 18

ARTICLE 41 IMPLEMENTATION SERVICES ..... 19

ARTICLE 42 TESTS ..... 20

ARTICLE 43 BUSINESS CONTINUITY AND DISASTER RECOVERY ..... 20

ARTICLE 44 SOLUTION WARRANTY ..... 20

ARTICLE 45 DATA STORAGE SPACE ..... 20

ARTICLE 46 THIRD PARTY WARRANTY ..... 20

ARTICLE 47 FUNCTIONALLY EQUIVALENT SOFTWARE..... 21

ARTICLE 48 PATENT AND COPYRIGHT INDEMNIFICATION ..... 21

ARTICLE 49 CONFIDENTIALITY ..... 21

ARTICLE 50 PROPRIETARY INFORMATION ..... 22

ARTICLE 51 PROPRIETARY RIGHTS..... 22

ARTICLE 52 VENDOR REGISTRATION/CONFLICT OF INTEREST ..... 23

ARTICLE 53 INSPECTOR GENERAL REVIEWS ..... 24

ARTICLE 54 FEDERAL, STATE, AND LOCAL COMPLIANCE REQUIREMENTS..... 25

ARTICLE 55 NONDISCRIMINATION ..... 26

ARTICLE 56 CONFLICT OF INTEREST..... 26

ARTICLE 57 PRESS RELEASE OR OTHER PUBLIC COMMUNICATION..... 27

ARTICLE 58 BANKRUPTCY ..... 27

ARTICLE 59 GOVERNING LAW ..... 27

ARTICLE 60 INTEREST OF MEMBERS, OFFICERS OR EMPLOYEES AND FORMER MEMBERS, OFFICERS OR EMPLOYEES..... 27

ARTICLE 61 LIENS..... 27

ARTICLE 62 FIRST SOURCE HIRING REFERRAL PROGRAM..... 27

ARTICLE 63 PUBLIC RECORDS AND CONTRACTS FOR SERVICES PERFORMED ON BEHALF OF MIAMI-DADE COUNTY..... 28

ARTICLE 64 VERIFICATION OF EMPLOYMENT ELIGIBILITY (E-VERIFY)..... 28

ARTICLE 65 ADDITIONAL LICENSES, SOFTWARE, OR SERVICES ..... 28

ARTICLE 66 CRIMINAL JUSTICE INFORMATION SYSTEMS SECURITY REQUIREMENTS ..... 28

ARTICLE 67 CYBERSECURITY AND INFORMATION TECHNOLOGY PROCUREMENT AND PROTECTION PROGRAM ..... 29

ARTICLE 68 TRANSITION ..... 29

ARTICLE 69 SURVIVAL..... 29

NOW, THEREFORE, in consideration of the mutual covenants and agreements herein contained, the Parties hereto agree as follows:

## **ARTICLE 1**      **DEFINITIONS**

The following words and expressions used in this Agreement shall be construed as follows, except when it is clear from the context that another meaning is intended:

- a) The words "Article" or "Articles" to mean the terms and conditions delineated in this Agreement.
- b) The word "Contract" or "Agreement" to mean collectively the (i) Articles, (ii) Scope of Work, (iii) Price Schedule, (iv) all other appendices and attachments hereto, and (v) all amendments issued hereto, and Contractor's Proposal.
- c) The words "Contract Manager" to mean the Director, Internal Services Department, or the duly authorized representative designated to manage the Contract.
- d) The word "Contractor" to mean Securus Technologies, LLC and its permitted successors.
- e) The word "Days" to mean calendar days.
- f) The word "Deliverables" to mean all documentation and any items of any nature submitted by the Contractor to the Project Manager for review and approval pursuant to the terms of this Agreement.
- g) The words "Developed Works" to mean all rights, title, and interest in and to certain inventions, ideas, designs and methods, specifications and other documentation related thereto developed by the Contractor and its Subcontractors specifically for the County.
- h) The words "Licensed Software" to mean the software component(s) provided pursuant to the Contract.
- i) The words "Project Manager" to mean the County Mayor or the duly authorized representative designated to manage the Project.
- j) The words "Scope of Work" to mean the document appended hereto as Attachment A, which details the Work to be performed by the Contractor.
- k) The words "Service", "Work", or "Services" to mean the provision of Detainee Communications and Media services in accordance with the Scope of Works.
- l) The word "Subcontractor" or "Subconsultant" to mean any person, entity, firm, or corporation, other than the employees of the Contractor, who furnishes labor and/or materials, in connection with the Work, whether directly or indirectly, on behalf and/or under the direction of the Contractor and whether or not in privity of Contract with the Contractor.
- m) The word "Work" to mean all matters and things required to be done by the Contractor in accordance with the provisions of this Contract.

## **ARTICLE 2**      **ORDER OF PRECEDENCE**

If there is a conflict between or among the provisions of the Contract, the order of precedence is as follows: 1) the Form of Agreement; 2) agreed upon Scope of Work (as may be negotiated); 3) addenda to the RFP; 4) attachments to the Request for Proposal; 4) the Request for Proposal; and 5) the Contractor's Proposal, which is incorporated herein as if fully set forth.

## **ARTICLE 3**      **RULES OF INTERPRETATION**

- a) References to a specified Article, section or schedule shall be construed as reference to that specified Article, or section

of, or schedule to this Agreement unless otherwise indicated.

- b) Reference to any agreement or other instrument shall be deemed to include such agreement or other instrument as such agreement or other instrument may, from time to time, be modified, amended, supplemented, or restated in accordance with its terms.
- c) The terms "hereof", "herein", "hereinafter", "hereby", "herewith", "hereto", and "hereunder" shall be deemed to refer to this Agreement.
- d) The terms "directed", "required", "permitted", "ordered", "designated", "selected", "prescribed" or words of like import to mean respectively, the direction, requirement, permission, order, designation, selection or prescription of the Project Manager.
- e) The terms "approved", "acceptable", "satisfactory", "equal", "necessary", or words of like import to mean respectively, approved by, or acceptable or satisfactory to, equal or necessary in the opinion of the Project Manager.
- f) The titles, headings, captions, and arrangements used in these Terms and Conditions are for convenience only and shall not be deemed to limit, amplify, or modify the terms of this Contract, nor affect the meaning thereof.

#### **ARTICLE 4      NATURE OF THE AGREEMENT**

- a) This Agreement incorporates and includes all prior negotiations, correspondence, conversations, agreements, and understandings applicable to the matters contained in this Agreement. The Parties agree that there are no commitments, agreements, or understandings concerning the subject matter of this Agreement that are not contained in this Agreement, and that this Agreement contains the entire agreement between the Parties as to all matters contained herein. Accordingly, it is agreed that no deviation from the terms hereof shall be predicated upon any prior representations or agreements, whether oral or written. It is further agreed that any oral representations or modifications concerning this Agreement shall be of no force or effect, and that this Agreement may be modified, altered, or amended only by a written amendment duly executed by the Parties hereto or their authorized representatives.
- b) The Contractor shall provide the services set forth in the Scope of Works and render full and prompt cooperation with the County in all aspects of the Work performed hereunder.
- c) The Contractor acknowledges that this Agreement requires the performance of all things necessary for or incidental to the effective and complete performance of all Work under this Contract. All things not expressly mentioned in this Agreement but necessary to carrying out its intent are required by this Agreement, and the Contractor shall perform the same as though they were specifically mentioned, described, and delineated.
- d) The Contractor shall furnish all labor, materials, tools, supplies, and other items required to perform the Work necessary for the completion of this Contract. All Work shall be accomplished at the direction of and to the satisfaction of the Project Manager.
- e) The Contractor acknowledges that the County shall make all policy decisions regarding the Scope of Works. The Contractor agrees to provide input on policy issues in the form of recommendations. The Contractor shall implement all reasonable changes in providing services hereunder as a result of a policy change implemented by the County, which do not constitute a material change to the Scope of Work. The Contractor agrees to act in an expeditious and fiscally sound manner in providing the County with input regarding the time and cost to implement said changes and in executing the activities required to implement said changes.

#### **ARTICLE 5      CONTRACT TERM**

The Contract shall become effective on the date of the Parties' execution, whichever is later, and shall continue through the last day of the sixtieth (60) month, thereafter. The County, at its sole discretion, may renew this Contract for one (1), five (5) year option to renew term. The County may extend this Contract for up to an additional one hundred-eighty (180) calendar days beyond the current Contract period and will notify the Contractor in writing of the extension. This Contract may be

extended beyond the initial one hundred-eighty (180) calendar day extension period by mutual agreement between the County and the Contractor, upon approval by the Board of County Commissioners (the "Board").

## **ARTICLE 6      EXTENSION OF TIME**

- a) If the Contractor is delayed at any time hereunder due to any of the following then the affected schedule or the required performance of Work may be extended by the County in the reasonable exercise of its discretion for such reasonable time as the County may determine, subject to the following conditions:
  - i. In accordance with the provisions of the Article titled, *Force Majeure*, the cause of the delay is beyond the Contractor's control and arises without its fault or negligence, and arises after the execution hereof and neither was nor could have been anticipated by the Contractor by reasonable investigation; and
  - ii. The completion of the Work will be actually and necessarily delayed by the causes set forth in "i" above; and
  - iii. The effect of such cause cannot be avoided or mitigated by the exercise of all reasonable precautions, efforts and measures whether before or after the occurrence of the cause of delay; and
  - iv. The Contractor has provided a written request and other information to the County, as described in subsection 17.4 below, within ten (10) days after the time the Contractor knows or reasonably should have known of any cause which might result in a delay for which the Contractor may request an extension of time (the "Delay Notice"). The Contractor shall specifically state in such Delay Notice that an extension is or may be requested and identify the cause of the delay, describing the nature and its effect on the completion of the affected portions of the Work identified in the Delay Notice. If the Contractor fails to give the Delay Notice timely, the right to request an extension for such cause shall be waived.
- b) All references in this Article to the Contractor shall be deemed to include Subcontractors and suppliers, all of whom shall be considered as agents of the Contractor.
- c) The period of any extension of time shall be only that which is necessary to make up the time actually lost. The County reserves the right to rescind or shorten any extension previously granted if the County subsequently determines that any information provided by the Contractor in support of its request for an extension of time was erroneous or that there has been a material change in the facts stated.
- d) The County may require the Contractor to furnish such additional information or documentation, as the County shall reasonably deem necessary or helpful in considering an extension request. The Contractor understands an extension of time will not be granted unless the Contractor affirmatively demonstrates to the County's reasonable satisfaction that the circumstances shown justify such extension.
- e) Within thirty (30) days of its receipt of all information and documentation as may be required by the County, the County shall advise the Contractor of its decision on such requested extension. Notwithstanding the foregoing, where it is not reasonably practicable for the County to render its decision within such thirty (30) day period, it shall, prior to the expiration of such period, advise the Contractor that it will require additional time and the approximate date upon which it expects to render such decision.
- f) Since the granting of an extension of time may materially alter the scheduling plans and other actions of the County and since, with sufficient notice, the County might, if it should so elect, attempt to mitigate the effect of the delay for which an extension of time might be claimed, and since mere oral notice may cause a dispute as to the existence or substance thereof, the giving of written notice as required in subsection (17.1)(iv) above shall be a condition precedent to the Contractor's rights hereunder.
- g) Should any person seek a restraining order, preliminary injunction or an injunction, of which the Contractor becomes aware, which may delay the Work, configuration, installation, or delivery of the Solution, the Contractor shall promptly give

the County a copy of all legal papers received or prepared or received by the Contractor in connection with such action or proceeding.

- h) Neither permitting the Contractor to proceed with the Work subsequent to any missed schedule or performance of any Work (as such date may have been extended pursuant to Article 7 "Extension of Time Not Cumulative"), nor the making of any payments to the Contractor shall compromise the County's contractual right to delay of payment as outlined within Attachment B, *Price and Payment Schedule*, or to declare the Contractor in default.
- i) County Extension of Time. The County may exercise upon reasonable notice to the Contractor, an extension of time not to exceed one hundred-eighty (180) calendar days, in accordance with Article 5, to complete any County responsibility outlined within the Scope of Works, within the limits set forth by Article. This notification shall include information as to the need for the extension and the anticipated date of completion. Contractor hereby agrees to make no claim for damages for the extension, whether contemplated or not contemplated, and agrees that any such claim shall be fully compensated for by an extension of time to complete performance of Services.

#### **ARTICLE 7      EXTENSION OF TIME NOT CUMULATIVE**

In the event the Contractor shall be delayed concurrently by two or more of the causes identified in Article 6 "Extension of Time" above, the Contractor shall be entitled to a separate extension of time for each one of the causes but only one period of extension shall be granted for the delay. In addition, the Contractor shall not be entitled, by reason of a delay, to an extension of time for the completion of the overall Services unless the overall services is necessarily affected by the delay. Accordingly, in the event of a delay, the Contractor shall proceed continuously and diligently with the performance of the unaffected portions of the Work.

#### **ARTICLE 8      FORCE MAJEURE**

Neither party shall be held liable or responsible to the other party nor be deemed to have defaulted under or breached this Agreement for failure or delay in fulfilling or performing any obligation under this Agreement when such failure or delay is caused by or results from causes beyond the reasonable control of the affected party, including but not limited to fire, floods, embargoes, war, acts of war, insurrections, riots, strikes, lockouts or other labor disturbances, or acts of God; provided, however, that the party so affected shall use reasonable commercial efforts to avoid or remove such causes of nonperformance, and shall continue performance hereunder with reasonable dispatch whenever such causes are removed. Either party shall provide the other party with prompt written notice of any delay or failure to perform that occurs by reason of force majeure.

#### **ARTICLE 9      EXCUSABLE DELAY**

- a) Upon providing the County notice and reasonably full particulars of an event of force majeure (as described below) in writing, within a reasonable time after the occurrence of such event of force majeure, the Contractor shall not be liable for any delay or failure to perform to the extent caused by fire, flood, severe weather conditions, explosion, labor disputes, strike, shortage of utilities, compliance with any laws, regulations, orders, acts or requirements from the government, civil authorities, government-mandated facility shutdowns or limitations, acts of God or the public enemy, pandemics or any other act or event of any nature reasonably beyond the Contractor's control. In such circumstances, the County may, at its option, elect to cancel or reschedule the portion of any order subject to such delay by providing to the Contractor prompt written notice of its election, provided that, such cancellation or rescheduling shall apply only to that portion of the order affected by the foregoing circumstances and the balance of the order shall continue in full force and effect.
- b) The Contractor is expected to request its permits, if applicable, with the permitting agency within a timeframe that will allow the permitting agency its normal processing time to review a permit request. A schedule delay due to the processing time of a permitting agency would only be deemed excusable if the Contractor demonstrated to the satisfaction of the County, through documented evidence, the permitting agency exceeded its standard time to review such permit.

**ARTICLE 10     EXTRA WORK**

- a) The County reserves the right to order changes that may result in additions to or reductions from the amount, type or value of the Work shown in the Contract and which are within the general scope of the Contract in accordance with this article. Any such changes which result in additions to the Work will be known as "Extra Work." The Parties further agree that any changes requested by the County, for the exclusive benefit of the County, shall be also handled in accordance with this article. The County may add or deduct services (including fees) available under the contract, by mutual agreement by the parties, via a Change Order (Contract Modification).

No Extra Work shall be performed except pursuant to a written Change Order (Contract Modification) issued by the County expressly authorizing the performance of such Work and explicitly declaring the intention of the County to treat the Work described therein as Extra Work.

- b) Within thirty (30) days of the Contractor's submission of written notice that an order, direction or requirement of the County Project Manager is deemed by the Contractor to involve Extra Work, the Contractor and each Subcontractor shall submit in a form satisfactory to the County a detailed proposal ("Change Order Proposal")(including the elements of cost identified in Article 11, *Change Order Basis For Payment*, Paragraphs a and b) which shall include adjustments to the Contract price or to any other provisions of the Contract necessary to accomplish the Extra Work. Upon written request of the Contractor, within the thirty (30) day period set forth above, for good cause shown, the County Project Manager may grant the Contractor additional time in which to submit a Change Order Proposal. The failure of the Contractor to submit a detailed proposal within the time limit stated therefor, or within such additional time as is granted by the County Project Manager at its sole discretion, shall be deemed a waiver of any claim for compensation that the Contractor may have with respect to the claimed Extra Work.
- c) The provisions of the Contract relating to the Work and its performance shall apply without exception to Extra Work and the performance thereof, except as otherwise provided in a written Change Order between the Contractor and the County.
- d) The Contractor must utilize the most recent updated schedule as required by the Contract to establish the price and schedule modifications. Contractor's Change Order Proposal must include a schedule subnet and an explanation of the cost, if applicable, and schedule impact of the claimed Extra Work on the Contract. The Contractor must demonstrate clearly how it proposes to incorporate the Extra Work into the schedule. If Contractor fails to notify the County Project Manager of the schedule changes associated with a Change Order Proposal by submitting a revised schedule, it will be deemed to be an acknowledgment by Contractor that the proposed Extra Work will not have any scheduling consequences.

**ARTICLE 11     CHANGE ORDER BASIS FOR PAYMENT**

If Extra Work requires the provision of items of Work or material for which compensation cannot be computed on the basis of unit prices, and the scope and extent of the Extra Work can be determined before the Extra Work is performed, the County will perform a cost analysis of the Contractor's proposal and negotiate a lump sum amount with the Contractor as compensation for such Work. The County Project Manager may in such case request the Contractor to proceed with the Extra Work pending performance of the cost analysis and negotiation of the amount of compensation for such Extra Work. The Contractor shall honor such request so long as it deems the financial risk of doing so to be viable.

**ARTICLE 12     NOTICE REQUIREMENTS**

All notices required or permitted under this Agreement shall be in writing and shall be deemed sufficiently served if delivered by: (i) Registered or Certified Mail, with return receipt requested; (ii) personally by a by courier service; (iii) Federal Express Corporation or other nationally recognized carrier to be delivered overnight; or (iv) via facsimile or e-mail (if provided below) with delivery of hard copy pursuant to (i), (ii), or (iii) in this paragraph.

The addresses for such notice are as follows:

**(1) To the County**

a) to the Project Manager:

Miami-Dade County  
Corrections and Rehabilitations Department  
Attention: Christopher Moreno  
Phone: (786) 719-3362  
E-mail: [christopher.moreno@miamidade.gov](mailto:christopher.moreno@miamidade.gov)

and

b) to the Contract Manager:

Miami-Dade County  
Internal Services Department, Strategic Procurement Department  
Attention: Chief Procurement Officer  
111 NW 1st Street, Suite 1300  
Miami, FL 33128-1974  
Phone: (305) 375-4900  
E-mail: [namita.uppal@miamidade.gov](mailto:namita.uppal@miamidade.gov)

**(2) To the Contractor**

Securus Technologies, LLC  
Attention: General Counsel  
4000 International Parkway  
Carrollton, Texas 75007  
Phone: (972) 277-0300  
Email: [josh.martin@aventiv.com](mailto:josh.martin@aventiv.com)

Either party may at any time designate a different address and/or contact person by giving notice as provided above to the other party. Such notices shall be deemed given upon receipt by the addressee.

**ARTICLE 13 FINANCIAL STRUCTURE**

a) Rates/Fees

Contractor shall provide a fee schedule, in accordance with Attachment B. The Contractor shall ensure all users can access content without unfair costs. For a single price of bundled minutes Detainees must be able to enjoy music, messaging, movies, games, and a library of modern books. In addition, Detainees must also be provided the ability to purchase items on a per minute basis.

b) Cost and Revenue Model

The County will forego a commission paid to the County. The Contractor shall provide detail revenue reports that clearly show total revenue from each Detainee telephone and kiosk usage, broken down by call type, and media consumed as well as total revenue for all calls and media consumption during the billing period. At the end of each month, by the fifth of the following month, the Contractor shall provide the monthly report for the preceding month. For transactions completed within the County's internal Detainee banking system, the County shall make all the required disbursements to the Contractor less any amounts due to the County by the Contractor under the terms of this Contract, such as penalties, and transfer to the Contractor the remainder of the proceeds along with any amount due from the County. Sales tax shall be paid by the Contractor in accordance with Section 2.2(c), Taxes, below.

Contractor shall be responsible for the investment and implementation/installation of the Solution in its totality. As such, Contractor shall have the financial capability to finance the investments required, including but not limited to, all start-up costs.

c) Taxes

Taxes shall be charged to end user customers based on when used and not at the time of deposit. Contractor shall calculate, collect, and remit all sales Tax due to the State of Florida Department of Revenue prior to paying commissions due to MDCR. Contractor agrees to pay all penalties, fines or interest that may be assessed against the contractor or the County as a result of the contractor's non-payment, partial payment or late payment of the sales tax.

**ARTICLE 14     SOLUTION AVAILABILITY**

The Contractor shall provide a service credit and or refund, for any failure to maintain contractually agreed upon Solution availability. Service credit/refund amount shall equal the full amount paid to the Contractor by the Detainee.

**ARTICLE 15     PAYMENT FOR SERVICES/AMOUNT OBLIGATED**

- a) The Contractor shall provide all Work, and all associated services, equipment and related items as stipulated in this Agreement. The County shall have no obligation to pay the Contractor any money to obtain such Work and Services, except for any change and/or modification to the Contract, which is approved and executed in writing by the County and the Contractor. All Services undertaken by the Contractor before County's approval of this Contract shall be at the Contractor's risk and expense.
- b) If applicable, with respect to any travel costs and travel-related expenses, the Contractor agrees to adhere to Section 112.061 of the Florida Statutes as they pertain to out-of-pocket expenses, including employee lodging, transportation, per diem, and all miscellaneous cost and fees. The County shall not be liable for any such expenses that have not been approved in advance, in writing, by the County.
- c) The Contractor warrants that it has reviewed the County's requirements and has asked such questions and conducted such other inquiries as the Contractor deemed necessary in order to determine the price the Contractor will charge to provide the Work to be performed under this Contract. The fees for all Services and Work performed under this Contract, including all costs associated, shall be compensated to the Contractor in accordance with Attachment B, *Price and Payment Schedule*. A change and/or modification to the Fee Structure shall only be approved and executed in writing by the County and the Contractor. All Work undertaken by the Contractor before County's approval of this Contract shall be at the Contractor's risk and expense.

**ARTICLE 16     INDEMNIFICATION AND INSURANCE**

The Contractor shall indemnify and hold harmless the County and its officers, employees, agents and instrumentalities from any and all liability, losses or damages, including attorneys' fees and costs of defense, which the County or its officers, employees, agents or instrumentalities may incur as a result of claims, demands, suits, causes of actions or proceedings of any kind or nature arising out of, relating to or resulting from the performance of this Agreement by the Contractor or its employees, agents, servants, partners principals or Subcontractors. The Contractor shall pay all claims and losses in connection therewith and shall investigate and defend all claims, suits or actions of any kind or nature in the name of the County, where applicable, including appellate proceedings, and shall pay all costs, judgments, and attorney's fees which may issue thereon. The Contractor expressly understands and agrees that any insurance protection required by this Agreement or otherwise provided by the Contractor shall in no way limit the responsibility to indemnify, keep and save harmless and defend the County or its officers, employees, agents, and instrumentalities as herein provided.

Upon County's notification, the Contractor shall furnish to the Internal Services Department, Strategic Procurement Division, certificate(s) of insurance that indicate that insurance coverage has been obtained, which meets the requirements as outlined below:

- a) Worker's Compensation Insurance for all employees of the Contractor as required by Florida Statute 440.
- b) Commercial General Liability in an amount not less than \$1,000,000 per occurrence, and \$2,000,000 in the aggregate not to exclude Products & Completed Operations. **Miami-Dade County must be shown as an additional insured with respect to this coverage.**
- c) Automobile Liability Insurance covering all owned, non-owned and hired vehicles, in an amount not less than \$300,000 combined single limit per occurrence for bodily injury and property damage.
- d) Professional Liability Insurance in an amount not less than \$1,000,000 per claim.
- e) Cyber Liability Insurance in an amount not less than \$1,000,000 per claim.

All insurance policies required above shall be issued by companies authorized to do business under the laws of the State of Florida, with the following qualifications:

The company must be rated no less than "A-" as to management, and no less than "Class VII" as to financial strength, by Best's Insurance Guide, published by A.M. Best Company, Oldwick, New Jersey, or its equivalent, subject to the approval of the County Risk Management Division.

or

The company must hold a valid Florida Certificate of Authority as shown in the latest "List of All Insurance Companies Authorized or Approved to Do Business in Florida", issued by the State of Florida Department of Financial Services and are a member of the Florida Guaranty Fund.

The mailing address of Miami-Dade County as the certificate holder must appear on the certificate of insurance as follows:

Miami-Dade County  
111 NW 1st Street  
Suite 2340  
Miami, Florida 33128-1974

Compliance with the foregoing requirements shall not relieve the Contractor of this liability and obligation under this section or under any other section in this Agreement.

Award of this Contract is contingent upon the receipt of the insurance documents, as required, within ten (10) business days. If the certificate of insurance is received within the specified timeframe but not in the manner prescribed in this Agreement, the Contractor shall have an additional five business days to submit a corrected certificate to the County. If the Contractor fails to submit the required insurance documents in the manner prescribed in this Agreement within fifteen (15) business days, the Contractor shall be in default of the contractual terms and conditions and award of the Contract may be rescinded, unless such timeframe for submission has been extended by the County.

The Contractor shall assure that the certificate of insurance required in conjunction with this section remain in full force for the term of the Contract, including any renewal or extension periods that may be exercised by the County. If the certificate of insurance is scheduled to expire during the term of the Contract, the Contractor shall submit new or renewed certificate of insurance to the County before such expiration. If expired certificate of insurance is/are not replaced or renewed to cover the Contract period, the County may suspend the Contract until the new or renewed certificate is/are received by the County in the manner prescribed herein. If such suspension exceeds thirty (30) calendar days, the County may, at its sole discretion,

terminate the Contract for cause and the Contractor shall be responsible for all direct and indirect costs associated with such termination.

#### **ARTICLE 17 MANNER OF PERFORMANCE**

- a) The Contractor shall provide the Work described herein in a competent and professional manner satisfactory to the County in accordance with the terms and conditions of this Agreement. The County shall be entitled to a satisfactory performance of all Work described herein and to full and prompt cooperation by the Contractor in all aspects of the Work. At the request of the County, the Contractor shall promptly remove from the Project any Contractor's employee, Subcontractor, or any other person performing Work hereunder, so long as such removal is not in violation of any applicable law. The Contractor agrees that such removal of any of its employees does not require the termination or demotion of any employee by the Contractor.
- b) The Contractor agrees to defend, hold harmless and indemnify the County and shall be liable and responsible for all claims, suits, actions, damages, and costs (including attorneys' fees and court costs) made against the County, occurring on account of, arising from or in connection with the removal and replacement of any Contractor's personnel performing Services hereunder at the behest of the County. Removal and replacement of any Contractor's personnel as used in this Article shall not require the termination and/or demotion of such Contractor's personnel.
- c) The Contractor always agrees that it will employ, maintain, and assign to the performance of the Work a sufficient number of competent and qualified professionals and other personnel to meet the requirements to which reference is hereinafter made. The Contractor agrees to adjust its personnel staffing levels or to replace any its personnel if so, directed upon reasonable request from the County, should the County make a determination, in its sole discretion, that said personnel staffing is inappropriate or that any individual is not performing in a manner consistent with the requirements for such a position.
- d) The Contractor warrants and represents that its personnel have the proper skill, training, background, knowledge, experience, rights, authorizations, integrity, character, and licenses as necessary to perform the Work described herein, in a competent and professional manner.
- e) The Contractor shall always cooperate with the County and coordinate its respective work efforts to maintain the progress most effectively and efficiently in performing the Work.
- f) The Contractor shall comply with all provisions of all federal, state, and local laws, statutes, ordinances, and regulations that are applicable to the performance of this Agreement.
- g) The Contractor shall provide contract services on an exclusive basis that are fee based, serving as revenue for the Contractor.

#### **ARTICLE 18 SOCIAL/FAIR LABOR STANDARDS**

- a) Contractor contributions to the health, well-being and development of its employees. Contractor shall support of safe, fair, and equitable work practices and ethical behavior, to include:
  1. Equitable wage/benefit determination practices
  2. Fair and equitable employee development and evaluation process
- b) Contractor shall provide equal access to small, diverse and disadvantaged suppliers. Contractor shall develop supplier diversity initiatives used to increase the participation of small, diverse and disadvantaged enterprises, in contracting opportunities.

#### **ARTICLE 19 SUSTAINABLE PROCUREMENT PRACTICES**

The County is committed to responsible stewardship of resources and to demonstrating leadership in sustainable business practices. Accordingly, the County has adopted sustainability policies which are incorporated into this Agreement. The County

will continue to explore and pursue sustainable procurement, development, and business practices that: (a) reduce greenhouse gases; (b) foster and integrate supplier small business opportunities; (c) support safe and fair labor practices and ethical behavior throughout the supply chain, and (d) maximize fiscally responsible "high value, high impact" actions. The Contractor shall have the ability to meet industry green standards.

#### **ARTICLE 20 EMPLOYEES OF THE CONTRACTOR**

All employees of the Contractor shall be, at all times, employees of the Contractor under its sole direction and not employees or agents of the County. The Contractor shall supply competent employees. Miami-Dade County may require the Contractor to remove an employee it deems careless, incompetent, insubordinate or otherwise objectionable and whose continued employment on County property is not in the best interest of the County. Each employee shall have and wear proper identification.

#### **ARTICLE 21 INDEPENDENT CONTRACTOR RELATIONSHIP**

The Contractor is, and shall be, in the performance of all Work and activities under this Agreement, an independent contractor, and not an employee, agent or servant of the County. All persons engaged in any of the Work performed or Services provided pursuant to this Agreement shall always, and in all places, be subject to the Contractor's sole direction, supervision, and control. The Contractor shall exercise control over the means and manner in which it and its employees perform the Work, and in all respects the Contractor's relationship and the relationship of its employees to the County shall be that of an independent contractor and not as employees and agents of the County.

The Contractor does not have the power or authority to bind the County in any promise, agreement, or representation other than specifically provided for in this Agreement.

#### **ARTICLE 22 DISPUTE RESOLUTION PROCEDURE**

- a) The Parties agree that in the event of any dispute of any nature whatsoever arising out of, under, or in connection with, or in any way related to or on account of, this Agreement, including without limitations: questions as to the value, acceptability and fitness of the Services; questions as to either party's fulfillment of its obligations under the Contract; negligence, fraud or misrepresentation before or subsequent to acceptance of the Contractor's Proposal; questions as to the interpretation of the Scope of Works; and claims for damages, compensation and losses, the Parties shall first seek to resolve such dispute through the senior executive level of the Contractor and the County Mayor or designee regarding matters within the County Mayor's purview. In the event the Parties are unable to resolve a dispute, any such dispute shall be brought before the County Mayor within 10 days of the occurrence, event, or act out of which the dispute arises if the matter was not brought before the County Mayor.
- b) The County Mayor may base a decision on such assistance as may be desirable, including advice of experts, but in any event shall base the decision on an independent and objective determination of whether Contractor's performance or any Deliverable meets the requirements of this Agreement and any specifications with respect thereto set forth herein. The effect of any decision shall not be impaired or waived by any negotiations or settlements or offers made in connection with the dispute, whether or not the County Mayor participated therein, or by any prior decision of others, which prior decision shall be deemed subject to review, or by any termination or cancellation of the Agreement. All such disputes shall be submitted in writing by the Contractor to the County Mayor for a decision, together with all evidence and other pertinent information in regard to such questions, in order that a fair and impartial decision may be made. Whenever the County Mayor is entitled to exercise discretion or judgement or to make a determination or form an opinion pursuant to the provisions of this article, such action shall be fair and impartial when exercised or taken. The County Mayor, as appropriate, shall render a decision in writing and deliver a copy of the same to the Contractor.
- c) If the Dispute is not resolved by the foregoing process, within five (5) days of the date of the notice to the Contractor referring to the determination of the County Mayor, the Contractor may, by the giving of written notice, cause the matter to be referred to mediation administered by the American Arbitration Association under its Commercial Mediation Procedures. The arbitration shall be held in Miami, FL. The arbitral award shall be final and binding upon the Parties.

d) This Article will survive the termination or expiration of this Agreement.

e)

**ARTICLE 23 MUTUAL OBLIGATIONS**

- a) This Agreement, including attachments to the Agreement, shall constitute the entire Agreement between the Parties with respect hereto and supersedes all previous communications and representations or agreements, whether written or oral, with respect to the subject matter hereto unless acknowledged in writing by the duly authorized representatives of the Parties.
- b) Nothing in this Agreement shall be construed for the benefit, intended or otherwise, of any third party that is not a parent or subsidiary of a party or otherwise related (by virtue of ownership control or statutory control) to a party.
- c) In those situations where this Agreement imposes an indemnity obligation on the Contractor, the County may, at its expense, elect to participate in the defense if the County should so choose. Furthermore, the County may at its own expense defend or settle any such claims if the Contractor fails to diligently defend such claims, and thereafter seek indemnity for such defense or settlement costs from the Contractor.

**ARTICLE 24 QUALITY ASSURANCE/QUALITY ASSURANCE RECORD KEEPING**

The Contractor shall maintain, and shall require that its Subcontractors and suppliers maintain, complete and accurate records to substantiate compliance with the requirements set forth in the Agreement. The Contractor and its Subcontractors and suppliers shall retain such records, and all other documents relevant to the Work furnished under this Agreement for a period of three years from the expiration date of this Agreement and any extension thereof.

**ARTICLE 25 AUDITS**

The County, or its duly authorized representatives and governmental agencies, shall until the expiration of three years after the expiration of this Agreement and any extension thereof, have access to and the right to examine and reproduce any of the Contractor's books, documents, papers and records and of its Subcontractors and suppliers which apply to all matters of the County. Such records shall subsequently conform to Generally Accepted Accounting Principles requirements, as applicable, and shall only address those transactions related to this Agreement.

Pursuant to Section 2-481 of the Code, the Contractor will grant access to the Commission Auditor to all financial and performance related records, property, and equipment purchased in whole or in part with government funds within five business days of the Commission Auditor's request. The Contractor agrees to maintain an accounting system that provides accounting records that are supported with adequate documentation, and adequate procedures for determining the allowability and allocability of costs.

**ARTICLE 26 SUBSTITUTION OF PERSONNEL**

In the event the Contractor needs to substitute personnel for the key personnel identified by the Contractor's Proposal, the Contractor must notify the County in writing and request written approval for the substitution at least ten (10) business days prior to effecting such substitution. However, such substitution shall not become effective until the County has approved said substitution.

**ARTICLE 27 CONSENT OF THE COUNTY REQUIRED FOR ASSIGNMENT**

The Contractor shall not assign, transfer, convey or otherwise dispose of this Agreement, including its rights, title, or interest in or to the same or any part thereof without the prior written consent of the County.

**ARTICLE 28 SUBCONTRACTUAL RELATIONS**

- a) If the Contractor causes any part of this Agreement to be performed by a Subcontractor, the provisions of this Contract will apply to such Subcontractor and its officers, agents and employees in all respects as if and they were employees of the Contractor; and the Contractor will not be in any manner thereby discharged from its obligations and liabilities

hereunder, but will be liable hereunder for all acts, omissions, and negligence of the Subcontractor, its officers, agents, and employees, as if they were employees of the Contractor. The services performed by the Subcontractor will be subject to the provisions hereof as if performed directly by the Contractor.

- b) The Contractor, before making any subcontract for any portion of the Work, will state in writing to the County the name of the proposed Subcontractor, the portion of the Work which the Subcontractor is to do, the place of business of such Subcontractor, and such other information as the County may require. The County will have the right to require the Contractor not to award any subcontract to a person, firm or corporation disapproved by the County.
- c) Before entering into any subcontract hereunder, the Contractor will inform the Subcontractor fully and completely of all provisions and requirements of this Agreement relating either directly or indirectly to the Work to be performed. Such Work performed by such Subcontractor will strictly comply with the requirements of this Contract.
- d) In order to qualify as a Subcontractor satisfactory to the County, in addition to the other requirements herein provided, the Subcontractor must be prepared to prove to the satisfaction of the County that it has the necessary facilities, skill and experience, and ample financial resources to perform the Work in a satisfactory manner. To be considered skilled and experienced, the Subcontractor must show to the satisfaction of the County that it has satisfactorily performed Work of the same general type which is required to be performed under this Agreement.
- e) The County shall have the right to withdraw its consent to a subcontract if it appears to the County that the Subcontractor will delay, prevent, or otherwise impair the performance of the Contractor's obligations under this Agreement. All Subcontractors are required to protect the confidentiality of the County's and County's proprietary and confidential information. Contractor shall furnish to the County copies of all subcontracts between Contractor and Subcontractors and suppliers hereunder. Within each such subcontract, there shall be a clause for the benefit of the County in the event the County finds the Contractor in breach of this Contract, permitting the County to request completion by the Subcontractor of its performance obligations under the subcontract. The clause shall include an option for the County to pay the Subcontractor directly for the performance by such Subcontractor. Notwithstanding, the foregoing shall neither convey nor imply any obligation or liability on the part of the County to any Subcontractor hereunder as more fully described herein.

#### **ARTICLE 29     ASSUMPTION, PARAMETERS, PROJECTIONS, ESTIMATES AND EXPLANATIONS**

The Contractor understands and agrees that any assumptions, parameters, projections, estimates, and explanations presented by the County were provided to the Contractor for evaluation purposes only. However, since these assumptions, parameters, projections, estimates, and explanations represent predictions of future events the County makes no representations or guarantees; and the County shall not be responsible for the accuracy of the assumptions presented; and the County shall not be responsible for conclusions to be drawn therefrom; and any assumptions, parameters, projections, estimates and explanations shall not form the basis of any claim by the Contractor. The Contractor accepts all risk associated with using this information.

#### **ARTICLE 30     SEVERABILITY**

If this Agreement contains any provision found to be unlawful, the same shall be deemed to be of no effect and shall be deemed stricken from this Agreement without affecting the binding force of this Agreement as it shall remain after omitting such provision.

#### **ARTICLE 31     TERMINATION AND SUSPENSION OF WORK**

- a) This Agreement may be terminated for cause by the County for reasons including, but not limited to, (i) the Contractor commits an Event of Default (as defined below in Article 32) and fails to cure said Event of Default (as delineated below in Article 33), or (ii) Contractor attempts to meet its contractual obligations with the County through fraud, misrepresentation, or material misstatement.
- b) This Agreement may also be terminated for convenience by the County. Termination for convenience is effective on the termination date stated in the written notice provided by the County.

- c) If County terminates this Agreement for cause under Article 31(a) above, the County may, in its sole discretion, also terminate or cancel any other contract(s) that such individual or corporation or other entity has with the County and that such individual, corporation or other entity shall pay all direct or indirect costs associated with such termination or cancellation, including attorneys' fees.
- d) The foregoing notwithstanding, if the Contractors attempts to meet its contractual obligations with the County through fraud, misrepresentation, or material misstatement, the Contractor may be debarred from County contracting in accordance with the County debarment procedures. The Contractor may be subject to debarment for failure to perform and all other reasons set forth in Section 10-38 of the Code.
- e) In the event that the County exercises its right to terminate this Agreement, the Contractor shall, upon receipt of such notice, unless otherwise directed by the County:
  - i. stop Work on the date specified in the notice (the "Effective Termination Date");
  - ii. take such action as may be necessary for the protection and preservation of the County's materials and property;
  - iii. cancel orders;
  - iv. assign to the County and deliver to any location designated by the County any non-cancelable orders for Deliverables that are not capable of use except in the performance of this Agreement and has been specifically developed for the sole purpose of this Agreement and not incorporated in the Services;
  - v. take no action which will increase the amounts payable by the County under this Agreement; and
  - vi. reimburse the County a proration of the fees paid annually based on the remaining months of the term per the compensation listed in Attachment B.
- f) In the event that the County exercises its right to terminate this Agreement, the Contractor will be compensated as stated in the payment Articles herein for the:
  - i. portion of the Services completed in accordance with the Agreement up to the Effective Termination Date; and
  - ii. non-cancelable Deliverables that are not capable of use except in the performance of this Agreement and has been specifically developed for the sole purpose of this Agreement, but not incorporated in the Services.
- g) All compensation pursuant to this Article are subject to audit.
- h) In the event the Contractor fails to cure an Event of Default timely, the County may terminate this Agreement, and the County or its designated representatives may immediately take possession of all applicable equipment, materials, products, documentation, reports, and data that belong to the County.

## **ARTICLE 32     EVENT OF DEFAULT**

- a) An Event of Default is a material breach of this Agreement by the Contractor, and includes but is not limited to the following and other reasonable determinations of the County:
  - i. the Contractor has not delivered Deliverables and/or Services on a timely basis;
  - ii. the Contractor has refused or failed to supply enough properly skilled staff personnel;
  - iii. the Contractor has failed to make prompt payment to Subcontractors or suppliers for any Services;
  - iv. the Contractor has become insolvent (other than as interdicted by the bankruptcy laws), or has assigned the

proceeds received for the benefit of the Contractor's creditors, or the Contractor has taken advantage of any insolvency statute or debtor/creditor law or if the Contractor's affairs have been put in the hands of a receiver;

- v. the Contractor has failed to obtain the approval of the County where required by this Agreement;
  - vi. the Contractor has failed to provide "adequate assurances" as required under subsection b below;
  - vii. the Contractor has failed in the representation of any warranties stated herein; or
- b) When, in the opinion of the County, reasonable grounds for uncertainty exist with respect to the Contractor's ability to perform the Work or any portion thereof, the County may request that the Contractor, within the timeframe set forth in the County's request, provide adequate assurances to the County, in writing, of the Contractor's ability to perform in accordance with the terms of this Agreement. Until the County receives such assurances, the County may request an adjustment to the compensation received by the Contractor for portions of the Work which the Contractor has not performed. In the event that the Contractor fails to provide to the County the requested assurances within the prescribed timeframe, the County may:
- i. treat such failure as a repudiation and/or material breach of this Agreement; and
  - ii. resort to any remedy for breach provided herein or at law, including but not limited to, taking over the performance of the Work or any part thereof either by itself or through others.

#### **ARTICLE 33 NOTICE OF DEFAULT - OPPORTUNITY TO CURE**

If an Event of Default occurs in the determination of the County, the County shall notify the Contractor (the "Default Notice"), specifying the basis for such default, and advising the Contractor that such default must be cured immediately, or this Agreement with the County may be terminated. Notwithstanding, the County may, in its sole discretion, allow the Contractor to rectify the default to the County's reasonable satisfaction within a thirty (30) day period. The County may grant an additional period of such duration as the County shall deem appropriate without waiver of any of the County's rights hereunder, so long as the Contractor has commenced curing such default and is effectuating a cure with diligence and continuity during such thirty (30) day period or any other period which the County prescribes. The Default Notice shall specify the date the Contractor shall discontinue the Work upon the Effective Termination Date.

#### **ARTICLE 34 REMEDIES IN THE EVENT OF DEFAULT**

If an Event of Default occurs, whether or not the County elects to terminate this Agreement as a result thereof, the Contractor shall be liable for all damages resulting from the default, irrespective of whether the County elects to terminate the Agreement, including but not limited to:

- a) lost revenues;
- b) the difference between the cost associated with procuring Services hereunder and the amount actually expended by the County for re-procurement of Services, including procurement and administrative costs; and
- c) such other direct damages.

The Contractor shall also remain liable for any liabilities and claims related to the Contractor's default. The County may also bring any suit or proceeding for specific performance or for an injunction.

#### **ARTICLE 35 EQUIPMENT**

The Contractor shall provide for all Systems a complete list of all equipment to be delivered by facility, which shall include the quantity and Serial Number; together with a delivery schedule. All equipment and software delivered at each facility shall be suitably durable for a correctional environment and constructed in such a way that no parts and/or pieces of the equipment can constitute a security risk. Any change or modification to the list of equipment to be delivered must be approved by the Project Manager before delivery is made.

**ARTICLE 36     GRANT OF LICENSE**

- a) License. Contractor agrees to provide the County with the Solution, Updates, Upgrades, and Documentation in accordance with the provisions contained within this Agreement.
- b) Contractor grants the County a limited, perpetual, non-transferable, non-exclusive license to use the Solution, Updates, Upgrades, and Documentation in accordance with the terms of this Agreement. Such license shall not be construed to be any license to source code for any component of the Solution.
- c) Post termination or expiration of the Contract, the County shall have access to call and visitation records and call recordings for a period of seven (7) years. The County shall have access to video visitation records and video recordings for a period of forty-five (45) days.

**ARTICLE 37     DELIVERY**

- a) Delivery of the Solution shall be according to Attachment A, *Scope of Work*, and contingent upon Final Acceptance by the County.
- b) Documentation. The Contractor shall provide electronic copies of the associated Documentation as provided by the developer(s) of the Solution to the County upon Final Acceptance.

**ARTICLE 38     MAINTENANCE AND TECHNICAL SUPPORT SERVICES**

Contractor shall provide the County with maintenance and technical support services in the manner outlined in Attachment C, *Maintenance and Support Services*, for the Solution throughout the term of this Agreement, including any options or extensions exercised by the County.

**ARTICLE 39     PROTECTION OF SOFTWARE**

- a) No Reverse Engineering. The County agrees not to modify, reverse engineer, disassemble, or decompile the Licensed Software, or any portion thereof.
- b) Ownership. County further acknowledges that all copies of the Licensed Software in any form provided by the Contractor are the sole property of the Contractor. The County shall not have any right, title, or interest to any License Software or copies thereof except as provided in this Agreement, and further shall secure and protect all Licensed Software and Documentation consistent with maintenance of Contractor's proprietary rights therein.

**ARTICLE 40     SOFTWARE MODIFICATIONS**

- a) Solution Enhancements or Modifications. The County may, from time to time, request that the Contractor incorporate certain features, enhancements or modifications into the Solution. When requested by the County, the Contractor shall provide the requested Solution enhancements/modifications. Upon the County's request for such enhancements/modifications, the Contractor shall prepare a Statement of Work ("SOW") for the specific Project that shall define the Work to be performed. The Contractor shall submit a cost proposal including all costs pertaining to the requested enhancements/modifications.
- b) After the County has accepted the SOW a detailed requirements and detailed design document shall be submitted illustrating the complete financial terms that govern the SOW, proposed Project staffing, anticipated Project schedule, and other information relevant to the Project. Each SOW executed hereunder shall automatically incorporate the terms and

conditions of this Agreement. Such enhancements or modifications shall become the property of the Contractor. Notwithstanding the foregoing, performance of any such modifications shall not compromise the Contractor's warranty obligations.

- c) The Contractor shall provide the County, if so requested, with written confirmation of the date the enhancements/modification was applied to the Solution.

#### **ARTICLE 41    IMPLEMENTATION SERVICES**

- a) If the Contractor fails to provide Deliverables, Solution, Updates, or Upgrades within the time specified or if the Solution delivered fails to conform to the requirements or are found to be defective in material or workmanship, then the County may (i) reject the Deliverable, Solution, Update, or Upgrade in totality or (ii) accept any portion of Deliverable, Solution, Update, or Upgrade and reject the balance of the Deliverable, Solution, Update, or Upgrade. The County shall notify Contractor of such rejection in writing and specify in such notice, the reasons for such rejection. Contractor agrees to deliver a fix or updated Deliverable, Solution, Update, or Upgrade within a mutually agreed upon time period following the Contractor's receipt of the County's rejection notice.
- b) The Contractor shall bear the risk of loss or damage to the Deliverable, Solution, Update, or Upgrade until the time the Project Manager certifies that the Deliverable, Solution, Update, or Upgrade has successfully completed the acceptance testing whether such loss or damage arises from acts or omissions (whether negligent or not) of the Contractor or the County or from any other cause whatsoever, except loss or damage arising solely from the gross negligence or willful acts of the County.
- c) The Contractor agrees to install the Solution at the County's facilities. Contractor agrees to commence installation of the Solution according to the Implementation Timeline (Attachment D) unless a different time for implementation is otherwise mutually agreed upon by the parties hereto. All implementation services will be performed during normal business hours. Whenever possible, however some services to be provided may be required outside of normal business hours to accommodate County operations. The County shall make reasonable accommodations for Contractor's request for access to County facilities and staff. Work to be performed outside normal business hours will be mutually agreed by both parties. Contractor shall diligently pursue and complete such implementation services without interruption and in accordance with the Implementation Timeline, so that such Solution is in good working order and ready for use by the dates set forth in the Timeline.
- d) Contractor agrees to do all things necessary for proper implementation of the Solution and to perform its implementation obligations hereunder in an orderly, skillful and expeditious manner, with sufficient labor and materials to ensure efficient and timely completion of such obligations. If applicable, Contractor shall coordinate with the Project Manager all Work with all other contractors and/or County personnel performing work to complete Solution installation. The County shall be responsible for resolving all disputes relating to site access between Contractor and/or County personnel. Contractor shall provide all materials necessary to properly implement the Solution. The County shall attempt to provide reasonable working and secure storage space for the performance by Contractor of the implementation services described herein.
- e) Unless otherwise agreed to by the County, Contractor agrees as part of the implementation to perform all required Work to successfully achieve all objectives set forth in the Scope of Works, including, but not limited to, (a) solution configuration; (b) interface development; (c) software testing; (d) acceptance and user acceptance testing; (e) training; (f) cooperating with all other contractors that are supplying peripheral or ancillary equipment required for the use of the Solution; and (g) any additional services necessary to ensure Contractor's compliance with this Article.
- f) Solution testing shall consist of the tests described in the Scope of Works which are to be conducted collectively by the Contractor and the County. The purpose of these tests is to demonstrate the complete operability of the Solution in conformance with the requirements of the Contract. This will include an actual demonstration of all required Solution functionality. All tests shall be in accordance with test plans and procedures prepared by Contractor and previously approved by the County. In the event of any outstanding deficiencies at the conclusion of installation testing, as determined by the County, Contractor shall be responsible for instituting necessary corrective measures, and for

subsequently satisfactorily demonstrating and/or re-demonstrating Solution performance.

#### **ARTICLE 42    TESTS**

- a) The Contractor shall configure and program the Solution to conform to the Scope of Works. The Solution shall be subject to numerous tests, including acceptance testing as further defined in the Scope of Works as developed and agreed by both parties. To assure Solution performance, the County's Project Manager will coordinate all testing of the Solution and provide Final Acceptance upon completion of all milestones and deliverables as outlined in the Scope of Works.
- b) Failure of the Solution to satisfy the acceptance criteria and conform to the requirements set forth in the Scope of Works by the timeframes set forth in the Implementation Timeline may result in the County withholding payment until satisfactory acceptance is granted to the Contractor.
- c) After Final Acceptance is granted, any modifications, fixes, enhancements, and/or new releases of the Solution require separate testing periods and sign-off from the Project Manager prior to Go-Live via mutually agreed upon acceptance testing process.

#### **ARTICLE 43    BUSINESS CONTINUITY AND DISASTER RECOVERY**

Contractor shall provide the County with business continuity and disaster recovery services in the manner outlined in Attachment E, *Business Continuity and Disaster Recovery*, for the Solution throughout the term of this Agreement, including any options or extensions exercised by the County.

#### **ARTICLE 44    SOLUTION WARRANTY**

- a) Contractor warrants that the Solution, upon Final Acceptance, shall conform to and function in accordance with the Scope of Works and shall meet or exceed the functionality and interoperability requirements as defined in the therein. In addition, Contractor warrants that its performance of the Scope of Works shall be in accordance with the methodology outlined therein. Further, Contractor warrants that the Solution shall be capable of handling both the current and anticipated volume of transactions specified in the Scope of Works.
- b) Remedies. If the Solution does not perform as warranted, Contractor shall use all reasonable efforts, consistent with industry standards, to cure the defect(s) as set forth in the Technical Support Services outlined in the Scope of Works. If the Contractor cannot cure the defect(s) within a mutually agreed upon timeframe, the Contractor, at the County's option, shall: 1) provide a functionally equivalent Solution, or portion thereof, from another provider; or 2) refunds all fees paid by the County to the Contractor for the Solution, or portion thereof.

#### **ARTICLE 45    DATA STORAGE SPACE**

The Contractor shall provide the County with storage space to allow for the uploading of County documents and videos to support operations. The total amount of storage space available to the County will be equal to 32 gigabytes multiplied by the total number of tablets deployed. The County will not be charged any fees for an overage of any individual tablet. The cost for additional storage space beyond the cumulative total will be billed in accordance with Attachment B.

#### **ARTICLE 46    THIRD PARTY WARRANTY**

In addition to the foregoing warranties, the Contractor hereby assigns to the County, and the County shall have the benefit of, any and all subcontractor's and suppliers' warranties and representations with respect to the Licensed Software provided hereunder. In the Contractor's agreements with subcontractors and suppliers, the Contractor shall require that such parties (i) consent to the assignment of such warranties and representations to the County; (ii) agree that such warranties and representations are enforceable by the County in its own name; and (iii) furnish to the County, the warranties and obligations as set forth in Articles 44, *Solution Warranty*.

**ARTICLE 47     FUNCTIONALLY EQUIVALENT SOFTWARE**

As long as the County maintains continuous Maintenance and Technical Support Services with Contractor for the Solution and (i) in the event the Solution is no longer supported, and (ii) the Contractor makes available successor software products (e.g., software products based on a new technical architecture) ("Successor Products") with substantially similar price, features, and functionality to the Solution during the Contract Term, including any extensions or renewals thereof, then County, at its sole discretion, may transfer the Solution to the Successor Products, for no additional license fees. In the event the County elects to transfer its license to the Solution to the Successor Products, the County shall return to Contractor the Licensed Software and pay the then-current maintenance fees for the Successor Products, and fees for services, third party hardware and software associated with the transfer to the Successor Products at mutually agreed cost.

**ARTICLE 48     PATENT AND COPYRIGHT INDEMNIFICATION**

- a) The Contractor shall not infringe on any copyrights, trademarks, service marks, trade secrets, patent rights, other intellectual property rights or any other third-party proprietary rights in the performance of the Work.
- b) The Contractor warrants that all Deliverables furnished hereunder, including but not limited to equipment, programs, documentation, software, analyses, applications, methods, ways, processes, and the like, do not infringe upon or violate any copyrights, trademarks, service marks, trade secrets, patent rights, other intellectual property rights or any other third party proprietary rights.
- c) The Contractor shall be liable and responsible for any and all claims made against the County for infringement of patents, copyrights, service marks, trade secrets or any other third party proprietary rights, by the use or supplying of any programs, documentation, software, analyses, applications, methods, ways, processes, and the like, in the course of performance or completion of, or in any way connected with, the Work, or the County's continued use of the Deliverables furnished hereunder. Accordingly, the Contractor at its own expense, including the payment of attorney's fees, shall indemnify, and hold harmless the County and defend any action brought against the County with respect to any claim, demand, cause of action, debt, or liability.
- d) In the event any Deliverable or anything provided to the County hereunder, or portion thereof is held to constitute an infringement and its use is or may be enjoined, the Contractor shall have the obligation to, at the County's option to (i) modify, or require that the applicable Subcontractor or supplier modify, the alleged infringing item(s) at its own expense, without impairing in any respect the functionality or performance of the item(s), or (ii) procure for the County, at the Contractor's expense, the rights provided under this Agreement to use the item(s).
- e) The Contractor shall be solely responsible for determining and informing the County whether a prospective supplier or Subcontractor is a party to any litigation involving patent or copyright infringement, service mark, trademark, violation, or proprietary rights claims or is subject to any injunction which may prohibit it from providing any Deliverable hereunder. The Contractor shall enter into agreements with all suppliers and Subcontractors at the Contractor's own risk. The County may reject any Deliverable that it believes to be the subject of any such litigation or injunction, or if, in the County's judgment, use thereof would delay the Work or be unlawful.

**ARTICLE 49     CONFIDENTIALITY**

- a) All Developed Works and other materials, data, transactions of all forms, financial information, documentation, inventions, designs and methods obtained from the County in connection with the Services performed under this Agreement, made or developed by the Contractor or its Subcontractors in the course of the performance of such Services, or the results of such Services, or for which the County holds the proprietary rights, constitute Confidential Information and may not, without the prior written consent of the County, be used by the Contractor or its employees, agents, Subcontractors or suppliers for any purpose other than for the benefit of the County, unless required by law. In addition to the foregoing, all County employee information and County financial information shall be considered Confidential Information and shall be subject to all the requirements stated herein. Neither the Contractor nor its employees, agents, Subcontractors, or suppliers may sell, transfer, publish, disclose, display, license or otherwise make available to others any part of such Confidential Information without the prior written consent of the County. Additionally, the Contractor expressly agrees to

be bound by and to defend, indemnify and hold harmless the County, and their officers and employees from the breach of any federal, state, or local law in regard to the privacy of individuals.

- b) The Contractor shall advise each of its employees, agents, Subcontractors, and suppliers who may be exposed to such Confidential Information of their obligation to keep such information confidential and shall promptly advise the County in writing if it learns of any unauthorized use or disclosure of the Confidential Information by any of its employees or agents, or Subcontractor's or supplier's employees, present or former. In addition, the Contractor agrees to cooperate fully and provide any assistance necessary to ensure the confidentiality of the Confidential Information.
- c) In the event of a breach of this Article damages may not be an adequate remedy and the County shall be entitled to injunctive relief to restrain any such breach or threatened breach. Unless otherwise requested by the County, upon the completion of the Services performed hereunder, the Contractor shall immediately turn over to the County all such Confidential Information existing in tangible form, and no copies thereof shall be retained by the Contractor or its employees, agents, Subcontractors, or suppliers without the prior written consent of the County. A certificate evidencing compliance with this provision and signed by an officer of the Contractor shall accompany such materials.

#### **ARTICLE 50     PROPRIETARY INFORMATION**

- a) As a political subdivision of the State of Florida, Miami-Dade County is subject to the stipulations of the public records laws of the State of Florida (the "Public Records Law").
- b) The Contractor acknowledges that all computer software in the County's possession may constitute or contain information or materials which the County has agreed to protect as proprietary information from disclosure or unauthorized use and may also constitute or contain information or materials which the County has developed at its own expense, the disclosure of which could harm the County's proprietary interest therein.
- c) During the term of the Contract, the Contractor will not use directly or indirectly for itself or for others, or publish or disclose to any third party, or remove from the County's property, any computer programs, data compilations, or other software which the County has developed, has used, or is using, is holding for use, or which are otherwise in the possession of the County (the "Computer Software"). All third-party license agreements must also be honored by the Contractor and its employees, except as authorized by the County and, if the Computer Software has been leased or purchased by the County, all hired party license agreements must also be honored by the contractors' employees with the approval of the lessor or Contractors thereof. This includes mainframe, minis, telecommunications, personal computers, and all information technology software.
- d) The Contractor will report to the County any information discovered or which is disclosed to the Contractor which may relate to the improper use, publication, disclosure, or removal from the County's property of any information technology software and hardware and will take such steps as are within the Contractor's authority to prevent improper use, disclosure, or removal.

#### **ARTICLE 51     PROPRIETARY RIGHTS**

- a) The Contractor hereby acknowledges and agrees that the County retains all rights, title and interests in and to all materials, data, documentation and copies thereof furnished by the County to the Contractor hereunder. All recorded communications are the property of the County and will be retained or provided to the County as set forth in this Agreement. The Contractor as well as its employees, agents, Subcontractors and suppliers may use such recorded communications only in connection with the performance of Services under this Agreement. The Contractor shall not, without the prior written consent of the County, use such documentation on any other project in which the Contractor or its employees, agents, Subcontractors, or suppliers are or may become engaged. Submission or distribution by the Contractor to meet official regulatory requirements or for other purposes in connection with the performance of Services under this Agreement shall not be construed as publication in derogation of the County's copyrights or other proprietary rights.

Other than the recorded communications as otherwise set forth herein, the Contractor does not grant or otherwise convey any license or other ownership right in or to any technology, data, or intellectual property rights associated with the products, services, software, or otherwise, as may be associated with this Agreement.

- d) Except as otherwise provided in subsections a, b, and c above, or elsewhere herein, the Contractor and its Subcontractors and suppliers hereunder shall retain all proprietary rights in and to all Licensed Software provided hereunder. Notwithstanding the foregoing, the Contractor hereby grants, and shall require that its Subcontractors and suppliers grant, if the County so desires, a perpetual, irrevocable and limited license to use, duplicate, disclose and/or permit any other person(s) or entity(ies) to use all such Licensed Software and the associated specifications, technical data and other Documentation for the operations of the County or entities controlling, controlled by, under common control with, or affiliated with the County, or organizations which may hereafter be formed by or become affiliated with the County. Such license specifically includes, but is not limited to, the right of the County to use and/or disclose, in whole or in part, the technical documentation and Licensed Software to any person or entity outside the County for such person's or entity's use in furnishing any and/or all of the Deliverables provided hereunder exclusively for the County or entities controlling, controlled by, under common control with, or affiliated with the County, or organizations which may hereafter be formed by or become affiliated with the County. No such License Software, specifications, data, documentation, or related information shall be deemed to have been given in confidence and any statement or legend to the contrary shall be void and of no effect.

**ARTICLE 52     VENDOR REGISTRATION/CONFLICT OF INTEREST**

a) Vendor Registration

The Contractor shall be a registered vendor with the County – Internal Services Department, Strategic Procurement Division, for the duration of this Agreement. In becoming a registered vendor with Miami-Dade County, the vendor's Federal Employer Identification Number (FEIN) must be provided, via submission of Form W-9 and 147c Letter, as required by the Internal Revenue Service (IRS). If no FEIN exists, the Social Security Number of the owner must be provided as the legal entity identifier. This number becomes Contractor's "County Vendor Number." To comply with Section 119.071(5) of the Florida Statutes relating to the collection of an individual's Social Security Number, be aware that the County requests the Social Security Number for the following purposes:

- Identification of individual account records
- Payments to individual/Contractor for goods and services provided to Miami-Dade County
- Tax reporting purposes
- Provision of unique identifier in the vendor database used for searching and sorting departmental records

The Contractor confirms its knowledge of and commitment to comply with the following:

- |  |  |
|--|--|
| <ol style="list-style-type: none"> <li>1. <b>Miami-Dade County Ownership Disclosure Affidavit</b><br/>(Section 2-8.1 of the Code of Miami-Dade County)</li> <li>2. <b>Miami-Dade County Employment Disclosure Affidavit</b><br/>(Section 2.8.1(d)(2) of the Code of Miami-Dade County)</li> <li>3. <b>Miami-Dade County Employment Drug-free Workplace Certification</b><br/>(Section 2-8.1.2(b) of the Code of Miami-Dade County)</li> <li>4. <b>Miami-Dade County Disability and Nondiscrimination Affidavit</b><br/>(Section 2-8.1.5 of the Code of Miami-Dade County)</li> <li>5. <b>Miami-Dade County Debarment Disclosure Affidavit</b><br/>(Section 10.38 of the Code of Miami-Dade County)</li> <li>6. <b>Miami-Dade County Vendor Obligation to County Affidavit</b><br/>(Section 2-8.1 of the Code of Miami-Dade County)</li> <li>7. <b>Miami-Dade County Code of Business Ethics Affidavit</b></li> </ol> | <ol style="list-style-type: none"> <li>8. <b>Miami-Dade County Family Leave Affidavit</b><br/>(Article V of Chapter 11 of the Code of Miami-Dade County)</li> <li>9. <b>Miami-Dade County Living Wage Affidavit</b><br/>(Section 2-8.9 of the Code of Miami-Dade County)</li> <li>10. <b>Miami-Dade County Domestic Leave and Reporting Affidavit</b> (Article VIII, Section 11A-60 - 11A-67 of the Code of Miami-Dade County)</li> <li>11. <b>Miami-Dade County Verification of Employment Eligibility (E-Verify) Affidavit</b><br/>(Section 448.095, of the Florida State Statutes)</li> <li>12. <b>Miami-Dade County Pay Parity Affidavit</b><br/>(Resolution No. R-1072-17)</li> <li>13. <b>Miami-Dade County Suspected Workers' Compensation Fraud Affidavit</b></li> </ol> |
|--|--|

(Resolution No. R-919-18)

Dade County and Title 49 of the Code of Federal Regulations.

**14. Office of the Inspector General**  
(Section 2-1076 of the Code of Miami-Dade County)

**15. Small Business Enterprises**  
The County endeavors to obtain the participation of all small business enterprises pursuant to Sections 2-8.1.1.1.1, 2-8.1.1.1.2 and 2-8.2.2 of the Code of Miami-

**16. Antitrust Laws**  
By acceptance of any contract, the Contractor agrees to comply with all antitrust laws of the United States and the State of Florida.

b) Conflict of Interest and Code of Ethics

Sections 2-11.1 (c) and (d) of the Code require that any County official, agency/board member or employee, or any member of his or her immediate family who, through a firm, corporation, partnership or business entity, has a financial interest, direct or indirect, with Miami-Dade County or any person or agency acting for Miami-Dade County, competing or applying for a contract, must first obtain and submit a written conflict of interest opinion from the County's Ethics Commission prior to the official, agency/board member or employee, or his or her immediate family member entering into any contract or transacting any business with Miami-Dade County or any person or agency acting for Miami-Dade County. Any such contract or business transaction entered in violation of these subsections, as amended, shall be rendered voidable. All County officials, autonomous personnel, quasi-judicial personnel, advisory personnel, and employees wishing to do business with the County are hereby advised they must comply with the applicable provisions of Section 2-11.1 of the Conflict of Interest and Code of Ethics Ordinance.

**ARTICLE 53 INSPECTOR GENERAL REVIEWS**

- a) Pursuant to Miami-Dade County Administrative Order No. 3-20, the County has the right to retain the services of an Independent Private Sector Inspector General (the "IPSIG"), whenever the County deems it appropriate to do so. Upon written notice from the County, the Contractor shall make available to the IPSIG retained by the County, all requested records and documentation pertaining to this Agreement for inspection and reproduction. The County shall be responsible for the payment of these IPSIG services, and under no circumstance shall the Contractor's prices and any changes thereto approved by the County, be inclusive of any charges relating to these IPSIG services. The terms of this provision apply to the Contractor, its officers, agents, employees, Subcontractors, and assignees. Nothing contained in this provision shall impair any independent right of the County to conduct an audit or investigate the operations, activities, and performance of the Contractor in connection with this Agreement. The terms of this Article shall not impose any liability on the County by the Contractor or any third party.
- b) Nothing contained above shall in any way limit the powers of the Inspector General to perform audits on all County contracts including, but not limited to, those contracts specifically exempted above. The Miami-Dade County Inspector General is authorized and empowered to review past, present, and proposed County and Trust contracts, transactions, accounts, records, and programs. In addition, the Inspector General has the power to subpoena witnesses, administer oaths, require the production of records, and monitor existing projects and programs. Monitoring of an existing project or program may include a report concerning whether the project is on time, within budget and in conformance with plans, specifications, and applicable law. The Inspector General is empowered to analyze the necessity of and reasonableness of proposed change orders to the Contract. The Inspector General is empowered to retain the services of IPSIGs to audit, investigate, monitor, oversee, inspect, and review operations, activities, performance and procurement process, including but not limited to project design, specifications, proposal submittals, activities of the Contractor, its officers, agents and employees, lobbyists, County staff and elected officials to ensure compliance with contract specifications and to detect fraud and corruption.
- c) Upon written notice to the Contractor from the Inspector General or IPSIG retained by the Inspector General, the Contractor shall make all requested records and documents available to the Inspector General or IPSIG for inspection and copying. The Inspector General and IPSIG shall have the right to inspect and copy all documents and records in the Contractor's possession, custody or control which, in the Inspector General's or IPSIG's sole judgment, pertain to performance of the Contract, including, but not limited to original estimate files, change order estimate files, worksheets, proposals and agreements form and which successful and unsuccessful Subcontractors and suppliers, all project-related correspondence, memoranda, instructions, financial documents, construction documents, proposal and contract documents, back-charge documents, all documents and records which involve cash, trade or volume discounts, insurance proceeds, rebates, or dividends received, payroll and personnel records, and supporting documentation for the aforesaid documents and records.

**ARTICLE 54 FEDERAL, STATE, AND LOCAL COMPLIANCE REQUIREMENTS**

As applicable, Contractor shall comply, subject to applicable professional standards, with the provisions of all applicable federal, state and the County orders, statutes, ordinances, rules and regulations which may pertain to the Services required under this Agreement, including, but not limited to:

- a) Equal Employment Opportunity clause provided under 41 C.F.R. Part 60-1.3 in accordance with Executive Order 11246, "Equal Employment Opportunity", as amended.
- b) Miami-Dade County Small Business Enterprises Development Participation Provisions.
- c) The Clean Air Act (42 U.S.C. § 7401-7671q.) and the Federal Water Pollution Contract Act (33 U.S.C. §§ 1251-1387), as amended.
- d) The Davis-Bacon Act (40 U.S.C. §§ 3141-3144 and 3146-3148) as supplemented by the Department of Labor regulations (29 C.F.R. Part 5).
- e) The Copeland "Anti-Kickback" Act (40 U.S.C. § 3145) as supplemented by the Department of Labor regulations (29 C.F.R. Part 2).
- f) Section 2-11.1 of the Code of Miami-Dade County, "Conflict of Interest and Code of Ethics".
- g) Section 10-38 of the Code of Miami-Dade County, "Debarment of Contractors from County Work".
- h) Section 11A-60 - 11A-67 of the Code of Miami-Dade County, "Domestic Leave".
- i) Section 21-255 of the Code of Miami-Dade County, prohibiting the presentation, maintenance, or prosecution of false or fraudulent claims against Miami-Dade County.
- j) The Equal Pay Act of 1963, as amended (29 U.S.C. § 206(d)).
- k) Section 448.07 of the Florida Statutes "Wage Rate Discrimination Based on Sex Prohibited".
- l) Chapter 11A of the Code of Miami-Dade County (§ 11A-1 *et seq.*) "Discrimination".
- m) Chapter 22 of the Code of Miami-Dade County (§ 22-1 *et seq.*) "Wage Theft".
- n) Chapter 8A, Article XIX, of the Code of Miami-Dade County (§ 8A-400 *et seq.*) "Business Regulations".
- o) Any other laws prohibiting wage rate discrimination based on sex.
- p) Byrd Anti-Lobbying Amendment (31 U.S.C. § 1352).
- q) Executive Order 12549 "Debarment and Suspension", which stipulates that no contract(s) are "to be awarded at any tier or to any party which is debarred or suspended or is otherwise excluded from or ineligible for participation in Federal assistance programs".
- r) The prohibitions against discrimination on the basis of age under the Age Discrimination Act of 1975 (42 U.S.C. §§ 6101-07) and regulations issued pursuant thereto (24 C.F.R. Part 146).

Pursuant to Resolution No. R-1072-17, by entering into this Contract, the Contractor is certifying that the Contractor is in compliance with, and will continue to comply with, the provisions of items "f" through "k" above.

The Contractor shall hold all licenses and/or certifications, obtain and pay for all permits and/or inspections, and comply with all laws, ordinances, regulations and building code requirements applicable to the work required herein. Damages, penalties, and/or fines imposed on the County or Contractor for failure to obtain and maintain required licenses, certifications, permits and/or inspections shall be borne by the Contractor. The Project Manager shall verify the certification(s), license(s), and permit(s) for the Contractor prior to authorizing Work and as needed.

Notwithstanding any other provision of this Agreement, Contractor shall not be required pursuant to this Agreement to take any action or abstain from taking any action if such action or abstention would, in the good faith determination of the Contractor, constitute a violation of any law or regulation to which Contractor is subject, including but not limited to laws and regulations requiring that Contractor conduct its operations in a safe and sound manner.

#### **ARTICLE 55     NONDISCRIMINATION**

During the performance of this Contract, Contractor agrees to not discriminate against any employee or applicant for employment because of race, color, religion, ancestry, national origin, sex, pregnancy, age, disability, marital status, familial status, sexual orientation, gender identity or gender expression, status as victim of domestic violence, dating violence or stalking, or veteran status, and on housing related contracts the source of income, and will take affirmative action to ensure that employees and applicants are afforded equal employment opportunities without discrimination. Such action shall be taken with reference to, but not limited to recruitment, employment, termination, rates of pay or other forms of compensation, and selection for training or retraining, including apprenticeship and on the job training.

By entering into this Contract, the Contractor attests that it is not in violation of the Americans with Disabilities Act of 1990 (and related Acts) or Miami-Dade County Resolution No. R-385-95. If the Contractor or any owner, subsidiary or other firm affiliated with or related to the Contractor is found by the responsible enforcement agency or the County to be in violation of the Act or the Resolution, such violation shall render this Contract void. This Contract shall be void if the Contractor submits a false affidavit pursuant to this Resolution or the Contractor violates the Act or the Resolution during the term of this Contract, even if the Contractor was not in violation at the time it submitted its affidavit.

#### **ARTICLE 56     CONFLICT OF INTEREST**

The Contractor represents that:

- a) No officer, director, employee, agent, or other consultant of the County or a member of the immediate family or household of the aforesaid has directly or indirectly received or been promised any form of benefit, payment, or compensation, whether tangible or intangible, in connection with the award of this Agreement.
- b) There are no undisclosed persons or entities interested with the Contractor in this Agreement. This Agreement is entered into by the Contractor without any connection with any other entity or person making a proposal for the same purpose, and without collusion, fraud or conflict of interest. No elected or appointed officer or official, director, employee, agent, or other consultant of the County, or of the State of Florida (including elected and appointed members of the legislative and executive branches of government), or a member of the immediate family or household of any of the aforesaid:
  - i) is interested on behalf of or through the Contractor directly or indirectly in any manner whatsoever in the execution or the performance of this Agreement, or in the Services, Deliverables or Work, to which this Agreement relates or in any portion of the revenues; or
  - ii) is an employee, agent, advisor, or consultant to the Contractor or to the best of the Contractor's knowledge any Subcontractor or supplier to the Contractor.
- c) Neither the Contractor nor any officer, director, employee, agency, parent, subsidiary, or affiliate of the Contractor shall have an interest which is in conflict with the Contractor's faithful performance of its obligation under this Agreement; provided that the County, in its sole discretion, may consent in writing to such a relationship, provided the Contractor provides the County with a written notice, in advance, which identifies all the individuals and entities involved and sets forth in detail the nature of the relationship and why it is in the County's best interest to consent to such relationship.
- d) The provisions of this Article are supplemental to, not in lieu of, all applicable laws with respect to conflict of interest. In the event there is a difference between the standards applicable under this Agreement and those provided by statute, the stricter standard shall apply.
- e) In the event Contractor has no prior knowledge of a conflict of interest as set forth above and acquires information which may indicate that there may be an actual or apparent violation of any of the above, Contractor shall promptly bring such information to the attention of the Project Manager. Contractor shall thereafter cooperate with the County's review and investigation of such information and comply with the instructions Contractor receives from the Project Manager regarding remedying the situation.

**ARTICLE 57 PRESS RELEASE OR OTHER PUBLIC COMMUNICATION**

Under no circumstances shall the Contractor without the express written consent of the County:

- a) Issue or permit to be issued any press release, advertisement or literature of any kind which refers to the County, or the Work being performed hereunder, unless the Contractor first obtains the written approval of the County. Such approval may be withheld if for any reason the County believes that the publication of such information would be harmful to the public interest or is in any way undesirable; and
- b) Communicate in any way with any contractor, department, board, agency, commission or other organization or any person whether governmental or private in connection with the Work to be performed hereunder except upon prior written approval and instruction of the County; and
- c) Except as may be required by law, the Contractor and its employees, agents, Subcontractors, and suppliers will not represent, directly or indirectly, that any Work, Deliverables or Services provided by the Contractor or such parties has been approved or endorsed by the County.

**ARTICLE 58 BANKRUPTCY**

The County may terminate this Contract, if, during the term of any contract the Contractor has with the County, the Contractor becomes involved as a debtor in a bankruptcy proceeding, or becomes involved in a reorganization, dissolution, or liquidation proceeding, or if a trustee or receiver is appointed over all or a substantial portion of the property of the Contractor under federal bankruptcy law or any state insolvency law.

**ARTICLE 59 GOVERNING LAW**

This Contract, including appendices, and all matters relating to this Contract (whether in contract, statute, tort (such as negligence), or otherwise) shall be governed by, and construed in accordance with, the laws of the State of Florida. Venue shall be in Miami-Dade County.

**ARTICLE 60 INTEREST OF MEMBERS, OFFICERS OR EMPLOYEES AND FORMER MEMBERS, OFFICERS OR EMPLOYEES**

No member, officer, or employee of the County, no member of the governing body of the locality in which the Project is situated, no member of the governing body in which the County was activated, and no other public official of such locality or localities who exercises any functions or responsibilities with respect to the project, shall, during his or her tenure, or for one year thereafter, have any interest, direct or indirect, in this Contract or the proceeds thereof.

**ARTICLE 61 LIENS**

The Contractor is prohibited from placing a lien on County property. This prohibition shall apply to all Subcontractors.

**ARTICLE 62 FIRST SOURCE HIRING REFERRAL PROGRAM**

Pursuant to Section 2-2113 of the Code, for all contracts for goods and services, the Contractor, prior to hiring to fill each vacancy arising under a County contract shall (1) first notify Career Source South Florida ("CSSF"), the designated Referral Agency, of the vacancy and list the vacancy with CSSF according to the Code, and (2) make good faith efforts as determined by the County to fill a minimum of fifty percent (50%) of its employment needs under the County contract through the CSSF. If no suitable candidates can be employed after a Referral Period of three to five days, the Contractor is free to fill its vacancies from other sources. Contractor will be required to provide quarterly reports to the CSSF indicating the name and number of employees hired in the previous quarter, or why referred candidates were rejected. Sanctions for non-compliance shall include, but not be limited to: (i) suspension of Contract until Contractor performs obligations, if appropriate; (ii) default and/or termination; and (iii) payment of \$1,500/employee, or the value of the wages that would have been earned given the noncompliance, whichever is less. Registration procedures and additional information regarding the First Source Hiring Referral Program are available at <https://iapps.careersourcesfl.com/firstsource/>.

**ARTICLE 63     PUBLIC RECORDS AND CONTRACTS FOR SERVICES PERFORMED ON BEHALF OF MIAMI-DADE COUNTY**

The Contractor shall comply with the Public Records Laws, including by not limited to, (1) keeping and maintaining all public records that ordinarily and necessarily would be required by the County in order to perform the service; (2) providing the public with access to public records on the same terms and conditions that the County would provide the records and at a cost that does not exceed the cost provided in Chapter 119, Florida Statutes, or as otherwise provided by law; (3) ensuring that public records that are exempt or confidential and exempt from public records disclosure requirements are not disclosed except as authorized by law; and (4) meeting all requirements for retaining public records and transferring, at no cost, to the County all public records in possession of the Contractor upon termination of the Contract and destroying any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements upon such transfer. In addition, all records stored electronically must be provided to the County in a format that is compatible with the information technology systems of the County. Failure to meet any of these provisions or to comply with Florida's Public Records Laws as applicable shall be a material breach of this Agreement and shall be enforced in accordance with the terms and conditions of the Agreement.

**IF THE CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO THE CONTRACTOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS CONTRACT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT (305) 375-5773, [ISD-VSS@MIAMIDADE.GOV](mailto:ISD-VSS@MIAMIDADE.GOV), 111 NW 1<sup>st</sup> STREET, SUITE 1300, MIAMI, FLORIDA 33128.**

**ARTICLE 64     VERIFICATION OF EMPLOYMENT ELIGIBILITY (E-VERIFY)**

By entering into this Contract, the Contractor becomes obligated to comply with the provisions of Section 448.095 of the Florida Statutes, titled "Verification of Employment Eligibility". This includes but is not limited to utilization of the U.S. Department of Homeland Security's E-Verify System to verify the employment eligibility of all newly hired employees by the Contractor effective January 1, 2021 and requiring all Subcontractors to provide an affidavit attesting that the Subcontractor does not employ, contract with, or subcontract with, an unauthorized alien. Failure to comply may lead to termination of this Contract, or if a Subcontractor knowingly violates the statute, the subcontract must be terminated immediately. Any challenge to termination under this provision must be filed in the Circuit Court no later than twenty (20) calendar days after the date of termination and the Contractor may be liable for any additional costs incurred by the County resulting from the termination of the Contract. If this Contract is terminated for a violation of the statute by the Contractor, the Contractor may not be awarded a public contract for a period of one year after the date of termination. Public and private employers must enroll in the E-Verify System (<http://www.uscis.gov/e-verify>) and retain the I-9 Forms for inspection.

**ARTICLE 65     ADDITIONAL LICENSES, SOFTWARE, OR SERVICES**

During the term of the contract, the County may purchase additional licenses, hardware, software, or services provided they are available. Each order must refer to this contract and must specify the pricing and delivery terms. Notwithstanding any additional or contrary terms in the order, the applicable provisions of this Contract will govern the purchase and sale of additional licenses, hardware, software, or services. Any modification to the Scope of Works of this Contract will require mutual written agreement between the Contractor and the County.

**ARTICLE 66     CRIMINAL JUSTICE INFORMATION SYSTEMS SECURITY REQUIREMENTS**

Any contract awarded to a private contractor/vendor wherein a software application/program that accesses, processes, and stores Criminal Justice Information (CJI) or Personally Identifiable Information (PII), or the selected private contractor/vendor requires physical or logical access to the MDPD's network which contains CJI or PII, must comply with all security policy requirements outlined in the Florida Department of Law Enforcement's (FDLE) Criminal Justice Information Systems (CJIS) Security Policy. Additionally, the selected private contractor/vendor, and any of its employees or subcontractors, that requires logical access to the MDPD's network must review the attached Federal Bureau of Investigation's (FBI) CJIS Security Addendum (Annex A), and sign the FBI's CJIS Security Addendum Certification (Annex B) upon completion of a state and national fingerprint-based record check, criminal background check, proof of citizenship or authorization to be employed in the United States, biennially. Further, support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.

**ARTICLE 67     CYBERSECURITY AND INFORMATION TECHNOLOGY PROCUREMENT AND PROTECTION PROGRAM**

All purchases of Cybersecurity Products shall abide by [Sec. 2-8.2.6.2](#) of the Code of Miami-Dade County, *titled* Cybersecurity and Information Technology Procurement and Protection Program. The proposed software and/or hardware shall be produced in the United States, with the following exceptions:

- (a) the required Cybersecurity Product is not produced in the United States, or if such required Cybersecurity Product is produced in the United States and it is not of a satisfactory quality to meet the needs of Miami-Dade County;
- (b) upon a written recommendation of the County Mayor and approved by a majority vote of the Board of County Commission members present, compliance with the procurement and contracting requirements of [Sec. 2-8.2.6.2](#) of the Code of Miami-Dade County, is not consistent with the best interests of the public; or,
- (c) the Cybersecurity Product is purchased from a company or subsidiary that is not on the list of prohibited telecommunications companies in the John S. McCain National Defense Authorization Act for Fiscal Year 2019, [Public Law 115-232](#), as that list may be amended from time.

Contractor's employees who have access to County owned, licensed, or operated Cybersecurity Products shall be subject to Heightened Security Review prior to such employees being granted access to County Cybersecurity Products.

**ARTICLE 68     TRANSITION**

In the event the County issues a new Agreement after this Agreement expires, the Contractor shall continue to operate and maintain the Solution under the terms and conditions of this Agreement, pending the transition and acceptance of any new Solution and services at each MDCR location. Contractor shall transfer the provided network to MDCR at the expiration of the contract. This shall include all applicable cabling and wireless equipment.

**ARTICLE 69     SURVIVAL**

The Parties acknowledge that any of the obligations in this Agreement will survive the term, termination, and cancellation hereof. Accordingly, the respective obligations of the Contractor and the County under this Agreement, which by nature would continue beyond the termination, cancellation, or expiration thereof, shall survive termination, cancellation or expiration hereof.

IN WITNESS WHEREOF, the Parties have executed this Agreement effective as of the last date that the Agreement is executed below,



Securus Technologies, LLC

Miami-Dade County

By:

*Alex Yeo*

By:

Name:

Alex Yeo

Name:

Daniella Levine Cava

Title:

Chief Revenue and Product Officer

Title:

Mayor

Date:

08/28/2023

Date:

Attest:

*Valerie Strzelecki*

Attest:

Corporate Secretary/Notary Public

Clerk of the Board

Corporate Seal/Notary Seal

Approved as to form and legal sufficiency



Assistant County Attorney

Attachments:

- A. Scope of Work
- B. Price and Payment Schedule
- C. FBI's CJIS Security Addendum (Annex A)
- D. FBI's CJIS Security Addendum Certification (Annex B)
- E. Cloud Service Usage Policy 102119a (003)
- F. Payment Card Industry ("PCI") Security Standards
- G. Information Technology Security Matrix
- H. Functional Requirements Matrix



**CONTRACT NO. RFP-02194**

**DETAINEE ELECTRONIC COMMUNICATIONS AND MEDIA SOLUTION**

**SCOPE OF WORK**

**MIAMI-DADE COUNTY:**

Miami-Dade Corrections and Rehabilitations Department

SCOPE OF WORK

CONTENTS

1.0 Background.....4

2.0 Current Operating Environment .....4

3.0 Purpose.....5

4.0 Contractor Responsibilities .....5

5.0 County Responsibilities.....5

6.0 Certification Requirement .....5

7.0 Codes, Permits, Licenses .....6

8.0 Project Schedule.....6

9.0 Testing Plan.....6

10.0 Project Implementation and Conversion Plans .....7

11.0 Data Conversion and Migration Plan .....7

12.0 Solution Software Support Plan .....8

13.0 Business Continuity and Disaster Recovery Plan .....8

14.0 Solution Maintenance Plan .....8

15.0 Behavioral Rewards Plan.....9

16.0 Solution Components and Functionality.....9

    16.1 General Functionality.....10

    16.2 Industry Standards .....10

    16.3 Administration/Operational Functionality .....11

    16.4 Network Security .....12

    16.5 Application Security .....12

    16.6 Tablet/Kiosk Requirements.....12

    16.7 Communication Requirements .....14

17.0 Content Packages.....21

    17.1 Standard Package.....21

    17.2 Premium Package.....22

18.0 System Updates to Services.....22

19.0 Solution Interface Requirements.....22

20.0 Data Backup/Storage.....26

21.0 System/Data Breach .....27

22.0 Maintenance and Support Commitment.....27

    22.1 Solution Maintenance and Support Plan.....27

    22.2 Customer Support Plan.....28

23.0 Installation Plan.....29

24.0 Training.....29

**SCOPE OF WORK**

25.0	Solution Acceptance .....	30
26.0	Solution Uptime and Downtime.....	30
27.0	Prepaid Accounts.....	31
28.0	Payment Card Industry Compliance .....	31

## SCOPE OF WORK

### 1.0 Background

- A. Miami-Dade County (the County) is the seventh most populous county in the United States and the most populous county east of Chicago with an estimated population of 2.8 million residents. The County also operates the 8th largest jail system in the United States and the largest in the state of Florida. As a thriving, innovative county with one of the most diverse populations in the nation, the County is holistically rethinking what “public safety” means. The County understands its role as a leader in moving its residents toward that holistic definition of “public safety.” The County can continue developing early intervention points and expanding social services to our incarcerated population by building a stronger system of support services for incarcerated and formerly incarcerated individuals, including access to support services, religious services, educational opportunities, job placement, substance abuse counseling, and work toward preventing recidivism.
  
- B. The County intends to utilize the scope of required services (the Solution) to help bridge the gap between our formerly incarcerated citizens and the community. This includes removing the financial burden on many of the families of incarcerated individuals by providing significant amounts of daily phone time, video visits and other services at zero cost, as studies have shown that the success rate of returning citizens from incarceration are significantly higher when there are connections to the community. As such, the County will **not** collect commissions from revenues generated through the resulting contract to further this goal. This will stop many families, friends and loved ones already facing disproportionate amounts of financial inequity in marginalized communities from subsidizing county operations and strengthen their community connections while ensuring that we achieve the lowest possible rates on all services.
  
- C. In all, the Solution will allow the Miami-Dade Corrections and Rehabilitation Department (MDCR) to further strengthen the commitment to our mission to; “Serve our community by providing safe, secure and humane detention of individuals in our custody while preparing them for a successful return to the community.”

### 2.0 Current Operating Environment

#### A. Facility Environment

MDCR presently operates four (4) correctional housing facilities with a total Average Daily Population (ADP) of approximately 4,400 detainees. These facilities include the Pre-Trial Detention Center, TGK Correctional Center, Metro West Detention Center, and the Boot Camp Program.

Metro West Detention Center	TGK Correctional Center	Pre-Trial Detention Center	Boot Camp Program
ADP- 2,300	ADP- 870	ADP- 1,200	ADP-100
Open Dormitory setting	Open Dorm with rooms	1 <sup>st</sup> generation housing	Dormitory housing
40 housing units	19 housing units	84 housing units	4 housing units
Average phone time per Detainee (last 12 months) = 27.5 minutes per day			

#### B. Information Systems Environment

The County’s Enterprise Technology Model has been included in Attachment F and describes the County’s technology environment. The Solution, and each module or component and function thereof, must be capable of operating fully and correctly, completely independently from the County’s technology environment, and shall not, under any circumstances, create interference with any of the systems, devices, or services contained in said environment. Further, the County’s policies for systems utilizing a cloud environment is described in detail within Attachment D – Cloud Service Usage Policy. The Contractor, in coordination and cooperation with MDCR, shall comply with the provisions of Attachment D.

## SCOPE OF WORK

### 3.0 Purpose

Contractor shall provide all detainee kiosks, infrastructure and related equipment, software, and services at no cost to the County. Further, the goals of this project is to better serve individuals in our custody by:

1. Electronically maintaining connections with friends and family.
2. Providing virtual access to an expansive collection of educational courses and material to prepare them for a successful re-entry into society.
3. Providing entertainment sources to keep detainees occupied in positive activities that will improve behavior for increased facility, staff, and detainees' security.
4. Ability to create profiles and resumes to search for employment after incarceration.
5. Support detainees' re-entry to their communities and rebuilding their futures.
6. Transitioning from a paper-based format to a digital environment that will provide:
  - a. uninterrupted access to all detainee service requests (medical, legal, faith based etc.)
  - b. a positive impact on the environment through a reduction of paper usage.
  - c. less physical property to safeguard, search and transport.
  - d. enhanced security through MDCR's ability to monitor detainees' activity using monitoring software.

### 4.0 Contractor Responsibilities

The Contractor shall assume prime contractor responsibility of the Contract to be the sole point of contact with regard to the Solution's installation, maintenance and training. The Contractor shall assume responsibility for all services and equipment obtained under or provided during the contract term.

The Contractor must provide reliable high speed fiber optic cabling and establish and maintain a private wireless network at each facility, at no cost to MDCR.

Except for any wiring or cabling installed by the Contractor within walls, floors, or ceilings of facility structures, all equipment and software provided by the Contractor shall remain the property and responsibility of the Contractor.

### 5.0 County Responsibilities

MDCR will demonstrate reasonable care but will not be liable in the event of loss, destruction, or theft of contractor owned equipment, software, or technical literature to be delivered or to be used in the installation of deliverables. The Contractor is required to retain total liability for the Solution. Except as provided on Attachment B, *Price and Payment Schedule*, At no time will MDCR be responsible or accept liability for any Contractor owned items.

### 6.0 Certification Requirement

Contractor shall at all times for the term of the contract, comply with the following requirements:

Contractor, including through a Subcontractor, must also hold (i) a Certificate of Registration as a General Contractor issued by the State of Florida Construction Industry Licensing Board pursuant to the provisions of Florida Statutes Section 489.115; or (ii) a Certificate of Registration as a General Contractor issued by the State of Florida Construction Industry Licensing Board pursuant to the provisions of Florida Statutes Section 489.117, and hold a Certification of Competency as a General Contractor issued by the Miami-Dade Construction Trades Qualifying Board pursuant to the provisions of Section 10-3(a) of the Miami-Dade County Code.

## SCOPE OF WORK

### 7.0 Codes, Permits, Licenses

The Contractor must comply with all mandatory licensing requirements. The Contractor must furnish and install all equipment, low voltage communication cable, power cables, miscellaneous hardware, and materials in compliance with all applicable codes, whether local, state or federal, and that all permits, or licenses required for installation will be obtained by the Contractor at no cost to MDCR.

### 8.0 Project Schedule

Within 30 days after the date of execution of the contract (Award Date), submit a Project Schedule including, the following:

- A. Identify specific key tasks and duration including an outline of a Quality Control Plan to manage the project to include an estimated timeframe for implementation of services after contract execution. Contractor shall provide a Project Schedule (Gantt Chart), preferably in Microsoft Project, as well as in PDF with the proposal submission, to include approximate timeframes for all implementation phases and key tasks to include activities such as business process review; software customization; County review/approval of deliverables; site preparation; unit, system and acceptance testing; load and balance testing; a phased approach to the training and implementation of the solution and post-implementation support.
- B. Include a project task list and timeline including detailed scope tasks/activities, organized in phases including, but not limited to project management activities, key resources, and estimated hours per key activity in order to facilitate resource availability and allocation.

### 9.0 Testing Plan

- A. Within 30 days after the date of execution of the contract (Award Date), submit a Testing Plan including, the following:
  - a) Overview and introduction of Solution's features and functions.
  - b) Outline of testing strategy.
  - c) Scope and expected duration of each testing phase (i.e., unit testing, integration testing, user acceptance testing, etc.).
  - d) Identify type and quantity of resources (users) for each testing phase (i.e., unit testing, integration testing, user acceptance testing, etc.).
  - e) Identify any systems function that will be tested.
  - f) Description of the procedure for tracking the resolution of any problems encountered during testing.
  - g) Description of the criteria that will be used to determine whether tests have been satisfactorily passed.
  - h) Proposed criteria for completion of testing tasks/phases and for resolution of any identified defects.
- B. Describe the recommended approach to the following types of testing to be performed on the project and the type of assistance to be provided to the County related to:
  - a) Functional Testing
  - b) Integration Testing
  - c) Stress / Performance Testing - User scalability, data volume scalability, load scalability
  - d) Interface Testing
  - e) Conversion Testing
  - f) Capacity Testing - network, hardware
  - g) Testing of Configuration Decisions
  - h) Workflow and Security Testing
  - i) Reliability Testing
  - j) User Acceptance Testing

## SCOPE OF WORK

### 10.0 Project Implementation and Conversion Plans

Within 30 days after the Award Date, submit an Implementation Plan to include, but not limited to, schedules for delivery and installation of hardware and software. The Conversion Plan should describe in detail how the Contractor will introduce its hardware and software. Provide a description of any anticipated challenges and steps to mitigate them.

1. Contractor shall detail their recommended Implementation Plan based upon industry best practices and previous experience and include:
  - a) description of proposed methodology
  - b) project phases
  - c) team roles, including subcontractors
  - d) milestones/deliverables
  - e) risks
  - f) which tasks are proposed to be completed on-site versus remotely
  - g) in a phased approach, how will active case data be reconciled between legacy systems and the Solution
  - h) critical success factors
  - i) assumptions
2. Provide a detailed description of the proposed use of County resources for the implementation of the Solution, including a County staffing plan outlining the anticipated role (i.e., subject matter expertise, technical support staff, application development), including work expected to be performed by County staff including:
  - a) List all key positions that will be required by Miami-Dade County for all phases of this project (e.g., project management, operational subject matter experts from MDCR and any other entity).
  - b) Describe the role and responsibility for each County position.
  - c) For key County positions listed above (e.g., Project Manager, System Administration and Technical positions), please describe all required knowledge, skills and abilities.
  - d) Describe the estimated level of effort and associated timeframes (e.g., percentage of an FTE) that will be required by each of the identified County positions for each phase of the project.

### 3. Solution Implementation and Configuration

Contractor shall describe their build and release approach, including at minimum:

- Required level of effort based on the expected configuration and customization work
- Software configuration approach including check-in and check-out procedures
- Software development approach including check-in and check-out procedures
- Code management approach and documentation
- Any other key activity.

For each of the above, the Contractor shall detail expected deliverables, the Contractor and County's respective responsibilities, and acceptance criteria.

### 11.0 Data Conversion and Migration Plan

Within 30 days after the Award Date, submit the Data Conversion and Migration Plan with requirements set forth by MDCR, address the following questions when preparing the plan:

- a) What County resources do you anticipate will be required for data migration and conversion?
- b) What are the County's responsibilities?

## SCOPE OF WORK

- c) What is your approach regarding definition of data mapping rules?
- d) What is your approach for the conversion and loading of digital images?
- e) How does your approach address extraction, transformation, staging, cleansing and validation?
- f) Is the County or Contractor responsible for cleansing County data prior to migration?
- g) What strategies do you employ to conduct the final conversion process?

### 12.0 Solution Software Support Plan

Within 60 days after the Date of Award, submit a Solution Software Support Plan that identifies:

- A. Solution maintenance, support, and change management including but not limited to: new software releases, software upgrades, updates, patches, bug fixes, and optional software features. Contractor shall provide documentation of quality control processes used to ensure the integrity of the software, application data, and future changes/patches.
- B. Describe the product release cycle including, but not limited to:
  - 1. Frequency of updates/enhancements or new versions (major and minor version releases).
  - 2. Contents of a release.
  - 3. Availability of release notes.
  - 4. Information contained in release notes (including known issues).
- C. Describe the degree to which the County will be able to configure/customize the Solution including:
  - 1. How does the Contractor define customization versus configuration?
  - 2. How are code tables / pick list values managed, both manually and via automated synchronization from external systems?
  - 3. Change existing workflows for reviewing and approving reports/records within the system, or creating new workflows entirely.
- D. Describe the process for managing local configurations/customizations.

### 13.0 Business Continuity and Disaster Recovery Plan

Within 30 days after the Award Date, submit a Business Continuity and Disaster Recovery Plan that includes procedural processes in the following categories:

- a) Hardware redundancy at the primary site for critical servers and components
- b) Contingency site hardware requirements, including environmental requirements
- c) Replication methodology and software requirements
- d) Estimated bandwidth requirements for internal networking
- e) Backup methodology for data and environmental software
- f) Methodology for handling downtime with relevant manual procedures, if any, to include recovery
- g) Failover procedures
- h) Recovery Time Objective (RTO) & Recovery Point Objective (RPO)
- i) Testing methodology

### 14.0 Solution Maintenance Plan

Within 90 days after the Award Date, submit a Solution Maintenance Plan that includes:

## SCOPE OF WORK

- A. The approach to the Solution maintenance, support, and change management including but not limited to: new software releases, software upgrades, updates, patches, bug fixes, and optional software features. Contractor shall provide documentation of quality control processes used to ensure the integrity of the software, application data, and future changes/patches.
- B. A detailed explanation of the post-implementation support to be provided for the Solution following Go-Live. Identify the resources to be committed to providing post-implementation support including role and responsibility. Include total duration in calendar days, hours of support, type of support (i.e., on-site, remote), and number of resources.
- C. A detailed description of the technical support and help desk services proposed. Include details regarding (i) opening a support ticket, (ii) electronic ticketing, (iii) weekly case reporting, (iv) number of steps to reach live support, and (v) other hardware/workstation support.

### **15.0 Behavioral Rewards Plan**

Within 6 months after the Award Date, submit a Behavioral Rewards Plan, in collaboration with MDCR, which defines a program that provides MDCR with the ability to have a Behavioral Rewards platform for Detainees. This platform will enable Detainees to earn credits to purchase premium items based on a behavior award system and the completion of educational material, as structured in the plan. MDCR will be responsible for all content costs related to the behavioral rewards plan.

### **16.0 Solution Components and Functionality**

Contractor shall provide a Solution with tablets, stationary and mobile kiosks through a secure wireless system that allows detainees to use a mobile device, analogous to commercial tablets, but with security and survivability features specialized for the MDCR environments. The Solution must access a secure, private Wi-Fi network within the facilities and make use of applications including but not limited to:

- a) (VOIP) Phone calling
- b) Video Visitation
- c) Educational and self-improvement programs, including religious materials
- d) E-mail and electronic messaging
- e) Legal Mail solution
- f) Detainee Personal Mail solution
- g) Facility Information/Notifications
- h) Entertainment (music, games, e-books)
- i) Commissary ordering online
- j) Electronic submission and tracking of requests and grievances
- k) Communications services to be managed by the Contractor for the reporting of system issues related to phones, videos, and tablets by Detainees.
- l) Ability to interface with any MDCR applications
- m) Communication monitoring/Investigative software
- n) Ability to audit inventory of tablets on a routine basis

The Contractor must confirm product solutions are part of an integrated solution owned by Contractor. The County desires a one-to-one detainee ratio for the Solution. The County requires the use of a reliable, proven state-of-the art technology for all of the components of the Solution. The County will work with the Contractor to coordinate all telecommunication, conduits, and data cabling needs; however, the Contractor shall be responsible for ensuring the successful installation and implementation of the Solution including all costs, The County reserves the right to request access to the Contractor's network for use of partner system devices as may become needed during the term of the contract and as agreed upon by both parties The County is seeking a Solution with 24/7 high availability, that is fault-tolerant with no single point of failures.

**SCOPE OF WORK**

The Solution should include the following functionality/components to support the described operational needs of the County:

1. Tablets, Mobile Kiosks, Stationary Kiosks, and adequate charging stations.
2. Americans with Disabilities Act (ADA) compliant
3. Communications network linking of all the above equipment.
4. Payment processing tools and applications.
5. Software as a service (SAS) through a cloud-based service that includes separate production, development and disaster recovery environments.
6. Ability to separately configure the Solution for County business rules.
7. The quantity of mobile kiosks and stationary kiosks shall be based on periodic site surveys. The quantity of such equipment may change as mutually agreed by the parties.

Below are the estimated quantities to be confirmed by site surveys:

Tablets	Mobile Kiosks	Stationary Kiosks
4,400 (1:1 Detainee to Tablet Ratio) 50 (MDCR Staff) 10%(replacement of inoperable tablets)	24	600

**16.1 General Functionality**

The Solution shall include, but not be limited to, the following functional specifications:

1. Proprietary operating system (OS). Commercial tablets are not acceptable.
2. Detainee telephone calling from Tablets, Mobile or Stationary Kiosks. Solution must prevent detainee from calling emergency services i.e., 911.
3. Detainee visitation management.
4. Video Visitation capabilities.
5. Interface with Miami-Dade Public Library’s digital content for detainees’ consumption, which is not in conflict with media offered by the Contractor (Option).
6. Mobile and fixed device menus, online messaging and postings, Detainee regular and medical requests, grievances, educational content, and etc., must be, trilingual. The applicable languages are English, Spanish, and Creole. The ability to translate to additional languages is beneficial but not a requirement.
7. Effectively, efficiently, and expeditiously interface with all current and future technology systems providing services to MDCR as requested by MDCR to reduce redundant data entry, avoid unnecessary duplication of services, and increase efficiencies.

**16.2 Industry Standards**

The Solution shall include, but not be limited to, the following functional specifications:

1. Comply with all applicable Federal, State, and local Americans with Disabilities Act (ADA) standards to include DISABILITY RIGHTS FLORIDA, INC., CASE NO.: 2019-CA-2825 settlement agreement between Florida Department of Corrections and Disability Rights Florida.
2. Deploy as a wireless network with the ability to wirelessly provide updates to Operating System, devices and applications, including security patches or fixes. Security updates shall be implemented within 30 days of release.
3. Provide a minimum of ten (10) Video Relay service devices to serve the hearing-impaired detainees.
4. Provide a minimum of five (5) UbiDuo3 wireless devices or comparable device and/or software for MDCR staff to communicate with detainees who are deaf or hard of hearing.
5. Conform to the most current CJIS Security Policy

## SCOPE OF WORK

### 16.3 Administration/Operational Functionality

The Solution shall include, but not be limited to, the following functional specifications:

1. Allow integrations to support MDCR custom analytic tools.
2. Communication monitoring/investigative software.
3. Ability to generate analytic reports for MDCR to respond to trends.
4. Ability to block service to any particular detainee for any particular amount of time and to remotely power off tablets and kiosk(s) using administrative tools.
5. Allow MDCR supervisory staff the ability to assign varying access rights to administrators based on their respective role.
6. Ability to receive/deliver secure privileged mail electronically.
7. Ability to scan existing detainee legal mail/documents and personal mail to digital format available via Detainee profile.
8. Ability to enable communications from a Detainee to the Contractor to resolve any questions, problems, or concerns regarding charges, refunds, or other financial inquires. MDCR will not be involved in any financial matters.
9. Ability to configure so that the Detainee must use an individual PIN at login. Cameras must be disabled via the software and are only active for video visits and when taking the Detainee's photo at login or for other security purposes.
10. Allow MDCR to conduct surveys and communicate/notify Detainees of new policy/statements/messages and keep track of acknowledgement or completion.
11. Content may be streamed or downloaded. Detainees shall not own any content.
12. Provide personal cloud storage at no cost that holds Detainees' files such as email, photos, and other document content. This feature shall provide Detainees with the ability to retrieve their digital content up to thirty (30) days post release from MDCR custody.
13. All data transferred to or from the tablets and kiosks must be wireless. No physically wired connection may be required to send messages or send and/or receive data.
14. Electronic messaging. Detainee must be able to receive a photo from friends and family after going through a vetting process.
15. Contain an approved library of music, e-books, movies, and games.
16. Provide the Detainee the ability to login to any tablet or kiosk to access their personal account.
17. Electronic submission and tracking of requests and grievances, including the ability to customize both systems to follow MDCR's current workflow.
18. Interface with the County's Mug shot System that provides photographs of all Detainees booked into custody in Miami-Dade County.
19. Controlled profile access; Detainees' profiles can only be accessed in their assigned cell location; to prevent unauthorized access to their profile.
20. Unlimited remote system access by users defined in MDCR based on Active Directory roles, broken down into multiple categories and capabilities, e.g., Super User – can record, view, download, burn, etc.
21. Radio Frequency transmitters for all unit televisions in all and future MDCR facilities. Radio frequency receivers shall be installed on all tablets and kiosks at no charge for usage.
22. Various charging options, i.e., wall-mounted and rolling mobile charging stations.
23. Caption Telephone software to accommodate detainees who can speak but cannot hear on the telephone.
24. Wide range of Talking/audio Books to accommodate visually impaired Detainees.
25. Text-to-speech software and training on its use to accommodate visually impaired Detainees.
26. Solution must log and retain all detainee and administrators logging and activity history for a given period. All changes to Detainee/administrator accounts shall be logged and retained.

## SCOPE OF WORK

### 16.4 Network Security

The Contractor must meet the following network security requirements:

1. Provide network and control internet access.
2. Network appliance must have access control lists that are capable of a 1) deny all or 2) whitelist approach.
3. Network appliance must have stateful inspection with 1) attack checking and 2) automatically discard traffic initiated from the internet.
4. Network appliance must have firewall and content filter capabilities
5. Network appliance must deploy only with Contractor's circuit so that only the Contractor's engineers have access to firewall.
6. Ability to encrypt transmitted data and authentication information.
7. Support for Secure Socket Layer (SSL) 128 bit and 256-bit encryption.
8. Contractor shall conduct interference (including network, Wi-Fi, or radio systems) testing prior to deployment and provide report to MDCR for review and approval.

### 16.5 Application Security

The Contractor must provide a mobile device management tool capable of the following:

1. Must be a custom solution to meet the needs of MDCR.
2. Built into the Operating System layer to prevent removal.
3. Critical Kiosk settings must be controlled remotely.
4. Ability to disable any Kiosk setting.
5. Ability to shut down any kiosk or group of kiosks remotely.
6. Ability to remotely erase/wipe (brick) device.
7. Ability to alert if device is root kitted (hacked).
8. Updated applications can be installed remotely.
9. Tablet and Kiosk applications can be removed remotely.
10. Provide the ability for each user to be uniquely identified by the existing Jail Number.
11. Provide basic authentication through use of PIN/Passwords.
12. Provide the ability to enforce password expiration.
13. Provide the ability to require automatic password expirations when initially assigned or reset.
14. Provide ability to support and configure complex password parameters such as password lengths, Upper/Lower alpha numeric and special characters configurable by MDCR, and user access to expiration settings and other behaviors.

### 16.6 Tablet/Kiosk Requirements

#### A. Stationary Kiosks

Stationary Kiosk enclosures shall include, but not be limited to, the following:

1. Be made of approved materials and shall meet specifications established and approved by MDCR. Kiosks shall be wall or floor mounted, locked, with no moving parts and equipped with industrial glass touch screen. Kiosks shall be made of non-breakable parts that cannot be fashioned into weapons. Kiosks should have tamper evident seals and/or door alarms to indicate if units have been tampered with or opened and be secured with security screws with unique unlocking tool.
2. Have floor and/or wall anchors. Contractor shall ensure that each kiosk can be easily unsecured from the floor or the wall by personnel authorized by the MDCR.
3. Be free of sharp edges.

## SCOPE OF WORK

4. Comply with all federal, state, and local ADA mandates to include DISABILITY RIGHTS FLORIDA, INC., CASE NO.: 2019-CA-2825 settlement agreement between Florida Department of Corrections and Disability Rights Florida, Inc. for accessible design to ensure ease of access for individuals with disabilities.
5. Supply a minimum of ten (10) Stationary Kiosks with durable security-centered keyboards for compliance with ADA, specifically visually impaired Detainees who could not use the kiosks utilizing the touchscreen. Location of These ADA Compliant Kiosk will be determined by MDCR.
6. Privacy enclosure: The Contractor shall supply a minimum of sixty (60) soundproof video conferencing privacy enclosures for existing facilities as well as any future facilities opened during the terms of this contract. The enclosures shall be same or similarly approved units comparable to Spaceworx Duramate Single POD with wall mounted Kiosk installed inside each unit. These corrections grade privacy enclosures will serve Detainees while engaging in privileged communication with attorneys. Up to four of these units may be required to meet ADA standards. Similar units may be acceptable if approved by the County.

### B. Mobile Kiosks

Contractor must provide a wireless high security rolling mobile Kiosk option (cart mounted) for MDCR high security areas of our Detention Facilities, at MDCR's discretion, with a minimum of six (6) at each facility as defined by MDCR, that addresses such needs as administrative segregation. MDCR facility staff will wheel the mobile/cart Kiosk to cells or dayrooms for Detainee usage.

The mobile/cart Kiosk instruments shall:

1. Be on a rigid cart with wheel castors, sufficiently sized to easily fit through thirty-six (36) inch doors and fit through the security flap.
2. The headset cord must be in armored flex tubing and must be permanently attached to the cart
3. Hardened, proven in the corrections environment device and not an off-the-shelf product.

Any departure from these specifications must be approved in writing by the MDCR Project Manager or designee.

### C. Tablets

Hardware and accessory capabilities must include the following:

1. Hardened, proven in the corrections environment device and not an off-the-shelf product.
2. Case should be either sealed or accessible only by security screws with unique unlock tool.
3. USB charging of tablets and mobile kiosks is not allowed. Preferred Scored - docked charging - the charging port attaches to and charges the tablets and kiosks via a magnetic connection. Tablets and Mobile Kiosks must not be able to be used to charge other devices. Any access ports must not allow data transfer by the Detainee.
4. Flame Resistant
5. Military Drop Tested
6. At least 32GB of onboard RAM, a battery of at least 8000mAh
7. Minimum 7" Screen Size
8. Non-Removable Lithium Battery
9. A variety of Tablet and Mobile Kiosk Charging Systems Available (i.e., mobile cart, secured wall units)
10. No working speakers, audio can only be activated by the use of headphones. Contractor must supply all Detainees with a pair of headphones, additional headphones may be purchased by the Detainee through commissary.

In addition to the tablets provided to Detainees, the Contractor shall provide a minimum of 50 administrative tablets with the ability to process, reply, and perform job functions with Detainees remotely and wirelessly. Tablets shall include, but not be limited to, the specifications listed in Section D below.

## SCOPE OF WORK

### D. Detainee Tablet and Kiosk Security Requirements

Tablet and Kiosk hardware security requirements should include the following:

1. Exoskeleton with a clear view of tablet and mobile kiosk components (so facility staff can visually inspect devices for physical intrusion and/or hardware modification)
2. USB port should not recognize human interface devices (i.e., keyboards).
3. USB port should not recognize Ethernet connections.

Tablet and Kiosk operating system security must include the following:

1. Locked bootloader (Only Operating Systems digitally signed by Contractor can be installed)
2. Custom OS that removes risky OS features such as safe boot, factory reset, command line access, blue tooth, wireless tethering, etc.
3. OS should be capable of remote management that is inaccessible to Detainees.
4. Should have custom software for communicating with tablets and mobile kiosks from a connected computer; tablets and mobile kiosk should be devoid of any standard communication tools.
5. All installed applications should be evaluated and approved by certified security experts in the field.
6. Wireless security provides the ability to remotely monitor the airspace of the prison and all wirelessly connected devices for security breaches.
7. Contractor shall monitor wireless activity and provide tools for facility security staff to monitor all wireless activity.
8. System should be able to remotely measure signal strength and noise floor of all tablets and mobile kiosks.

Instrument requirements are based on current technology and facility need. New technology and/or Instruments determined to be better suited for the custody and detention environment may be substituted at the request of County or Contractor with County approval of the Agreement.

### 16.7 Communication Requirements

The Solution shall include, but not be limited to, the following functional specifications:

#### A. Video Visitation Module/Application

The Video Visitation Module/Application should be available on tablets, stationary and mobile kiosks and include the following functionalities:

1. Ability to support multiple onsite visitation centers.
2. Ability to provide multiple off-site visitation centers within Miami Dade County.
3. Ability for staff to enroll, schedule, and manage visitation sessions at each onsite/off-site facility and/or remote visits.
4. Ability for friends and family registration for video visitation to be verified utilizing a government Identification
5. Ability to provide a unified system to manage both onsite and web-based visitation from within the same Client Application.
6. Ability to assign a configurable fee based on visitor type.
7. Ability to configure visitation time slots and visitation policy language.
8. Ability for visitation scheduling system to consider the following factors when allowing/denying visitation: detainee quotas, detainee classification/location, detainee visitation bans, visitor visitation bans, visitor categories, overall visitation time policy, blackout dates or configurable holidays, detainee unavailable due to court, medical, or other reasons.

## SCOPE OF WORK

9. Allow all stations and ancillary components of the system to continue to operate without County staff or Contractor intervention in the event of primary failure.
10. When failover occurs, send an alert displayed to officers using the system.
11. Web-based visitation site that allows users to register, schedule visitation, and conduct web-based visitation.
12. Web-based visitation site that provides interfaces at a minimum in English, Spanish, and Creole.
13. Capability to deliver media to a large variety of devices/operating systems (e.g., computers, tablets, mobile devices, etc.) and platforms.
14. Recording and storage of all friends and families visits and strict non-recording of any privileged visits.
15. Ability to save recording and provide transcriptions of all friends and families visits in real time.
16. Ability to provide Officers with the capability to ban visitors either temporarily or indefinitely based on IP address.
17. System automatically removes a ban upon its expiration without MDCR staff intervention.
18. Allow Attorney visitor records to be clearly distinguishable from other visitor records, via an icon on the record.
19. Allow "In custody" detainee details such as cell location, etc. to be periodically imported into the system.
20. When detainees are released from custody, allow the record to be retained along with the detainee's visitation history.
21. Detainees visit quotas that are configurable based on visits per day, per week, and visits per month.
22. Require the public to accept a visitation policy that is configurable by MDCR prior to scheduling visitation.
23. Allow the public to cancel a visit when the visit is within a predetermined time frame of the visit's start time (e.g., 24 hours), as configured by MDCR.
24. Ability to monitor all friends and family visits in real time.
25. Ability to easily terminate a session from the live monitor screen and input a reason for termination.
26. Headsets at each station to allow the officers to privately monitor and/or conference into a visitation session.
27. Ability to allow investigators to view historical visitation sessions.
28. Ability to define privileged/attorney visit sessions in order to prevent recording.
29. Ability to quickly flag visitation sessions for future investigation.
30. Ability to download certain recordings on an as needed basis.
31. Ability to allow officers to define custom messages that will display on the detainee and visitor screens during a visitation session, at the start and end of a session, each with different possible messages.
32. Ability for MDCR staff to customize an audible file that will play shortly after both parties connect to a visit and near the end of the visit. Ability to define holidays and limit visitation based on holiday schedules.
33. Under no circumstance are privileged video visits to be recorded. Contractor will conduct quarterly self-audits to ensure that no privileged communication is recorded and provide reports to MDCR accordingly.
34. Ability to block visitors that are banned due to a no-contact order, order for protection, or other reasons.

### B. Telephone Module/Application

Tablets, stationary and mobile kiosk solutions must have a phone module with an automated operator, collect call service for local, domestic and for pre-paid calling services. The phone module shall include all necessary telephone platforms and interfaces to CJIS, and all other equipment necessary to perform the functions and services described in the Agreement and the Scope of Work. The phone module must comply with the American with Disabilities Act, the Prison Rape Elimination Act, and the Civil Rights of Institutionalized Persons Act.

The phone module shall include:

1. Ability to require a secondary biometric and voice PIN prior to placing a phone call.
2. Combination PIN and/or biometric features with a 99% cumulative reliability rate - initialization of telephone account to occur at the time of booking, and deactivation at time of release.
3. An interface with the Miami-Dade County Criminal Justice Information System ("CJIS"), the Automated A-Form System, the Detainee Profile System, the Mug-shot system to manage active jail numbers (records) in real time, and any applicable Jail Management System.
4. Customized and comprehensive Call Detail Reports as defined by MDCR.

## SCOPE OF WORK

5. The ability to provide/receive an encrypted file to other law enforcement Agency or State Attorney's Office through a secure FTP site.
6. Perpetual Reverse Phone Number Look-up of all employee/volunteer/contractor phone numbers provided in MDCR's employee system of record database and ability to run large list of staff/ contractors/ volunteers' phone numbers on demand. Ability to receive alerts regarding any staff/contractor/volunteers for receipt of detainee phone calls. The Contractor will ensure that the integrity of this information is protected in accordance with the exemptions stipulated in Florida State Statute 119 titled, "Public Records.
7. Redaction software with the ability to locate and permanently remove personal and sensitive data within the recorded telephone call, as well the ability to encrypt and secure the file.
8. Enhanced security and alert features to show patterns of hotline or toll-free abuse or misuse.
9. Ability to exempt calls by phone number from recording and/or from billing, i.e., attorney's offices and the Public Defender -- but with the ability to have a call record that the call was made, by whom, date, time, status, and duration of the call.
10. Ability to exempt phone numbers from billing of charges (toll free) with all other features of the phone system as defined by MDCR.
11. Automatic hours of operations - ability to schedule active and non-active phone service by facility, cell/unit, or system-wide.
12. Real-time back up of all data, recordings, and information maintained for the life of the Agreement on an archive system.
13. Excellent call clarity and reception to ensure quality recordings and monitoring of information.
14. Recorded record retention in alignment with a schedule mutually agreed upon by the Contractor and MDCR to allow for manual and scheduled off-line archiving of recorded phone calls.
15. System must be capable of sealing and expunging records in compliance with Court Orders.
16. A periodic update of the Florida Bar Directory.
17. A leave behind system of all historical recorded calls, with a solution for all authorized investigators to remotely access the information wherever the system is located.
18. Telephone Module should follow a pre-determined schedule established by MDCR, generally from 8:00 a.m. to 12:00 midnight, from Sunday to Thursday, and 8a.m. to 2a.m., from Friday to Saturday. An exception exists on Holidays when access to telecommunication services may be extended and during other timeframes as granted by MDCR. The exception to this policy is when detainee is in lockdown or on disciplinary confinement.
19. All calls are timed out at 15 minutes. This will not change unless otherwise requested by MDCR.
20. The Telephone Module phone calls must be capable of being monitored, recorded, and archived, with the exception of privileged communication.
21. The recordings of Detainee conversations are considered the property of MDCR. These recordings shall be transferred onto a leave behind system.
22. The Contractor shall flag and archive all Unauthorized Call attempts (incoming and outgoing) and shall generate alert reports to be made available to the MDCR.
23. The Telephone Module shall provide the ability to selectively monitor call activity in real time and initiate appropriate action as necessary.
24. The Telephone Module shall retrieve and generate Detainee Unauthorized Call activity logs for specified periods.
25. Recording and storage of all friends and families calls and strict non-recording of any privileged calls.
26. Ability to save recordings and provide transcriptions of all friends and families calls in real time.
27. The Telephone Module shall be designed for use by the hearing impaired. Provisions for the deaf must comply with Americans with Disabilities Act (ADA) and Telephone Devices for the Deaf (TDD) regulations and standards. A minimum of two (2) TDD Detainee Telephone Instruments are required at each MDCR Department Custody and Detention Facility.
28. The Contractor's automated operator shall be capable of prompting a caller to select the appropriate language by pressing the appropriate keypad digit. The Contractor's automated operator shall be capable of supporting English, Spanish, and Haitian Creole or other languages required by the MDCR Department. The visual training aid to learn how to use the telephone module shall be provided written, verbal, and a video supporting English, Spanish, and Haitian Creole or other languages required by the MDCR Department.

## SCOPE OF WORK

29. When a Detainee places a call, the Telephone Module shall announce the following to the Detainee: “This telephone call is subject to monitoring or recording.” When a call to an authorized number is answered, the MDCR Department Telephone Module shall announce to the recipient of the call the following: “This telephone call is coming from “Detainee’s name”, a detainee at “name of the specific MDCR Department Detention Facility”. This telephone call is subject to monitoring or recording. To consent to the monitoring or recording of this call, please press <keypad digit> now. The use of special calling features is not permitted during this call.” When a call to an authorized number is answered, the Telephone Module shall announce to the recipient of the call the following: “This is “Telephone Contractor”. You have a call from “Detainee’s name”, a detainee in “name of the specific MDCR Department Detention Facility. To accept this call, please press <keypad digit> now. The use of special calling features is not permitted during this call.”
30. The Contractor’s automated operator shall be capable of continuous 24x7x365 operation and Contractor shall ensure line concentration shall not adversely affect Detainee’ ability to initiate and successfully negotiate outbound calls from within an MDCR Custody and Detention Facilities. Adequate bandwidth, lines, equipment, platform efficiencies, etc., in directing and handling calls must be sufficiently pre-considered and provided by the Contractor to ensure the County’s connect call ratio remains in the 99-100% range.
31. The Contractor’s automated operator shall support the capability to program shut-downs by Detainee profile, cellblock, floor, day room, dormitory, pod, facility, or System-wide features that will enable/disable Detainee telephone operations by time of day or day of week. MDCR will have the ability via designated System Administrative Workstations to perform shutdowns when needed.
32. The Contractor’s automated operator shall be capable of setting call duration limits by telephone, cellblock, floor, day room, dormitory, pod, facility, or system-wide remotely from the System Administrative Workstations provided under this Scope of Work.
33. The Contractor’s automated operator shall identify the Detainee to the called party by recording his/her spoken name, in response to the pre-recorded System prompt.
34. The Contractor’s automated operator shall verify that a destination number called is an authorized number (not blocked or restricted), prior to placing a Collect Call to the destination telephone number. If the Collect Call is to an authorized number, then call set-up shall continue and placement of the detainee’s call to the destination number is accomplished. If the Collect Call is to an unauthorized number (Unauthorized Call) or blocked number (Blocked Call), then the Collect Call shall be blocked, and the detainee notified that the call to an unauthorized or blocked telephone number will not be completed.
35. The Contractor’s automated operator shall provide for free and unlimited calls to the Detainee’s private Attorney or public defender. Such calls shall not be monitored or recorded by the Telephone Module. Prior to completing a connection, the Telephone Module shall compare the dialed number with a list of telephone numbers known to be private attorneys and/or public defenders. This list shall be compiled from the Florida Bar Association and approved by the MDCR Professional Compliance Division and be capable of being updated or modified frequently. If a number appears on this list, the Telephone Module must automatically disable monitoring and recording of that call.
36. All requests received by the Contractor from attorneys for inclusion on the list of non-recorded numbers shall be forwarded to the MDCR Professional Compliance Division. MDCR Professional Compliance Investigative Unit personnel will have the option to physically input approved attorney telephone numbers. This electronic listing shall be maintained by the Contractor’s System in such a manner that record of any additions, edits, and deletions are archived and able to be queried and immediately retrieved upon request by the County. The master listing and archived records shall be accessible via specified System Administrative Workstations by the MDCR Project Director and MDCR Project Manager and designated administrative and/or specified MDCR Professional Compliance investigative personnel.
37. The Contractor’s automated operator shall provide for Collect Calls and Pre-Paid Calls, as permitted in accordance with procedures authorized by the MDCR Project Manager or designee. The call recipient shall have the option to refuse calls from the Detainee, either by blocking the call by keypad entry or by written notification to the MDCR Project Manager or designee indicating that they do not wish to receive calls from the Detainee. Requests to unblock any currently blocked numbers shall be processed in accordance with procedures authorized by the MDCR Project Manager or designee.

## SCOPE OF WORK

38. The Contractor's Telephone Module must have ability to build a timetable for Pro Se calls that are on flexible timetable, with the ability to add specific telephone numbers, and allow recorded or not recorded call selections, which can be created by MDCR Project Manager, and designated administrative and/or specified MDCR Professional Compliance investigative personnel.
39. The Contractor's automated operator shall prevent all incoming calls to tablets and mobile/stationary kiosks in MDCR Detention Facilities. Any attempted incoming calls shall be rejected, and appropriate information (if available) shall be recorded, archived and reported to the County Project Manager or designee.
40. The Contractor's Telephone Module must have ability to build a pre-approved phone number list.
41. The Contractor's automated operator shall maintain a database containing blocked telephone numbers. The Telephone Module shall be capable of blocking calls by area code, prefix, or destination numbers. A master listing of blocked numbers shall be available for query/review at any time electronically on System Administrative Workstations provided under this Scope of Work.
42. The Telephone Module shall also afford a means for the MDCR Project Manager, and the designees, including Professional Compliance investigative staff, to block numbers (in real time) electronically and independently via designated System Administrative Workstations provided under this Scope of Work.
43. The MDCR Project Manager or designee may also notify the Contractor of the telephone number(s) the County wishes to be blocked. The Contractor shall block telephone number(s) when requested as soon as practical, but under no circumstances greater than eight (8) hours after the initial request.
44. The Contractor's automated operator shall employ appropriate security safeguards to detect, and block attempted three-way calls with a 99% reliability rate to include, pre- detection and warnings embedded in the call in English, Spanish, and Creole. Appropriate information regarding any detected possible three-way call attempts shall be recorded, archived, and the County Project Manager alerted for possible Detainee call monitoring, recording, or other corrective action. When applicable, the Contractor's automated operator shall be capable of System sensitivity modifications and shall be configurable to prevent attempts at three-way calls, Unauthorized Calls, while simultaneously preserving legitimate calls and avoiding erroneous disconnects. Failure to achieve a mutually agreed upon successful detection rate will result in the imposition of financial penalties.
45. The Contractor's automated operator shall detect, and block attempted Detainee calls to unauthorized telephone numbers. Unauthorized numbers shall include but are not limited to the following: Public officials; government agencies; businesses; news media; numbers blocked by family members; and any other numbers, or blocks of numbers, identified by the County or ordered by a court of law. A master listing of unauthorized numbers shall be available for query/review/modification by County at any time electronically on System Administrative Workstations provided under this Scope of Work.
46. The Contractor's automated operator shall detect, and block attempted Collect Calls to restricted numbers. A master listing of restricted numbers shall be available for query/review/modification by the County at any time electronically on System Administrative Workstations provided under this Scope of Work.
47. The Contractor's automated operator shall employ appropriate security safeguards to detect, and block attempted call forwarding of Detainee calls. Appropriate information regarding any detected Detainee call forwarding attempts shall be recorded, archived, and the concerned County Project Manager alerted for possible Detainee call monitoring, recording, or other corrective action.
48. At regular intervals, the Contractor shall keep the MDCR Project Manager or designee apprised of current sensitivity settings, any success, and/or perceived or actual negative affect on calls as a result of current settings. Prior to any System modifications in this area, which could affect the County, the Contractor shall apprise and receive written approval from the County Project Manager or designee.
49. Detainee telephone calls to a live operator are absolutely prohibited. The Contractor's Detainee telephone module shall be limited solely to the placing of automated operator assisted Collect Calls and Pre-Paid calls.
50. The Contractor's automated operator shall detect and block all other types of Detainee calls including but not limited to local operator calls (0), Information (411), Emergency Services (911), time (555-1212), businesses or special service numbers (such as 1-700, 1-800, 1-887, 1- 888, 1-900 and 1-976 numbers). No numeric sequences associated with other call carriers for operator services (such as 1-950 numbers, or as otherwise specified in this document) are allowed.

## SCOPE OF WORK

51. The Contractor's automated operator shall detect and block Detainee long distance telephone call attempts to by-pass the County's Detainee telephone services, utilizing numeric access codes to alternative calling plans provided by other long distance service vendors.
52. The Contractor's automated operator shall detect and block Detainee telephone calls to 1-0- XXX, 1-0-1-0-XXX, or any other similar numeric sequences intended to reach another long-distance carrier. The Contractor's automated operator shall detect and block commercially available debit calling cards.
53. The Contractor's automated operator shall detect, and block Detainee telephone calls intended to cause a public nuisance. The candidate list of telephone numbers likely to be targets of public nuisance calls will be provided by the MDCR Project Manager or designee as needed.
54. The complete list of unauthorized telephone numbers to be blocked will be developed jointly by County and Contractor's staff and updated as needed. The Contractor shall prepare and maintain the list of blocked telephone numbers and submit the list to the MDCR Project Director or designee for review and written approval. This listing shall be available for query/review/modification by County at any time electronically on specified System Administrative Workstations provided under this Scope of Work.
55. Appropriate information regarding any detected Detainee call attempts to unauthorized telephone numbers shall be recorded, archived, and the MDCR Project Manager or designee alerted for possible Detainee call monitoring, recording, or other corrective action.
56. Contractor's automated operator shall provide capability to monitor Detainee telephone calls at MDCR Custody and Detention Facilities.
57. Contractor's automated operator shall provide the capability to monitor any Detainee Telephone Instrument and any Detainee telephone call, via laptops utilizing Web access, or via System Administrative Workstations.
58. The Contractor shall provide remote access via Virtual Private Network (VPN) for laptop access, to all program features to monitor calls, for MDCR personnel explicitly authorized by the MDCR Project Manager or designee.
59. Administrative Workstation for MDCR staff, as specified by the MDCR Project Manager for the purpose of monitoring and recording Detainee phone calls. The requirements for the System Administrative Workstation are described further in this document.
60. The Contractor shall supply a means to identify call recipient information associated with the dialed telephone numbers (e.g., Haines reverse directory). When the call recipient information is confidential as determined by the Contractor, the Contractor shall have no obligation to reveal the information without a court order.
61. Contractor's automated operator shall provide capability to record Detainee telephone calls at MDCR Custodial and Detention Facilities. The Telephone Module must be capable of recording one hundred percent (100%) of all Detainee telephone calls. Calls must be recorded in their entirety, up to the thirty (30) minutes time limit for Detainee calls. Recordings must be selectable by Telephone Instrument, group of Telephone Instruments, facility or called number.
62. The Telephone Module shall capture unauthorized activities. System Administrative Workstations provided under this Scope of Work shall be capable of reporting unauthorized Detainee calls.
63. The Contractor's automated operator shall provide capability to archive and immediately retrieve via VPN access or from System Administrative Workstation all recorded Detainee telephone calls. Once recorded, the content of the call must be stored by the Contractor and be available for immediate retrieval via method determined by the MDCR Project Manager or designee for a period of up to three (3) years and at the discretion of the MDCR Project Manager or designee. The Telephone Module must have the capability to transfer the recorded calls to an off-line media for archiving, or review. (NOTE: The Telephone Module must be capable of preventing recording of calls in certain sections of the facilities as it pertains to Pro-Se Detainee, as the calls of Pro-Se Detainee are not recorded.)
64. All recorded telephone calls (files) shall be accompanied by the following data:
  - Salutory call branding information.
  - Date and time the telephone call was placed.
  - Location from which the telephone call was placed.
  - Telephone number that was dialed.
  - Duration of the telephone call.

## SCOPE OF WORK

- Time that the telephone call was terminated.
  - PIN, if applicable.
65. The Contractor shall copy, save, and store off-line data for archived Detainee calls in the agreed upon media format and retrieval rate.
  66. The Telephone Module must continue to record calls, without interruption, while copying and saving previously recorded calls. The recorded call file format shall be compatible with Microsoft Windows 10 based personal computer, or another format to be determined by the County.
  67. The Telephone Module shall provide the capability of naming each file, or automatically generating a file name. Each recorded telephone call or any copies shall be security encoded, in order to detect any attempted alterations to the recorded telephone call.
  68. The Detainee Telephone Module provides a secure logon procedure, which guards against fraudulent use. The Telephone Module possesses a feature in which established passwords auto-expire at a period determined by the County. Levels of permissions exist which allow the County Project Managers or designees the ability to create, edit, or view user accounts and assign permissions. The Telephone Module provides detailed explanation as to System Administrator, user, or other definable levels of access.
  69. The Telephone Module provides a feature, which allows users to attach "notes" which provide additional documentation to Call Records. Notes are logged by the username, and date and time of entry. Notes are capable of being printed or updated.
  70. The Telephone Module is capable of displaying historical user data including, but not limited to, a list of users who opened the same call recording, when users were granted access to the System and by whom.
  71. The Telephone Module is capable of displaying data on copied files containing each user's information including, but not limited to, username, date and time of each copy.
  72. The Telephone Module allows users to print, e-mail, or export the current page of a report and to export in various file formats (i.e., PDF, Excel, RTF, TXT, or TIFF).
  73. The Telephone Module is capable of displaying attempted and successful user logon transactions for each logon username and includes, but is not limited to, date and time of attempt of logon and activity.
  74. The Telephone Module allows users to view the call activities of each Detainee telephone located within a particular facility and listen to calls in real time.
  75. The Telephone Module allows users to lock recordings. Locked recordings are not deleted or unlocked without the approval of the appropriate authorized user. Users may only lock files if there is a recording associated with that call detail record.
  76. The Telephone Module allows users to monitor calls through workstation computer speakers or by sending calls to a designated telephone number (e.g., cell phone, home phone, or office phone without an extension).
  77. The Telephone Module allows authorized users to disconnect any Detainee call as it is being monitored, immediately and without warning to parties participating in the conversation. The System allows the County Project Managers, or designees, the capacity to turn off (and on) individual, specified group, or all Detainee telephones from any authorized workstation.
  78. The Telephone Module provides a means by which authorized users can add numbers to a destination number list. Numbers may be added to this list for various reasons including, but not limited to blocking the number, adding privileged numbers, creating a calling schedule, selecting a number for no recording or creating an alert. Once a phone number is blocked, no Detainee telephone calls to that destination number will be allowed from any Detainee telephone.
  79. The Telephone Module provides a thorough complement of search and sort features both investigative and administrative which includes, but is not limited to, played calls, recorded calls, completed calls, incomplete calls, copied or downloaded calls, calls with notes, note content, locked calls, call duration, manner in which call was initiated, manner in which call was terminated, type of call, three-way calls, and rate type.
  80. The Telephone Module provides a report which tracks the total number of calls by both origination number (Detainee telephone) and call destination number (number dialed by the Detainee). Information in this report includes, but is not limited to, the origination number, location of the Detainee telephone within the facility, number of calls attempts from the Detainee telephone, number of accepts (calls accepted by the called party from this

## SCOPE OF WORK

- Detainee telephone), destination number (number dialed by the Detainee), the number of attempts to the destination number, and the number of accepted calls at the destination number.
81. The Telephone Module provides a report indicating activities associated with destination numbers placed on an alert list provided by the County. Calls to specified destination numbers are monitored each time they are dialed by a Detainee. This report contains call detail information including, but not be limited to, if call was recorded, if call had notes attached, if call was locked, facility, destination, date/time of alert, call length, cost of call and manner in which the call started and ended.
  82. The Telephone Module provides a means which allows investigators to utilize “bookmarks” or “timeline markers” to tag a particular location, in time, within a recording for future reference and enter comments or notes within the bookmark. Bookmarks are not retained unless a voice-recording file is downloaded or saved.
  83. The Telephone Module provides a security method for verifying authenticity of recordings. Completed Detainee calls stored for retrieval are protected from fraud and tampering throughout the storage term.
  84. The Telephone Module provides a means of immediately alerting a collection of user-defined phone numbers attached to an individual or group with monitoring rights. Each time a Detainee places a call to a designated destination number, the Telephone Module begins dialing the specified contact phone numbers immediately, one by one, in the succession specified. If contact cannot be established (i.e., busy or unanswered) at a called number, the Telephone Module moves on to the next number, respectively, until contact is made with a member of the group, at which time the dialing may cease. If no contact is made after exhausting the list, the System repeats the list, in succession, until contact is made.
  85. The Telephone Module provides a means for compressing "dead space" in recorded Detainee phone calls where no voice is detected, to be eliminated, leaving only the actual voice recordings in a compressed/abbreviated form. Such feature does not alter the Telephone Module capacity to retain the original file with security envelope.
  86. Under no circumstance are privileged communications/phone calls be recorded. Contractor will conduct quarterly self-audits to ensure that no privilege communication is recorded and provide MDCR reports accordingly.

### 17.0 Content Packages

Contractor shall provide Content packages to meet the various needs of MDCR including a Standard Package at no charge and a Premium Package a per-minute (use) basis.

#### 17.1 Standard Package

Contractor shall provide a wide variety of standard content to keep Detainees occupied in meaningful and self-improving activities to help Detainees satisfy social and emotional needs. At a minimum, Contractor shall provide the following content and services to all Detainees at no charge to either the Detainee or the County.

##### A. Communication

- Ninety (90) minutes of phone calls per day
- Two (2) hours of video visitation per week
- Five (5) electronic messages per week
- Unlimited receipt of digitized personal mail
- Unlimited receipt of digitized privileged mail

##### B. Detainee Resources

- Unlimited access to religious content (recorded services and religious texts)
- Access to County funded Legal Research Associates through interface
- Unlimited access to various request systems
- Expansive collection of E-books and magazines
- Educational Content

## SCOPE OF WORK

- Job and Life skills content
- Newsfeeds
- Contractor must supply all Detainees with One (1) pair of wired ear buds. Additional headphones may be purchased through commissary.
- One (1) free movie per month
- Two (2) free games, at a minimum, updated quarterly (i.e., chess, Sudoku, solitaire)

### 17.2 Premium Package

Applications available above the standard items may be purchased on a per minute/each basis.

- Telephone usage above Ninety (90) minutes per day
- Video visitation above Two (2) hours per week
- Electronic messages above Five (5) per week
- Movies
- Music
- E-Books/Magazines (newly released content)
- Games
- Any other services that Contractor wishes to offer as long as they are approved by MDCR

### 18.0 System Updates to Services

The County reserves the right to request from the Contractor updates to services, technology, and hardware. Without limiting Contractor's obligation to provide system updates, Contractor and County acknowledge the probability that the technology of the Detainee Kiosk, or any of its components provided under the Agreement will change and improve during the Term. Contractor shall provide the flexibility to incorporate into the Detainee Kiosk any new technologies, as they may become available in new releases or the marketplace. Contractor shall report to MDCR, new trends and technological enhancements at least twice per year.

### 19.0 Solution Interface Requirements

The Solution should provide one-way and bi-directional interfaces to various third party and internal County systems, current and future through open Application Programming Interface (API). All data derived from the Solution shall be made available via the API. Contractor should conduct a thorough review / assessment of all interfaces to be provided. Noted below are the principal recognized application interfaces required for the Solution.

The column heading "Req'd for Go-Live" indicates the need for the specific interface to be operational with the initial deployment of the Solution.

The column heading "Frequency of Data Flow" describes the anticipated occurrence or regularity of the interface's data transfer.

- Real time: Indicates an interface that must operate dynamically, on demand between systems.
- Batch: Indicates a grouped, multiple record/transaction based interface between systems. Typically file based in nature, and often on a predetermined interval (e.g. hourly, daily, weekly, monthly, etc.)

The column heading "Mode" describes the direction of the interface between the Solution and the County systems.

- Data Exchange: Signifies a bidirectional functional interface between the application and the Solution where data is exchanged.
- One-way / Solution: Signifies a unidirectional interface in which data is pushed from the County to the Solution.
- One-way / County: Signifies a unidirectional interface in which data is pushed from the Solution to the County.

**SCOPE OF WORK**

The Solution must interface with all current and future MDCR systems to include but not limited to the systems as identified below:

Interface	Req'd for Go-Live	Description	Frequency of Data Flow	Mode
<p><b>Interface:</b> Bookings/Releases/Transfers <b>Vendor:</b> ITD <b>Application:</b> CJS (Criminal Justice System) <b>Platform:</b> CA-IDMS mainframe-based DBMS running under MVS. IDMS Release 18.0. <b>Development Tool:</b> ADSO, IDD, IDMS COBOL <b>Keys:</b> Jail Number, CIN Number, Case Number, Name, IDS Number</p>	<p><b>Yes</b></p>	<p>CJIS posts any Bookings, Releases, and Transfers to a web service. The Vendor's application should look to the web service to pull the Detainee records waiting to be retrieved</p> <p>Data Exchange Values: Type (Booking, Release, or Transfer) Book Date/Time Release Date/Time Booking Number Permanent Number (CIN) Name fields Housing Locations SSN Race Gender DOB Address</p>	<p><b>Every Minute</b></p>	<p><b>Auto</b></p>

**SCOPE OF WORK**

Interface	Req'd for Go-Live	Description	Frequency of Data Flow	Mode
<p><b>Interface:</b> CJIS Permanent Number (CIN) Lookup <b>Vendor:</b> ITD <b>Application:</b> CJS (Criminal Justice System) <b>Platform:</b> CA-IDMS mainframe-based DBMS running under MVS. IDMS Release 18.0. <b>Development Tool:</b> ADSO, IDD, IDMS COBOL <b>Keys:</b> Jail Number, CIN Number, Case Number, Name, IDS Number</p>	<p><b>Yes</b></p>	<p>The interface is used to look for Detainees that are not assigned a CIN at time of booking. The interface checks the CJIS web service for any Detainee in the Vendor system without a CIN. If the CIN has been updated/assigned, the Vendor updates the system with the proper CIN.</p> <p>Data Exchange Values: Data element passed to CJIS for Detainee lookup: Booking Number</p> <p>Data elements received from CJIS: Book Date/Time Release Date/Time Booking Number Permanent Number (CIN) Name fields Housing Locations SSN Race Gender DOB Address</p>	<p><b>Real Time</b></p>	<p><b>Auto</b></p>
<p><b>Interface:</b> CJIS JMS Active Roster <b>Vendor:</b> ITD <b>Application:</b> CJS (Criminal Justice System) <b>Platform:</b> CA-IDMS mainframe-based DBMS running under MVS. IDMS Release 18.0. <b>Development Tool:</b> ADSO, IDD, IDMS COBOL <b>Keys:</b> Jail Number, CIN Number, Case Number, Name, IDS Number</p>	<p><b>Yes</b></p>	<p>CJIS creates and updates in a SFTP site an ascii text file of all active Detainees to be retrieved by the Vendor's application. This information is used to capture any Detainees that may have been missed in the Web Service Interface (possible network outage or CJIS maintenance). This also is used to update Detainee housing locations.</p> <p>Data Exchange Values: Booking Number Permanent Number (CIN) Name fields Housing Locations SSN Race Gender</p>	<p><b>Real Time</b></p>	<p><b>Auto</b></p>

## SCOPE OF WORK

Interface	Req'd for Go-Live	Description	Frequency of Data Flow	Mode
		DOB Address		
<b>Interface:</b> Mugshot Interface <b>Vendor:</b> DataWorks <b>Application:</b> Mugshot <b>Platform:</b> Microsoft SQL Server 2014 - 12.0.2000.8 (X64) <b>Development Tool:</b> Microsoft .Net Development platform <b>Keys:</b> Jail Number, Mugshot ID, CIN, SID, FBI #, OBTS, SSN	Yes	The Vendor's application retrieves Mugshot and Property Images from Mugshot system to display Detainee mugshots and for property verification upon release Data Exchange Values: Booking number Mugshot Image Property image	Real Time	Auto
<b>Interface:</b> Detainee Commissary and Banking Services <b>Vendor:</b> ARAMARK <b>Application:</b> Commissary, Personal Property, Detainee Banking and Visitation <b>Platform:</b> SQL Server 2016 <b>Development Tool:</b> Microsoft Visual Studio with .NET Framework, with custom components/controls (i.e. signature pad, grids, etc.) <b>Keys:</b> Jail Number, CIN (Permanent number), First Name, Middle Name, Last Name, DOB, Gender, Race, Address, Book Stamp, Release Stamp, Building, POD, Cell Number	Yes	The Vendor's application retrieves and send back Detainee Commissary and Banking Services information from this interface. Data Exchange Values: Jail Number CIN (Permanent number) First Name Middle Name Book Stamp Release Stamp Facility Cell Number Detainees' commissary information Detainees' Banking and Financial information	Real Time	Auto
<b>Interface:</b> IPS Visitor Interface <b>Vendor:</b> ITD <b>Application:</b> IPS (Detainee Profile System) <b>Platform:</b> CA-IDMS mainframe-based DBMS running under MVS. IDMS Release 18.0. <b>Development Tool:</b> ADSO, IDD, IDMS COBOL <b>Keys:</b> Jail Number, CIN Number, Name, Incident	Yes	The list of visitors allowed to each Detainee is provided by a web service. The Vendor's application takes the information from the IPS web service to retrieve a read-only view of the list of Visitors. This information is displayed on the Innate Kiosk.  The Detainee can then make changes to the visitor list from the kiosk and the changes are put on an SFTP site to be retrieved by IPS.	12 Hours	Auto

**SCOPE OF WORK**

Interface	Req'd for Go-Live	Description	Frequency of Data Flow	Mode
<b>Interface:</b> Legal Research Associates <b>Vendor:</b> Legal research Associates <b>Application</b> Legal Research Associates <b>Platform:</b> TBD <b>Development Tool:</b> TBD <b>Keys:</b> TBD	<b>Yes</b>	This is MDCR's current Law library/Legal Research vendor.	<b>Real Time</b>	<b>Auto</b>
<b>Interface:</b> Detainee Request and Grievances <b>Vendor:</b> ITD <b>Application:</b> Detainee Grievance System <b>Platform:</b> SQL Server 2016 <b>Development Tool:</b> Microsoft Visual Studio with .NET Framework, <b>Keys:</b> Jail Number, CIN (Permanent number), First Name, Middle Name	<b>Yes</b>	A web service is provided that will allow the vendor to interface with the Detainee Grievance System. Using this interface, the Vendor will allow the Detainees to generate Grievances and Detainee Request from the Detainee Kiosk  Data Exchange Values: Jail Number CIN (Permanent number) First Name Middle Name Facility Cell Number Grievance number Grievance content Request number Request content	<b>Real Time</b>	<b>Auto</b>

**20.0 Data Backup/Storage**

- A. Contractor shall perform all database backups used by the system, archiving data from phone calls, audio and video recordings, text messages, emails, and usage data. All hardware used for database backup, archiving, network, and recovery procedures, which ensure that no data is lost, will be provided by the Contractor at no cost to the MDCR. The Contractor shall keep all such information stored for the length of the contract, in accordance with durations set forth by Article 36, *Grant of License*, of the Agreement.
- B. All data will remain the property of the MDCR, and the Contractor shall not use the data for any purpose other than as required in the Contract. Contractor is strictly prohibited from sharing/selling any data with any third party to include any biometric identifiers.
- C. Contractor shall have a written Disaster Recovery Plan and Continuity of Operations Plan, as well as the necessary equipment to provide support in the event of a disaster situation, natural or man-made.

## SCOPE OF WORK

### 21.0 System/Data Breach

#### A. System Breach

The Contractor shall report, in writing immediately upon their determination, to the County Project Manager any County system breach by an unauthorized individual. The Contractor shall be liable for all damages, fines and corrective action arising from any County system breach on a contractor provided system. The penalty fine amount for such breach is set at one (1) Million dollars in the form of a check and shall be issued to the MDCR.

#### B. Data Breach

The Contractor shall report, in writing, to the County Project Manager any use or disclosure of County data, usage data, or content not authorized by this Contract or in writing by the County, including any reasonable belief that an unauthorized individual has accessed County data, usage data or content. The Contractor shall make the report to the County immediately upon discovery of any unauthorized disclosure, but in no event more than two (2) business days after Contractor reasonably believes there has been such unauthorized use or disclosure. The Contractor's report shall identify (i) the nature of the unauthorized use or disclosure, (ii) the County covered data or content, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what the Contractor has done or shall do to mitigate and deleterious effect of the unauthorized use or disclosure, and (v) what corrective action the Contractor has taken or shall take to prevent future similar unauthorized use or disclosure. The Contractor shall provide such other information, including a written report, as reasonably requested by the County. Notwithstanding any other provisions in this Contract, the Contractor shall be liable for all damages, fines and corrective action arising from disclosure of such information caused by the Contractor's breach of its data security or confidentiality provisions.

### 22.0 Maintenance and Support Commitment

The Contractor shall provide 24/7 technical support and maintain sole and absolute responsibility for the maintenance and service of the Contractor's systems at no cost to MDCR. The Contractor shall coordinate planned system maintenance with MDCR Project Manager or designee not less than forty-eight (48) hours in advance. System maintenance shall be scheduled, whenever possible, to minimize potential impact to prime Detainee calling periods. Any deviations will require the County Project Managers' written approval.

#### 22.1 Solution Maintenance and Support Plan

Contractor shall describe in detail how the systems are maintained and supported to ensure, for the duration of the contract term, reliable service for detainees and consistent access to system controls and reporting capabilities by MDCR.

The Contractor's service and support plan must address at a minimum the following topics:

#### A. Local Maintenance and Repair Service

The Contractor shall provide local service personnel to maintain and/or replace broken or malfunctioning kiosks or system equipment as needed. Contractor must provide 24/7/365 technical support and a secure depot to store an inventory of replacement tablets and mobile kiosks (10% of total tablets and mobile kiosks in circulation) to replace damaged or malfunctioning tablets or kiosks at no cost to MDCR.

Remote Access for System Monitoring and Software Maintenance: The Contractor's technical experts must be able to remotely monitor system performance and, if necessary, remotely reconfigure or repair the system's software control program. Include the company's policy for updating the user interface software as new versions are released.

## SCOPE OF WORK

### B. Help Desk

Contractor shall provide facility staff a toll-free Help Desk number that can be reached 24 hours a day, 365 days a year to report system problems, ask for help with system functionality or submit requests for additional equipment or services. The Help Desk should be Contractor-run and staffed with the Contractor's trained personnel. Help Desk support shall be decentralized to ensure support availability during regionalized natural disasters.

### C. Trouble Ticket Tracking and Escalation

Upon the request of the County, the Contractor shall provide documents that verify its compliance with the requirements stated in this section. Contractor must have a well-defined process for logging, tracking, and resolving issues related to the Contractor's systems and services. The Contractor shall have defined emergency-priority levels, responses, and resolution times for each level. The Contractor shall have an escalation plan for dealing with issues that are not resolved within the agreed upon time frame. Upon contract award, the Contractor shall provide MDCR with specific names, titles, and personal-contact information for all individuals involved in ticket escalation.

The County reserves the right to request from the Contractor, enhancements, or modifications to the Solution's Software. No enhancements or modifications should be performed by the Contractor unless preapproved and scheduled by MDCR. Contractor shall provide a test system capable of validating enhancements or modifications prior to deployment on the production system. County shall not be responsible for any costs thereof, even if the County requests such enhancements or modifications.

## 22.2 Customer Support Plan

Contractor shall provide a contractor-run and staffed billing customer support help desk for public users of the Contractor's systems. Describe in detail the availability of the help desk as well as the services provided to the public by this support group. Contractor must address at a minimum the following requirements:

Contractor shall provide one (1) on-site technician with extensive knowledge of the hardware and software to service the County and be on call to support the operation twenty-four (24) hours a day, seven (7) days a week and three hundred sixty-five (365) days per year. Technicians shall respond within Two (2) hours and resolve the problem within Four (4) hours. If the problem is not resolvable within Four (4) hours, the technicians shall provide a work plan and schedule acceptable to MDCR for resolving any outstanding issues. Technicians must be familiar with all aspects of the operating system. Technicians shall be certified as an A+, Security+, Network+ or current level of Microsoft Certified Professional Systems Engineer (MCSE) or Microsoft Certified Solutions Associate (MCSA).

Primary problem reporting will be made through the Contractor's onsite technical support staff. In the event that the onsite technical support staff is unavailable, MDCR will contact the Contractor at the pre-agreed help desk number to open a ticket for resolution of problem(s). Contractor shall provide an alternate telephone number in the event that MDCR needs to escalate any outstanding technical issues.

Contractor shall handle all Detainee Complaints/Grievances concerning tablets and stationary/mobile kiosks services in a cost effective and expeditious manner. Contractor shall provide weekly reports electronically to MDCR of all Complaints/Grievances and resolutions.

### A. Online Messaging service

Detainee must be able to contact the Contractor's online messaging service for assistance with any issues including but not limited to billing disputes, blocked calls from Detainee, dropped calls or video sessions. Contractor shall respond to Detainee inquiries within five (5) business days. At no time shall any Detainees have access to a live operator.

## SCOPE OF WORK

### B. Live Service via Toll Free Number

Non-Detainees must be able to contact the Contractor's live customer service representatives seven (7) days a week via a toll-free number for assistance with any issues, including but not limited to: billing disputes, blocked calls from Detainees, dropped calls or video sessions, and setting up or replenishing prepaid accounts.

### C. Service via Phone Interactive Voice Response (IVR) and Website

The Contractor shall include self-help options via an automated telephone IVR system and a user-friendly navigation tool for the Website.

## 23.0 Installation Plan

The Contractor shall provide and be responsible for the installation of all equipment and any necessary cabling related to the required services at no cost to MDCR. Installation of the system shall be at the Contractor's expense, as will removal if required by MDCR of same upon cancellation or completion of the contract. The Contractor shall be totally responsible for all equipment and services.

### A. Installation Plan

Contractors must submit an Installation Plan in accordance with Section 8, *Project Schedule*, which identifies the time and activities required for installation, utility coordination, training, cut over and testing. The system must be installed in a manner and under a timeframe designed to minimize disruption of the normal functioning of MDCR and security concerns. Any delay in contractor's implementation schedule that is caused by MDCR personnel will increase the contractor's time allowed to cut-over by the length of such delay. The County desires a fully implemented and installed Solution within one hundred twenty (120) days from the Award Date.

### B. Risk of Loss

The risk of loss and/or damage to Contractor's equipment will be fully assumed by the Contractor during shipment, unloading, installation, and for the entire lifecycle of the contract.

### C. Delivery and Unloading

The Contractor must provide transportation to and unloading of equipment at MDCR's designated locations. MDCR will not be liable for any charges related to packaging, delivery, or storage of equipment or materials required for proper implementation of the required services. All packing crates, boxes, paper, packing materials, and all other such extraneous material shall be removed from the premises by the Contractor at the Contractor's expense after installation.

## 24.0 Training

### A. MDCR Personnel

The Contractor must provide hands-on training on-site for fifty (50) MDCR personnel identified as super users of the Solution at a mutually agreed upon schedule. The Contractor must provide hands-on training to line staff during implementation as well as training tutorials and videos to educate all MDCR personnel. At no charge, the Contractor must provide one (1) set of appropriate documentation, Video, and Manuals per installed facility upon completion of training.

## SCOPE OF WORK

### B. Detainee Training

The Contractor must provide hands-on training, and written instructions in English, Spanish and Creole to the entire current Detainee population. The Contractor must provide training tutorials and/or videos to educate future Detainee population on how to use the solution.

### C. Additional Training as Needed

In addition to initial training required at the time of system installation, the Contractor must offer and provide additional training to existing or new MDCR employees, at a mutually agreed upon schedule.

## 25.0 Solution Acceptance

Contractor must demonstrate all system modules, functionalities and applications are operational as described in this document prior to MDCR finally accepting the Solution. Contractor agrees as part of the implementation to perform all required services to successfully achieve all objectives herein set forth in all MDCR facilities, including, but not limited to, (a) system configuration; (b) interface development. (c) software testing; (d) acceptance and user acceptance testing; (e) training; (f) cooperating with all other vendors supplying peripheral or ancillary equipment that will interface with the Solution.

Solution acceptance shall be determined by a consecutive thirty (30) day period during which the Solution must function ninety-nine percent (99%) of the time. The Contractor must work with MDCR to determine the actual uptime and downtime operation of the Solution. No Deficiency shall be deemed remedied until all necessary remedial action has been completed and approved in writing by the concerned County Project Manager in accordance with the procedures set forth in the agreement.

## 26.0 Solution Uptime and Downtime

The County has established target levels of the Solution availability to require no system outages longer than four (4) consecutive hours. If the Solution offering fails to be available for longer than four (4) hours at any given time, a fee shall be charged to the Contractor payable to MDCR in accordance with the schedule below:

<b>Occurrence</b>	<b>Fee Amount</b>
1 <sup>st</sup> occurrence	\$5,000 as a fixed fee
2 <sup>nd</sup> occurrence	\$10,000 as a fixed fee
3 <sup>rd</sup> occurrence or more	\$15,000 as a fixed fee

Downtime means that the Solution, any individual feature or function or any combination thereof, is not accessible to the County or its customers and shall not include periods of routine maintenance or administrative procedures that are scheduled during non-operating hours with the prior approval of the County. For clarity, should the Solution be not accessible by the County or its customers at any individual facility covered under this Agreement shall be considered Downtime.

The concerned County Project Manager shall notify Contractor's Project Manager in writing, or orally to either Contractor Project Director or Contractor Project Manager, of any Deficiency. Upon the notice (orally or in writing) from County, or the Contractors discovery of such Deficiency, Contractor shall promptly commence corrective measures to remedy any Deficiency, and shall remedy such Deficiency, in accordance with the timeline set forth and agreed upon by both parties. Contractor acknowledges that, as part of Maintenance and Technical Support Services provided to County, Contractor may be required to repair, replace, or reinstall all or any part of the Detainee Kiosk, or other material, or create an Update, in order to remedy a Deficiency.

## SCOPE OF WORK

Contractor shall provide MDCR a report monthly with the solution uptime and downtime by the 7<sup>th</sup> of each month. MDCR has 60 days from the receipt of the uptime and downtime report to dispute the calculations. After the dispute is filed, both parties will attempt to reach an agreement to resolve the dispute. If no resolution is able to be reached, the County will refer the matter to the County Attorney's Office.

In the event media paid by the Detainee is interrupted due to a system outage, after the restoration of the system, the Detainee shall have restored, access to the paid media for the full period of time allotted for the media.

### **27.0 Prepaid Accounts**

The Contractor shall have the ability to provide prepaid account funding for services provided via the Detainee Kiosk system. Contractor shall provide a system for automated payment and deposit options which shall be available online and to visitors at any of the facilities. The payment and deposit options shall be fully integrated with the Contractor's banking (accounting) software. Funds deposited during the day from all sources shall be electronically transferred nightly to Detainee Trust Fund Account and deposited directly to individual detainee accounts. Deposits shall be added to General Ledger and Bank Reconciliation file.

### **28.0 Payment Card Industry Compliance**

The Solution must fully comply with Payment Card Industry ("PCI") Security Standards. The County's current process for establishing and maintaining such compliance is outlined in Attachment E. The Contractor shall provide turnkey encryption services for all payment options within the Solution. These services, including any third-party agreements required to be executed by the County, and costs shall be disclosed in any Proposal. Contractor shall submit its PCI DSS Attestation of Compliance (AOC) to MDCR annually. The Contractor is responsible for any costs associated with conducting PCI audits and all cost of resolving any PCI audit findings (or penalties).



FORM 2 - PRICE PROPOSAL SCHEDULE

Educational Content	Contractor will provide no cost access to educational program for all Delawareans including GED preparatory content access to online college classes and self improvement courses and videos. Contractor will partner with local universities to deliver on-line access to education to support continuing education upon release.	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	
Equipment collection of e-books and magazines (minimum \$100)	Contractor will provide no cost access to all databases for the Galenborg Library containing over 51,000 books.	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	
Additional skills content	Contractor will provide all databases no cost access to job and life skills content including TVSO, JobView, Evidence to Contract and additional videos and content to support improvement in the pursuit of employment and improvement of general life skills.	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	
Newspaper	Access to news covering multiple areas of interest.	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	
One (1) pair of headphones	Contractor will provide each Delawarean with one (1) pair of headphones. Additional headphones can be purchased through commissary if the provided pair is destroyed or lost.	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	
One (1) free movie per month	Contractor will provide each Delawarean with one (1) free movie per month.	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	
Two (2) free games, at a minimum, updated quarterly (i.e., chess, solitaire, sudoku)	Contractor will provide each Delawarean with Two (2) free games to be updated quarterly. Games will be cycled to keep the Delawareans interested.	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	
Table A-4 - Additional Free Resource Applications may be added below (To Deleted):													
Document Acceptance	Ability for MDCR to perform document reviews, initial signatures to the states and videos for review at any time. The nodes acts as acceptance of the provision by the contractor in relation to delivery of services as stated in the MDCR acquisition pricing code strategy.	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	
FV1 Application	The FV1 Application will allow MDCR to send notification to the entire MDCR network, a mandated study, study, or a specific Delawarean.	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	
PIN Booklet	Provides Delawareans with no cost access to PIN Modules for in pod TVs.	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	
Commissary Ordering	Provides Delawareans with commissary ordering access to eliminate paper forms.	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	
Contractor Outputs	Policies and Videos with recognized re-entry reports and former incarcerated individuals to help promote a successful re-entry effort.	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	NO CHANGE	

MDC073

Table B: The applications below shall represent additional services available through the Contractor, which may be provided to the Dealers and public at the stated fees on a per minute basis.

Table B-1: Additional Communication Applications (Per Minute)	Contractor Assumptions Contractor has stated below, in narrative form and in detail, ANY AND ALL applications available within the bundle at the stated fee, and ANY AND ALL assumptions, limitations, and explanations that the Contractor has made in providing the stated services.	INITIAL TERM					OPTION TO RENEW TERM					Total			
		Year 1	Year 2	Year 3	Year 4	Year 5	Year 1	Year 2	Year 3	Year 4	Year 5				
Per Minute, Response usage above thirty (30) minutes per day	Upon exceeding ninety (90) ten minutes daily, additional minutes will be charged, excluding calls to public defenders or other court appointed service numbers. Rate is \$0.0185 per minute.	\$0.02	\$0.02	\$0.02	\$0.02	\$0.02	\$0.02	\$0.02	\$0.02	\$0.02	\$0.02	\$0.02	\$0.02	\$0.19	
Per Minute, Video resolution above two (2) hours per week	Additional per minute rate for video resolution.	\$0.15	\$0.15	\$0.15	\$0.15	\$0.15	\$0.15	\$0.15	\$0.15	\$0.15	\$0.15	\$0.15	\$0.15	\$1.22	
Electronic messages sent above five (5) per week	Additional electronic messages sent over five (5) per week.	\$0.20	\$0.20	\$0.20	\$0.20	\$0.20	\$0.20	\$0.20	\$0.20	\$0.20	\$0.20	\$0.20	\$0.20	\$2.00	
<b>Table B-2: Resource Application (Each)</b>	<b>Contractor Assumptions</b> Contractor has stated below, in narrative form and in detail, ANY AND ALL applications available within the bundle at the stated fee, and ANY AND ALL assumptions, limitations, and explanations that the Contractor has made in providing the stated services.	<b>INITIAL TERM</b>											<b>Total Table B-1:</b>		
Music (Album)	Contractor provides content without a per minute fee, in a manner consistent with that used for non-licensed products. Music will be accessible at one flat rate for the duration of their person incarceration. Albums may be played as frequently as desired for this one flat rate. The rate shown is not per minute, it is per album.	\$119 - \$223	\$119 - \$223	\$119 - \$223	\$119 - \$223	\$119 - \$223	\$119 - \$223	\$119 - \$223	\$119 - \$223	\$119 - \$223	\$119 - \$223	\$119 - \$223	\$119 - \$223	\$119 - \$223	\$56.90
Movies (above one (1) per month)	Contractor will provide access to more current content to our model inmate than the process used for non-licensed products. Once a film or television show is ended, the Dealer will have 24 or 48 hours to view the film, once it has begun, and can watch the program as frequently as desired during that time period. The price shown is per movie, not per minute.	\$3.99 - \$9.99	\$3.99 - \$9.99	\$3.99 - \$9.99	\$3.99 - \$9.99	\$3.99 - \$9.99	\$3.99 - \$9.99	\$3.99 - \$9.99	\$3.99 - \$9.99	\$3.99 - \$9.99	\$3.99 - \$9.99	\$3.99 - \$9.99	\$3.99 - \$9.99	\$0.00	
Per minute Ebook/Articles	In addition to the 50,000 books included in our library, premium ebooks and articles, top magazines can also be purchased, and processed for a single cost, without a per minute fee. Prices will vary by book/magazine.	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$56.90	
Games above two (2) has offered	Contractor offers hundreds of game files, and will provide MDCR with the flexibility to add new games, to keep content fresh, and provide activities for the Dealers. The price shown is per game, not per minute.	\$0 - \$8.99	\$0 - \$8.99	\$0 - \$8.99	\$0 - \$8.99	\$0 - \$8.99	\$0 - \$8.99	\$0 - \$8.99	\$0 - \$8.99	\$0 - \$8.99	\$0 - \$8.99	\$0 - \$8.99	\$0 - \$8.99	\$0.00	
<b>Table B-3: Additional Communication Applications may be added below:</b>	<b>Contractor Assumptions</b> Contractor has stated below, in narrative form and in detail, ANY AND ALL applications available within the bundle at the stated fee, and ANY AND ALL assumptions, limitations, and explanations that the Contractor has made in providing the stated services.	<b>INITIAL TERM</b>											<b>Total Table B-2:</b>		
Transaction with Miami Data Public Library's digital content for Dealer's consumption which is not in contract provided by the Contractor	Contractor will provide access to the Miami Data Public Library's digital content for Dealers at no cost. Miami Data Public Library would be responsible.	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	
Contractor TextConnect Package	Text Connect 100 Text Message Bundle	\$9.99	\$9.99	\$9.99	\$9.99	\$9.99	\$9.99	\$9.99	\$9.99	\$9.99	\$9.99	\$9.99	\$9.99	\$89.91	
TextConnect Messages	Text Connect's SMS messages sent through Contractor's system. Text Connect messages contain fewer characters than messages. All messages can be reviewed and are stored for ongoing access if needed.	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$1.00	
Feeds	Electronic Message picture attachments. Pictures can be updated, and must be approved by MDCR prior to release to the Dealer.	\$0.25	\$0.25	\$0.25	\$0.25	\$0.25	\$0.25	\$0.25	\$0.25	\$0.25	\$0.25	\$0.25	\$0.25	\$2.50	

MDC074

FORM 2 - PRICE PROPOSAL SCHEDULE

Table B-4: Additional Resource Applications may be added below:	Contractor Assumptions Contractor has stated below, in narrative form and in detail, ANY AND ALL applications available within the bundle at the stated fee, and ANY AND ALL assumptions, limitations, and explanations that the Contractor has made in providing the stated services.	INITIAL TERM					OPTION TO RENEW TERM					Total Table B-3 Per Unit Year 5	Total INITIAL TERM AND OPTION TO RENEW		
		Per Unit Year 1	Per Unit Year 2	Per Unit Year 3	Per Unit Year 4	Per Unit Year 5	Per Unit Year 1	Per Unit Year 2	Per Unit Year 3	Per Unit Year 4	Per Unit Year 5				
VideoGems	VideoGems allow fee updating for thirty (30) second videos, which may be rewatched at no additional cost. MDCR will have the ability to provide all VideoGems prior to release to the Detainee.	\$0.50	\$0.50	\$0.50	\$0.50	\$0.50	\$0.50	\$0.50	\$0.50	\$0.50	\$0.50	\$0.50	\$0.50	\$0.50	\$500
Table B-4: Additional Resource Applications may be added below:	Contractor Assumptions Contractor has stated below, in narrative form and in detail, ANY AND ALL applications available within the bundle at the stated fee, and ANY AND ALL assumptions, limitations, and explanations that the Contractor has made in providing the stated services.	Per Unit Year 1	Per Unit Year 2	Per Unit Year 3	Per Unit Year 4	Per Unit Year 5	Per Unit Year 1	Per Unit Year 2	Per Unit Year 3	Per Unit Year 4	Per Unit Year 5	Per Unit Year 5	Total INITIAL TERM AND OPTION TO RENEW	\$38,411	
Contractor SMS Based Recovery Tool	Contractor SMS Based Recovery Tool is available for an agency to take advantage of and make available for any released individual and unit of (3) additional inmate members. The cost to the agency per serviced inmate, would be \$5 per month. The Recovery Tool provides access to additional recovery support, newsletters and mental health support and additional services covering access to de-stigmatization, food benefit programs, and educational and financial assistance.	\$6.00 per user per month	\$6.00 per user per month	\$6.00 per user per month	\$6.00 per user per month	\$6.00 per user per month	\$6.00 per user per month	\$6.00 per user per month	\$6.00 per user per month	\$6.00 per user per month	\$6.00 per user per month	\$6.00 per user per month	\$6.00 per user per month	\$0.00	
Contractor Label Personalization	The "Make Me" fee allows the personalization of a label for a monthly period and gives immediate access to all content without an ongoing cost. As an example, once a Detainee has personalized a label, any songs or games listed will be available throughout the duration of the label personalization. Should a Detainee depart, and then return, all previously leased songs and games would again be available.	\$5.00	\$5.00	\$5.00	\$5.00	\$5.00	\$5.00	\$5.00	\$5.00	\$5.00	\$5.00	\$5.00	\$5.00	\$90.00	
Television Programs	Contractor will provide access to a number of content television show files. Benefits will be provided for periods of 12/1 or 48 hours, with the retail period beginning once the content has been accessed. Prices shown are per program, not per minute.	\$17.74 - \$2.49	\$17.74 - \$2.49	\$17.74 - \$2.49	\$17.74 - \$2.49	\$17.74 - \$2.49	\$17.74 - \$2.49	\$17.74 - \$2.49	\$17.74 - \$2.49	\$17.74 - \$2.49	\$17.74 - \$2.49	\$17.74 - \$2.49	\$17.74 - \$2.49	\$0.00	
Monthly News Feed	Premium News Feed incorporating national outlets that are refreshed and updated every 15 minutes.	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$59.90	
Guarded Exchange Monitoring Services (Telephone) (Contract Option)	Telephone Monitoring and Reporting - \$7/Telephone Monitoring and Reporting - \$12 per minute for monitoring of Five (5%) Percent of the total call volume.	\$0.02/minute	\$0.02/minute	\$0.02/minute	\$0.02/minute	\$0.02/minute	\$0.02/minute	\$0.02/minute	\$0.02/minute	\$0.02/minute	\$0.02/minute	\$0.02/minute	\$0.02/minute	\$0.00	
Guarded Exchange Monitoring Services (Video Visitation) (Contract Option)	Remote Video Visitation Monitoring and Reporting - Daily monitoring of Remote with daily reporting to Authorized MDCR staff (example below) - \$.05 per minute	\$0.05/minute	\$0.05/minute	\$0.05/minute	\$0.05/minute	\$0.05/minute	\$0.05/minute	\$0.05/minute	\$0.05/minute	\$0.05/minute	\$0.05/minute	\$0.05/minute	\$0.05/minute	\$0.00	
Word Alert and PRO (Contract Option)	Full Investigative Suite of Both Applications	\$0.01/minute	\$0.01/minute	\$0.01/minute	\$0.01/minute	\$0.01/minute	\$0.01/minute	\$0.01/minute	\$0.01/minute	\$0.01/minute	\$0.01/minute	\$0.01/minute	\$0.01/minute	\$0.00	
Detainee Disciplinary Sanction Fee for Excessive Breakage of Tablets or Video Kiosks	Sanction for a Detainee that is found guilty through a disciplinary hearing of inflicting damage to Tablets or Video Kiosks (if- pool) due to vandalism and not due to defective devices.	\$7.00/infraction for tablets \$4,500 for Video Kiosks	\$7.00/infraction for tablets \$4,500 for Video Kiosks	\$7.00/infraction for tablets \$4,500 for Video Kiosks	\$7.00/infraction for tablets \$4,500 for Video Kiosks	\$7.00/infraction for tablets \$4,500 for Video Kiosks	\$7.00/infraction for tablets \$4,500 for Video Kiosks	\$7.00/infraction for tablets \$4,500 for Video Kiosks	\$7.00/infraction for tablets \$4,500 for Video Kiosks	\$7.00/infraction for tablets \$4,500 for Video Kiosks	\$7.00/infraction for tablets \$4,500 for Video Kiosks	\$7.00/infraction for tablets \$4,500 for Video Kiosks	\$7.00/infraction for tablets \$4,500 for Video Kiosks	\$0.00	
Transition Call Rate	Match current call rate until label implementation is complete	\$0.045/minute	\$0.045/minute	\$0.045/minute	\$0.045/minute	\$0.045/minute	\$0.045/minute	\$0.045/minute	\$0.045/minute	\$0.045/minute	\$0.045/minute	\$0.045/minute	\$0.045/minute	\$0.00	
<b>Total Table B-4: \$108.90</b>															
<b>Table C</b>															
The Bundle Packages below shall represent all additional services available through the Contractor, which may be provided to the Detainees and public at the stated fees.															
Bundle Packages/Subscription name	Contractor Assumptions Contractor has stated below, in narrative form and in detail, ANY AND ALL applications available within the bundle at the stated fee, and ANY AND ALL assumptions, limitations and explanations that the Contractor has made in providing the stated services.	Fee	Fee	Fee	Fee	Fee	Fee	Fee	Fee	Fee	Fee	Fee	Fee	Total	
		Year 1	Year 2	Year 3	Year 4	Year 5	Year 1	Year 2	Year 3	Year 4	Year 5	Year 5	INITIAL TERM AND OPTION TO RENEW		
Contractor Move and TV Bundle (monthly)	Contractor offers the opportunity to rent individual movies and TV shows, individual movie and TV shows prices range from five up to \$9.99 per movie or TV show. Optional monthly subscription services are available based on the quality and quantity of movies and TV shows included. The Bronze package includes 50 basic movies and TV shows at a monthly fee of \$3.99, the Silver package includes 50 newer feature movies and TV shows at a monthly fee of \$5.99, and the Gold package includes 100 newly released movies and TV shows at a monthly fee of \$7.99. The price shown is for the BRONZE PACKAGE.	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$5.99	\$59.90	
Movie Share Package Bundle (monthly)	SILVER PACKAGE as described above.	\$11.99	\$11.99	\$11.99	\$11.99	\$11.99	\$11.99	\$11.99	\$11.99	\$11.99	\$11.99	\$11.99	\$11.99	\$119.81	

MDC075



## **SECURITY ADDENDUM**

---

The following pages contain the legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum (H2-H4); the Security Addendum itself (H5-H6); and the Security Addendum Certification page (H7).

## **Annex A**

### **FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM**

#### **Legal Authority for and Purpose and Genesis of the Security Addendum**

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.

We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental

agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

- a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:
  - 1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.
  - 2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and
  - 3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United

States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

**FEDERAL BUREAU OF INVESTIGATION**  
**CRIMINAL JUSTICE INFORMATION SERVICES**  
**SECURITY ADDENDUM**

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

- a. Investigate or decline to investigate any report of unauthorized use;
- b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Assistant Director

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

## Annex B

### FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM

#### CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

---

Printed Name/Signature of Contractor Employee

---

Date

---

Printed Name/Signature of Contractor Representative

---

Date

---

Organization and Title of Contractor Representative



## Cloud Service Usage Policy

### 1. History:

Effective Date	Version	Version Date	Purpose of Revision	Author
	0.1	11/15/2017	Base Document	David Piniella
	0.2	11/16/2017	Extending scope, additional detail	David Piniella
	1.0	09/26/2018	Extending scope, additional detail	Lawrence Embil
	1.1	11/21/2019	Extending scope, additional detail, clarity	Lawrence Embil

### 2. Overview:

The purpose of this policy is to provide guidance and governance pertaining to permitted usage of cloud services by Miami-Dade County.

### 3. Scope:

This standard applies to all departments, employees, contractors, consultants, temporary and other workers at MDC, including all personnel affiliated with third parties providing services to, or on behalf of MDC.

### 4. Authority:

This standard is being implemented under the authority of the ITD Department Director, and the Chief Information Security Officer (CISO) in compliance with **Procedures for the Protection of County Protected Data**.

### 5. Related Publications:

[MDC Enterprise Information Security Policy Manual](#)

Procedures for the Protection of County Protected Data

### 6. Supersedes:

In the event that this standard, in whole or in part, overlaps any portion of any other ITD information security policy, the most restrictive setting of those in question will take effect.

### 7. Definitions:

- **Cloud Services:** A computing or storage service hosted online or in a server/infrastructure/datacentre outside of Miami-Dade County's datacenter/infrastructure. Including but not limited to, Amazon Web Service (AWS), Microsoft Azure, Google Drive, Box, Dropbox, Google Cloud Platform, IBM Cloud, VMWare Cloud, DigitalOcean, Rackspace, etc.
- **Software As A Service (SaaS):** Cloud computing service models include network access to business software applications hosted in the cloud by a third party. This model allows costs of software development and hosting to be shared among subscribers. Business software in this category is often configurable to a limited extent with standard options offered to all subscribers.
- **Infrastructure As A Service (IaaS):** Cloud services which permit network access to traditional computing resources such as processing power and storage.

- **Platform As A Service (PaaS):** Cloud services which permit network access to an environment for agencies to use, build or operate their own software.
- **File Sharing Sites:** Online storage repository site or service including (but not limited to) Dropbox, Google Drive, Microsoft OneDrive, Box, Apple iCloud, etc
- **Machine Learning Analytics:** A smart data discovery service available on the cloud, it guides data exploration, automates predictive analytics and enables effortless dashboard and infographic creation.
- **Personally Identifiable Information (PII):** Information that can be used (either alone or in combination with other information) to identify, contact or locate a unique person. Examples include (but are not limited to): name, social security number, address, birth date, telephone number, account numbers, etc.
- **Service Organization Control report (SOC2):** Service Organization Controls reports are designed to help service organizations, organizations that operate information systems and provide information system services to other entities, build trust and confidence in their service delivery processes and controls

8. Content:

- A. Cloud services (SaaS, PaaS or IaaS) are not allowed for Miami-Dade County use except as an exemption from the Enterprise Security Office or according to the provisions of this standard. Miami-Dade County departments and individuals are allowed to request an exemption for a specific cloud service.
- B. A request for exemption from the MDC Enterprise Security Office for any Cloud service shall be submitted by way of a Security Review Request and include the following documentation
- C. Description of the project for which an exemption is requested. The description shall include the name of the service (application), its function, and its intended use by the agency. In addition, the description shall identify the hosting entity, the entity that provides the service (developer) and supports the service (maintains, provides trouble support, etc.), and the locations at which the service will be hosted.
- D. Assurance that the agency has submitted a Business Case to MDC/ESO, or information in lieu of these items required by the Request for Exemption form.
- E. A security review for the proposed usage, including business impact and security implications/risks posed.
- F. Appropriate back-up, data retention, and recovery services to meet the needs of the agency and that state data can be retrieved should it be necessary.
- G. Data protection measures including encryption of sensitive data at rest and sensitive data in while being transmitted. This includes data stored on or transmitted to portable devices. Encryption keys will be maintained by the data owner or in a key escrow of MDC's choosing.
- H. Cloud providers servicing MDC departments or individuals should have SOC2 reporting capabilities available. Appropriate audit and security controls must be available, in place and in use with the appropriate level of care required for the data classification involved (PII, PCI, CJIS, HIPAA, etc).
- I. Cloud Service providers must have Risk Management policies and strategies in place to mitigate data security risks and safety. FedRAMP certification is preferred but not required.
- J. Cloud Service used must store or limit MDC-affiliated data within the continental United States (CONUS). Use of non-US cloud computing resources (storage, processing, analysis etc) is not permitted.
- K. Cloud computing agreements between Miami-Dade County and any service providers must specify that Miami-Dade County data ownership is retained by Miami-Dade County and non-Miami-Dade County usage of MDC-related data, specifically including but not limited to PII, PCI, HIPAA and CJIS data is not permitted. Data will be stored and located in servers/datacenters within the continental US. Any use of Miami-Dade County data with any cloud services providers will allow for export and removal of Miami-Dade County data from the cloud service providers use/control upon request.

- L. Cloud computing providers will have availability and disaster recovery policies and strategies policies and strategies in place to ensure mission-critical data or resources are available if required for business continuity purposes.
- M. Cloud service providers will perform criminal background checks on staff and subcontractors.
- N. Cloud service provider agreements must provide for orderly data transfer in an agreeable format in the event of termination and suspension of service. Contracts will set out specific time periods in which the service provider must continue to maintain the data. The service provider agrees to provide any post-termination assistance that it generally makes available to other clients, unless the parties agree to a specific and unique procedure in the SLA. The service provider agrees to destroy all data when requested by the public jurisdiction in accordance with NIST-approved methods and provide a certificate of destruction.

9. Exceptions:

All exception requests must be submitted for approval through the Network Service Desk (nsd) or Remedy service queue. Verbal and email approvals will not be accepted.

10. Review:

This standard will be reviewed one (1) year from the effective date, and every two (2) years thereafter.

This standard will be reviewed by the Chief Security Officer by this date: October 1, 2021.

11. Compliance:

Non-compliance may result in escalation to the Department Director and as a result, parties may be subject to formal reprimands and other progressive disciplinary actions as prescribed in Dade County Personnel Rules and [Administrative Order 7-3: Disciplinary Action](#).

X 

---

Lars M. Schmekel  
Chief Security Officer



## **Miami Dade County**

### **Payment Card Industry**

# **Executive Charter and Compliance Policy 332**

Updated: 11/2021

MDC087

**Revisions to Policy:**

This section documents the revisions made to this policy since the last approved version dated January 2021.

<b>Effective Date</b>	<b>Version</b>	<b>Description</b>	<b>Pages</b>
October 2019	332.1.0	General grammatical changes	
January 2021	332.2.0	Added Applicable Policies and Procedures and required training	8
		General grammatical changes	3,5,6,8,9,10,13,14,16,17,18,20,21
November 2021	332.3.0	Updated number of departments accepting payments	3
		Updated Required Training title	8
		Added bullet item where Vendor is Contractually Liable	9
		Updated PCI Liaison Responsibilities	10
		Added language for Quarterly vulnerability scans	13
		Third-party Vendor Risk Management requirement update	14
		Project Calendar items updated	19,20,21
		General Grammatical changes	3,6,8,9,10,13,14,16,17,18,19,20,21

## Table of Contents

I.	Purpose .....	3
II.	Overview.....	3
III.	Definitions.....	4
IV.	Accountability.....	6
V.	Applicability.....	6
VI.	Goals and Applicable Policies and Standards.....	7
	A. Goals.....	7
	B. Applicable Policies and Procedures.....	8
	C. Required Information Security and PCI Training.....	8
VII.	Roles and Responsibilities.....	8
	A. Departments.....	8
	B. Department’s PCI Liaison.....	9
	C. Internal Services.....	11
	D. Finance.....	11
	E. Information Technology.....	12
VIII.	PCI Compliance Measures of Success.....	13
IX.	Retention and Disposal.....	14
X.	Annual PCI-DSS Assessment.....	14
XI.	Response to a Security Breach.....	14
XII.	Third Party Vendor Risk Management.....	14
XIII.	Annual Review.....	15
XIV.	Credit Card Acceptance and Processing Procedures.....	15
XV.	Contract Language for Credit Card Payment System.....	15
XVI.	PCI Project Calendar.....	16
XVII.	Signature Page.....	22

## **I. Purpose**

The purpose of this policy is to assist in mitigating the risk of credit card fraud, hacking, and various other security vulnerabilities and threats, and to reduce the risk of a breach of cardholder data by adhering to the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS was developed by the founding members, comprised of American Express, MasterCard Worldwide, Visa Inc. Discover Financial Services, and JCB International, of the Payment Card Industry Security Standards Council (PCI SSC). The PCI SSC is responsible for managing and updating the security standards while compliance is enforced by the individual payment card brands. This policy will provide strategic direction and support to Miami-Dade County's (MDC) departments/agencies processing credit card transactions as required by PCI DSS Req.#12.4.1.

## **II. Overview**

MDC processes more than five million transactions annually accounting for over \$508 million dollars in credit card payments. There are twenty-three (23) departments/agencies in MDC that process credit card payments at over 200 locations using a variety of payment channels, including but not limited to, Point of Sale (POS) devices, in-house developed applications, third-party payment applications, phone, and in-person.

Annually, each department is required to complete and update its credit card procedures explaining how transactions are processed in their respective department. These procedures shall be approved and signed by the department's PCI Liaison and the department's executive management (Department Directors). The updates include: credit card procedures, Merchant ID (MID) report, the vendor's PCI compliance certification, technical diagrams, and inventory reports. The approved procedures along with the additional documentation are submitted to the Finance department by the respective department's PCI Liaison and posted to the PCI share drive (shared file access point). The Finance Cash Management and the Compliance and Administration Division's will review procedures and MID reports to ensure compliance with County's Policy and PCI requirements. The Information Technology Department Security Division (ITD) reviews PCI certification, technical diagrams and inventory reports for compliance with PCI, technical, and security policies/procedures.

New department requests to process credit card transactions or changes in processes require resubmittal of procedures to be approved prior to procurement and/or development. A review for internal controls and

compliance with the Payment Card Industry Data Security Standards (PCI-DSS) is completed and reviewed for approval by the Finance Department.

ITD conducts monthly internal scans based on inventory reports as provided by each of the departments and regularly checks the network and processes for any vulnerabilities. A quarterly scan result for the external facing devices is submitted to County processor(s). Annual internal and external penetration tests and risk assessment are completed to identify any threats and/or vulnerabilities requiring remediation. Bi-annual field visits are conducted by the Finance Compliance section to monitor for and assist departments with PCI compliance.

### III. Definitions

**Account Number** – The unique payment card number (credit or debit card) that identifies the issuer and the particular cardholder account. Also referred to as “PAN” or “Primary Account Number”.

**Acquirer** – Also referred to as “acquiring bank” or “acquiring financial institution”. Entity that initiates and maintains relationships with merchants for acceptance of payment cards.

**AOC** - Acronym for “Attestation of Compliance.” The AOC is a form for merchants and service providers to attest to the results of a PCI DSS assessment, as documented in the Self-Assessment Questionnaire or Report on Compliance.

**ASV** – “Approved Scanning Vendor” - vendor who provides security and compliance services. For PCI compliance we are required to do a Quarterly external vulnerability scan using the services of an ASV and achieve a “PASS”.

**Cardholder** – Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card.

**Cardholder data** - any personally-identifiable data associated with a cardholder. Examples include, but are not limited to account number, expiration date, card type, name, address, and card validation code – the three or four-digit value printed on the front or back of a payment card referred to as CAV, CVC, CVV, or CSC depending on the payment card brand. The term cardholder data is interchangeable with payment card data throughout this policy.

**Card Skimmer** - A physical device, often attached to a legitimate card-reading device, designed to illegitimately capture and/or store the information from a payment card.

**Masking** - In the context of PCI DSS, it is a method of concealing a segment of data when displayed or printed. Masking is used when there is no business

requirement to view the entire PAN. Masking relates to protection of PAN when displayed or printed. See “Truncation” (definition below) for protection of PAN when stored in files, databases, etc.

**Merchant** – A department approved to accept payment cards at a given location as payment for goods and/or services or receipt of donations.

**Merchant Identification Number** – A unique number that identifies the department approved to accept payment cards.

**P2PE (Point to Point Encryption)** – is a combination of secure devices, applications and processes that encrypt data from the point of interaction (for example, at the point of swipe, insert, tap, dip or manual entry) until the data reaches the solution providers’ secure decryption environment.

**Payment Card** – Any credit, debit, or private label card accepted as a form of payment for goods and/or services or receipt of donations.

**Payment Card Application** – Any hardware, software, or combination of hardware and software that aid in the processing, transmitting or storing of cardholder data as part of authorization or settlement. Examples include point of sale (POS) devices, ecommerce shopping carts, web-based payment applications, and third party (vendor) provided systems.

**PCI** - Acronym for “Payment Card Industry.”

**Payment Card Industry Data Security Standard (PCI DSS)** – PCI DSS is a worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard applies to all organizations that hold, process, or pass cardholder information from any card branded with the logo of one of the card brands. The standard is maintained by the PCI SSC, which maintains both the PCI DSS and a number of other standards, such as the Payment Card Industry PIN Entry Device security requirements (PCI PED) and the Payment Application Data Security Standard (PA DSS). The PCI DSS includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. The PCI DSS may be accessed at: <https://www.pcisecuritystandards.org/>.

**Payment Card Industry Data Security Standard Self-Assessment Questionnaire (PCI DSS SAQ)** – The PCI DSS SAQ is a validation tool intended to assist merchants and service providers in self-evaluating their compliance with the PCI DSS. There are multiple versions of the PCI DSS SAQ to meet various scenarios. Each unique version of the PCI DSS SAQ includes a Self-Assessment Questionnaire and Attestation of Compliance that must be completed annually by the merchant and/or service provider as appropriate.

**Payment Card Processing** – The processing, transmitting, and/or storing of cardholder data, i.e., acceptance of credit or debit cards.

**Primary Account Number (PAN)** – The unique payment card number (credit or debit card) that identifies the issuer and the particular cardholder account. Also referred to as “Account Number”.

**QSA** - Acronym for “Qualified Security Assessor.” QSAs are qualified by PCI SSC to perform PCI DSS on-site assessments. Refer to the QSA Qualification Requirements for details about requirements for QSA Companies and Employees.

**ROC** - Acronym for “Report on Compliance.” Report documenting detailed results from an entity’s PCI DSS assessment.

**SAQ** - Acronym for “Self-Assessment Questionnaire.” See “Payment Card Industry Data Security Standard Self-Assessment Questionnaire” (definition above) reporting tool used to document self-assessment results from an entity’s PCI DSS assessment.

**Truncation** - Method of rendering the full PAN unreadable by permanently removing a segment of PAN data. Truncation relates to protection of PAN when stored in files, databases, etc. See “Masking” (definition above) for protection of PAN when displayed on screens, paper receipts, etc.

#### **IV. Accountability**

MDC departments processing credit card transactions are required to adhere and comply with all applicable policies and procedures. Department Directors have full oversight over their respective departments and provide appropriate approvals including those of the SAQ and AOC. The Finance department reviews and monitors departmental PCI compliance and applicable policies and procedures. ITD reviews and monitors departmental PCI compliance and compliance with technology related guidelines/regulations. The Chief Financial Officer/Finance Director approves the countywide SAQ and AOC.

The objectives of this policy are to ensure compliance with the PCI DSS and other applicable policies and standards, establish the governance structure for payment card processing and compliance activities, define responsibilities for payment card services, and provide general guidelines regarding the handling of cardholder data.

#### **V. Applicability**

This policy applies to all personnel responsible for processing, reviewing, reconciling, approving credit transactions or processes, and/or developing credit card applications. This policy also applies to any department who contracts with a third-party vendor to handle and/or process cardholder data

on behalf of MDC. All vendors, contractors, and business partners who store, process, transmit, or have access to cardholder data on behalf of MDC must contractually agree to be compliant with the current version of the PCI DSS during the contract period.

## **VI. Goals and Applicable Policies and Standards**

### **Payment Card Industry Data Security Standard**

The PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store, or transmit cardholder data. It consists of common sense steps that mirror security best practices. Below is a high-level overview of the PCI DSS requirements. The complete standard is accessible at the [PCI Security Council website](#).

#### **A. Goals**

##### **Build and maintain secure network and systems.**

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

##### **Protect Cardholder Data**

3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.

##### **Maintain a Vulnerability Management Program**

5. Protect all systems against malware and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.

##### **Implement Strong Access Control Measures**

7. Restrict access to cardholder data by business need to know.
8. Identify and authenticate access to system components.
9. Restrict physical access to cardholder data.

##### **Regularly monitor and test networks.**

10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.

##### **Maintain an Information Security Policy.**

12. Maintain a policy that addresses information security for all personnel.

## B. Applicable Policies and Procedures

1. 333 - Credit Card Acceptance and Processing Procedures  
<https://www.miamidade.gov/managementandbudget/library/procedures/333.pdf>
2. PCI Incident Response Plan  
<http://intra.miamidade.gov/finance/library/guidelines/incident-response-plan.pdf>
3. MDC Enterprise Information Security Policy Manual  
<http://intra.miamidade.gov/technology/library/guidelines/security-policy-manual.pdf>
4. Miami Dade County Identity Theft Prevention Program (Red Flags)- Resolution R-580-10  
<http://www.miamidade.gov/govaction/legistarfiles/Matters/Y2010/101045.pdf>

## C. Required Information Security and PCI Training

1. New Employees
  - Security Awareness Training
  - Defending Against Phishers
  - PCI Essentials for Account Data Handlers and Supervisors
2. Current Employees
  - Security Awareness Annual re-fresher
  - PCI Essentials for Account Data Handlers and Supervisors

## VII. Roles and Responsibilities

### A. **Departments processing credit card payments** – are responsible for:

- Assigning a PCI Liaison.
- Management and employees responsible for processing, reviewing, reconciling, and approving credit card payments must be familiar with and adhere to the PCI DSS requirements of the PCI Security Standards Council; management must also ensure employees take the annual mandatory courses as outlined in Section C: above.
- Requesting approval from Finance and Information Technology prior to purchase of payment application/software to ensure PCI Compliance.
- Ensure vendors adhere to “Contract Language for Credit Card Payment Systems” for new third-party payment applications prior to executing a contract in Procedure #333, as referenced in Section B above.

- Ensuring that the vendor agrees to be held contractually liable for adherence to the Payment Card Industry compliance for the contract period, including subsequent contract renewals/extensions.
- Implement and annually update the business procedures described in Procedure #333, as referenced in Section B above, including completion of the “Template for Requesting New and Updated Services” and following those guidelines when requesting approval prior to procurement and/or development from the Finance Department to process credit card payments for new services (Merchant Identification Number (MID’s) requests).
- Protecting credit card data in compliance with policies referenced in Section B. above, and the PCI DSS Standards.
- Reviewing and updating departmental procedures annually in accordance with established guidelines.
- On an annual basis, obtain certification of PCI compliance for vendor applications, such as, PA DSS, P2PE validation, or AOC. In addition, departments must retain vendor PCI related documentation, including but not limited to credit card diagrams/flow, policies, procedures, and tampering logs.
- Ensuring that sensitive credit card data is not stored in any form (digitally, hardcopy or voice recording).
- For third-party payment systems, apply patches for applications within 30 days of release.
- Reviewing and taking corrective action on the monthly security scan reports from the ASV and any other application security scans provided.
- Regularly checking Point of Sale (POS) devices for tampering (skimmers) and documenting/logging findings (even if no evidence of tampering is evident).
- Assisting Finance, ITD, and the QSA during the compliance process.
- Annual Review and approval of SAQ, ROC, and AOC for credit card applications.

**B. Department PCI Liaison’s** – are responsible for:

- Adhering to the responsibilities under the *Departments Processing Credit Card Payments*, Section A above, as well as those listed in this section.

- Adhering to MDC Payment Card Industry Executive Charter and Compliance Policy, in addition to the policies and procedures outlined in Section B above, and the PCI-DSS Standards.
- Reminding department divisions/sections of the requirements regarding prior approvals for purchases of payment applications/software on a quarterly basis.
- Ensuring that all staff involved with the credit card processing functions has had appropriate training which includes a review of all required PCI annual on-line training courses as outlined in Section C: above. All required training must be completed annually. Annual certification of training completion must be reviewed and approved by the respective department Director and submitted to the Finance Department.
- Informing employees of any changes and updates with the MDC Payment Card Industry Executive Charter, Credit Card Acceptance and Processing Procedures, and the PCI DSS standards.
- Implementing the business procedures described in Procedure #333, Credit Card Acceptance and Processing Procedures, including completion of the “Template for Requesting New and Updated Services” and following those guidelines when requesting approval prior to procurement and/or development from the Finance Department to process credit card payments for new services or Merchant Identification Number(s) (MID’s).
- Updating departmental procedures annually in accordance with established guidelines.
- Updating, maintaining and uploading PCI device inventory annually and as changes are made in a central location.
- On an annual basis, obtain certification of PCI compliance for vendor applications, (such as, PA DSS, P2PE validation or AOC). In addition, departments must retain vendor PCI related documentation, including but not limited to credit card diagrams/flow, policies, procedures, and tampering logs.
- Providing terminal inspection logs and ensuring that these are reviewed at least quarterly (even if no evidence of tampering is evident).
- Assisting Finance, ITD, and the QSA during the compliance process.
- Obtaining department approvals (by the Department Director) on the SAQ and AOC form, as mandated by the PCI DSS.

- In the event of a breach, or the suspicion that payment card data has been exposed, lost, stolen, or misused, immediately submit a PCI Incident Report to ITD. The Department's Liaison will work with the PCI Core Team (members from ITD and Finance) and follow the appropriate instructions in accordance with MDC's PCI DSS Incident Response Plan found in the PCI SharePoint.

**C. Internal Services Department** – is responsible for:

- Ensuring that vendors provide official documentation as listed in Policy 332 MDC Payment Card Industry Executive Charter and Compliance Policy, and the "Contract Language for Credit Card Payment Systems".
- Including the "Contract Language for Credit Card Payment Systems" language in contracts/agreements for credit card payment applications/services. The Payment Card Industry Compliance language must be included in all RFP's, contracts, and agreements related to credit card payment applications.
- Ensuring that the vendor agrees to be held contractually liable for adherence to the Payment Card Industry compliance for the contract period, including subsequent contract renewals/extensions.

**D. Finance Department** – is responsible for:

- Establishing and enforcing policies and procedures for PCI DSS compliance.
- Assisting departments with understanding and documenting PCI DSS requirements.
- Establishing and maintaining relationships with the credit card payment merchant processing provider (currently Elavon).
- Reviewing and approving request for new credit card services ensuring that processes are in compliance with MDC procedures.
- Working with merchant provider to establish new credit card set up including the new MIDs.
- Jointly with ITD, reviewing documentation for PCI compliance certification.
- Jointly with ITD, approving any POS device or system to be used within MDC.

- Working together with ITD to engage the services of a PCI QSA, in consultation with the County Attorney's Office and Internal Services Department.
- Requesting, reviewing, and approving annual updates from each department for credit card procedures, third (3rd) party payment vendor compliance, training, and other documents required for the annual compliance and attestation process.
- Jointly with ITD, working with the QSA during the compliance review process to provide documentation, respond to inquiries, and conduct on-site visits.
- Obtain completed SAQ and AOC from QSA. Review and distribute to Departments PCI Liaison and Director for their review and approval.
- Approval of final SAQ and AOC by Deputy Mayor/Finance Director.
- Maintaining an updated listing of all departments that process credit card transactions using an approved merchant account.
- Conducting annual/bi-annual on-site visits to review processes and assists departments with PCI Compliance.
- Working together with ITD to conduct annual PCI presentations, training/education.
- Working together with ITD to monitor compliance with this policy.

**E. Information Technology Department** – is responsible for:

- Establishing and enforcing policies and procedures for PCI DSS compliance.
- Assisting departments with understanding and implementing PCI DSS technical security requirements.
- Ensuring that payment applications/software request for procurement through ITD have prior approval from ITD Security and Finance.
- Providing vulnerability assessments, technology reviews, risk assessment, compliance assessment and network segmentation services.
- Working together with the Finance Department to engage the services of a PCI QSA, in consultation with the County Attorney's Office and Internal Services Department.
- Jointly with the Finance Department, working with the QSA during the compliance review process to provide documentation, respond to inquiries, and conduct on-site visits.

- Jointly with the Finance Department, reviewing documentation for PCI compliance certification.
- Obtain completed SAQ and AOC from QSA. Review documents and obtain approvals for the Service Provider SAQ and AOC.
- Working together with the Finance Department to monitor and audit compliance with this policy.
- Working together with the Finance Department to conduct annual PCI presentations and training/education.
- Providing incident response and investigation services for security events impacting the cardholder data environment.
- Monitoring and reviewing computer and/or computer networks to ensure that security features are in place and are adequate to protect credit card data.
- Annually complete internal and external penetration testing.
- Bi-annually complete segmentation penetration testing.
- Semi-annually complete internal and external scans. Results are sent to merchant processor.
- Quarterly vulnerability scans and timely fixes to any risks identified.
- Annually update secure build standards and risk assessment.
- Provide online payment application development services:
  - Credit card transaction processing via MDC's Payment Gateway using MDC's credit card processor.

### **VIII. PCI Compliance Measures of Success**

1. Trained staff in the latest PCI DSS standards.
2. Updated and accessible MDC PCI Compliance Policy and Credit Card Processing Procedures.
3. Completed POS Tampering Inspection Logs.
4. Passing scores on ASV's Quarterly Scans.
5. Annual and Semi-Annual completion and follow-up on actionable items on Penetration Test(s).
6. Timely and compliant completion of annual PCI Compliance reporting (SAQs, AOCs, and/or ROC).

## **IX. Retention and Disposal**

Cardholder data shall not be retained/stored electronically or in paper form.

## **X. Annual PCI DSS Self-Assessment**

MDC's PCI Team (Finance and ITD Staff) will contact each department to schedule their annual self-assessment. Each department must have staff available to assist Finance and ITD when the QSA completes their assessment. Each department must complete and have the Department Director approve an annual self-assessment questionnaire to attest compliance with this policy, PCI DSS, and other applicable standards and policies. Departments found not in compliance will need to work to implement appropriate compensating controls or remediation activities.

## **XI. Response to a Security Breach (Incident Response Plan)**

In the event of a breach, or the suspicion that payment card data has been exposed, lost, stolen, or misused, the department must immediately submit a PCI incident report at: <https://nsd.miamidade.gov/sr/pciincrep>. The PCI Core Team (members from ITD and Finance) will review the incident response report. A member of the PCI Core Team will respond to the departmental PCI Liaison with appropriate instructions in accordance with MDC's PCI DSS Incident Response Plan found at: <https://miamidadecounty.sharepoint.com/sites/ITD-Intra/Shared%20Documents/Security/incident-response-plan.pdf?cid=e05afa4a-e09a-4a48-bb03-5506fa50bab7> .

In addition, refer to the Incident Response Plan for further instructions.

## **XII. Third Party Vendor Risk Management**

Before Miami Dade County executes an agreement with a payment application vendor, or contracts to do business with a vendor for credit card services, the vendor must adhere to the Contract Language for Credit Card Payment Systems; the initiating department must also obtain proof of PCI compliance/certification. The vendor must be held contractually liable for maintaining the PCI certification and all sections of the Contract Language for Credit Card Payment Systems, for the contract period, including subsequent contract renewals/extensions.

Any third-party vendor that processes, transmits, generates, stores, or otherwise accesses credit card data on MDC's behalf must sign MDC's Security Addendum. Departments should work with the Internal Services Department's Purchasing Division to initiate this process.

**XIII. Annual Review**

This policy will be reviewed on an annual basis in accordance with the PCI Standard. Departments that process credit card data will submit updated credit card procedures, a SAQ, network diagram, card flow diagram, and a signed AOC annually. Individuals who handle credit card data must complete education specific to the PCI standard annually. In addition, MDC will conduct a risk assessment in connection with PCI compliance that identifies emerging threats and vulnerabilities.

**XIV. Credit Card Acceptance and Processing Procedures**

A. Refer to County Policy # 333 regarding applicable procedures for credit card acceptance and processing, as outlined in Section VI, above.

**XV. Contract Language for Credit Card Payment Systems**

A. Refer to County procedure # 333, Credit Card Acceptance and Processing Procedures, Section V., for requirements applicable to all third-party payment vendor systems. Outlined in Section VI, above.

## **XVI. PCI Project Calendar**

### **JANUARY**

- County-wide kick-off meeting for current year credit card procedures, departments PCI compliance, and new year reporting period.
- Departments submit updated PCI documentation required:
  - Credit Card Procedures (SOPs)
  - PCI Compliance from 3<sup>rd</sup> party payment vendors
  - Updated Technical and Card Flow Diagrams
  - MID Listing
  - Inventory Report
- ITD completes quarterly review of monthly patch management for all system components and software application to credit card environment, as per PCI requirement 6.2. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD and Aviation completes quarterly internal and external vulnerability scans with summary report. Reports of results are provided to senior management by the 15<sup>th</sup> of the month and to merchant processor, as per PCI requirements 11.2.1 and 11.2.2.
- ITD completes quarterly anti-virus review, as per PCI requirement 5.2. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes quarterly review ensuring personnel are following security policies and operational procedures, as per PCI requirement 12.11. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completed quarterly testing for Wireless Wardriving to detect and identify all authorized and unauthorized wireless access points, as per PCI requirement 11.1. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- Finance Compliance section to work with departments to update the following for the new year: credit card policy, MID reports, inventory list, and detailed credit card flows. Annual sign-off sheet with results is uploaded into the central location.
- Departments deadline to complete PCI online course.

- Departments to submit their annual PCI device inventory into the central location semi-annually.
- PCI Core Team members (ITD & Finance) meet bi-weekly.
- PCI Core Team and senior management quarterly meeting updates.

## **FEBRUARY**

- Finance's Compliance section to create a report of departmental staff that completed PCI Course and provide to PCI Liaisons for review and approval by Department Director.
- Department's deadline to submit approved training reports to Finance and post in PCI central location.
- ITD completes patch management updates on all system components and software.
- ITD to conduct Risk Assessment Analysis of cardholder data environment.
- PCI Core Team members (ITD & Finance) meet bi-weekly.

## **MARCH**

- Finance Compliance section to create a Vendor Management listing and file with copies of all third-party vendor applications PCI compliance documents and upload to PCI central location. (Include Compensating Controls, if required).
- ITD completes patch management updates on all system components and software.
- PCI Core Team members (ITD & Finance) meet weekly.
- Jointly, Finance and ITD to begin working on annual AOC process with QSA.

## **APRIL**

- Departmental onsite/remote visits with QSA.
- Continue Attestation process.
- ITD conducts bi-annual Penetration Testing.
- ITD completes quarterly review of monthly patch management for all system components and software application to credit card environment,

as per PCI requirement 6.2. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.

- ITD and Aviation completes quarterly internal and external vulnerability scans with summary report. Reports of results are provided to senior management by the 15<sup>th</sup> of the month and to Merchant Processor, as per PCI requirements 11.2.1 and 11.2.2.
- ITD completes quarterly anti-virus review, as per PCI requirement 5.2. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes quarterly review, ensuring personnel are following security policies and operational procedures, as per PCI requirement 12.11. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completed quarterly testing for Wireless Wardriving to detect and identify all authorized and unauthorized wireless access points, as per PCI requirement 11.1. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- PCI Core Team members (ITD & Finance) meet weekly.
- PCI Core Team and senior management quarterly meeting updates.

### **MAY**

- Continue Attestation and Departmental on-site/remote visits by QSA.
- Finance Compliance section to obtain drafts of SAQs from QSA and send to Departments for review and approval by PCI Liaisons.
- ITD completes patch management updates on all system components and software.
- PCI Core Team members (ITD & Finance) meet weekly.

## **JUNE**

- Finance Compliance section to obtain final SAQ and Attestation documents for review and final signatures by Department Directors.
- Finance Compliance section to obtain final approved forms from Departments.
- Obtain final approval on submittal SAQs and Attestation from Deputy Mayor.
- Submission deadline for PCI compliance, submit final forms to Merchant providers.
- ITD completes patch management updates on all system components and software.
- PCI Core Team members (ITD & Finance) meet weekly.

## **JULY**

- Post-compliance review meeting with QSA, senior management, and PCI Core Team.
- Begin work on follow-up items.
- Procedural on-site visits conducted by Finance.
- ITD completes quarterly review of monthly patch management for all system components and software application to credit card environment, as per PCI requirement 6.2. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD and Aviation completes quarterly internal and external vulnerability scans with summary report. Reports of results are provided to senior management by the 15<sup>th</sup> of the month and to Merchant Processor, as per PCI requirements 11.2.1 and 11.2.2.
- ITD completes quarterly anti-virus review, as per PCI requirement 5.2. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes quarterly review ensuring personnel are following security policies and operational procedures, as per PCI requirement 12.11. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completed quarterly testing for Wireless Wardriving to detect and identify all authorized and unauthorized wireless access points, as per PCI

requirement 11.1. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.

- PCI Core Team and senior management quarterly meeting updates.

### **AUGUST**

- Post Audit work.
- Procedural on-site visits conducted by Finance Compliance section.
- ITD completes patch management updates on all system components and software.

### **SEPTEMBER**

- Procedural on-site visits conducted by Finance Compliance Section.
- Post Audit work.
- PCI Core Team to update PCI on-line training course to include new changes.
- ITD completes patch management updates on all system components and software.
- Quarterly sign-off sheet to be provided.

### **OCTOBER**

- Post Audit work.
- Procedural on-site visits conducted by Finance Compliance section.
- PCI Core Team to complete PCI on-line training course to include new changes.
- Bi-Annual Penetration Test.
- PCI Core Team to prepare PCI annual presentation.
- ITD completes quarterly review of monthly patch management for all system components and software application to credit card environment, as per PCI requirement 6.2. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD and Aviation completes quarterly internal and external vulnerability scans with summary report. Reports of results are provided to senior management by the 15<sup>th</sup> of the month and to Merchant Processor, as per PCI requirements 11.2.1 and 11.2.2.

- ITD completes quarterly anti-virus review, as per PCI requirement 5.2. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes quarterly review ensuring personnel are following security policies and operational procedures, as per PCI requirement 12.11. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completed quarterly testing for Wireless Wardriving to detect and identify all authorized and unauthorized wireless access points, as per PCI requirement 11.1. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- PCI Core Team to finalize PCI On-line training course to include new changes.
- PCI Core Team and senior management quarterly meeting updates.

#### **NOVEMBER/DECEMBER**

- PCI on-line training course available for employees that are responsible for processing, reviewing, reconciling, or approving credit card transactions, process, or systems.
- ITD to update and complete configuration standards.
- PCI Core Team to complete PCI annual presentation.
- Updates to policies and procedures (Finance & ITD policies).
- Finalize Post Audit recommendation and/or new year PCI requirements.
- Procedural on-site visits conducted by Finance Compliance section.
- ITD completes patch management updates on all system components and software.

**CONTRACT NO. RFP-02194  
ATTACHMENT G – INFORMATION TECHNOLOGY SECURITY MATRIX**

**Contractor's compliance with system requirements shall conform to the Contractor's affirmations below.**

The acceptable codes are as follows:  
 "Y" – Will be FULLY met (without configuration or modification).  
 "C" – Will be met via configuration (without changing base source code).  
 "M" – Will be met via modification of the base source code.  
 "N" – Will not be met. If an alternative compensating control is being proposed, please provide a detailed explanation. A blank or N/A in any box will be interpreted as an "N".

Requirement No.	Functionality	Meet (Y/C/M/N)	Module / Detailed Explanation
1	Solution uniquely identifies each user.	Y	
2	Solution provides integration with Microsoft Active Directory or Azure Active Directory for user authentication of Internal Users. (ADFS, FIM, MIM)	Y	
3	Solution can be installed and maintained in accordance to the Microsoft Active Directory administrative tier model: <a href="https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/reference-material">https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/reference-material</a>	Y	
4	Solution can be installed and maintained in accordance to the principle of least privilege for LINUX/UNIX systems.	Y	
5	Solution can be installed and maintained in accordance to the principle of least privilege for Database systems.	Y	

6	Solution uniquely identifies each process (system, service) account.	Y	
7	Solution supports scheduled password rotation of process (system, service) accounts.	Y	
8	Default System accounts are either disabled or capable of being renamed. (e.g. administrator/admin, guest)	Y	
9	Accounts are automatically disabled after a configurable period of inactivity (e.g. 30 days).	Y	
10	Solution utilizes account passwords for authentication.	Y	
11	Account Password complexity is configurable to allow for a minimum of 12 characters comprised of upper and lower alpha, numeric and special characters (e.g. !, @, #, \$, %, &, *)	Y	
12	Passwords are suppressed (not echoed back) when entered by users.	Y	

13	Solution supports Multi-Factor Authentication (MFA)	Y	
14	User login credentials (user account/password) are encrypted in transmission with a minimum of AES 256 bit encryption	Y	
15	Solution supports password history functionality whereby password reuse is prohibited for a configurable number of prior passwords of at least 10.	Y	
16	Solution supports administrative passwords aging of 30 days.	Y	
17	Administrative accounts have the capability of resetting passwords	Y	
18	Solution provides user self-service password reset functionality utilizing a challenge and response authentication	Y	
19	Solution includes self-service challenge and response that are comprised of 3 challenge questions and stores user's responses during registration. Responses must be stored with a minimum of AES 256 bit encryption	Y	

20	Solution includes self-service password reset that presents user with a configurable number of random challenge questions which when answered correctly will enable the password to be reset.	Y	
21	Solution supports the ability to limit unsuccessful login attempts to 5. If the number of unsuccessful login attempts is exceeded, system locks out or disables user account.	Y	
22	Solution supports limiting concurrent user sessions to 1 by default, and the number of concurrent user sessions is configurable by administrators.	Y	
23	Solution provides administrative capability to lock or disable accounts whenever necessary.	Y	
24	Solution supports the display of a configurable warning pre-login banner during solution login indicating that unauthorized access is prohibited.	Y	
25	Solution supports the ability to manage users based on group membership. (role-based privileges) In addition to assigning/revoking specific user based privileges	Y	
26	Solution provides tools and reporting to enumerate user rights/privileges, group membership, access to locations/functions or user profiles	Y	

27	Solution provides audit logging capability which captures successful logins, unsuccessful logins, records viewed, printed, added, deleted or modified and has the capability to retain logs for a period of 5 years plus current.	Y	
28	Solution audit logs captures date and time, user account, source IP address, audit event and success or failure of event	Y	
29	Solution prohibits administrators from disabling the audit mechanism.	Y	
30	Solution ensures the audit log is protected from unauthorized access. (i.e. logs are capable of simultaneously being sent to a logging server or SIEM in addition to being maintained locally)	Y	
31	Solution prevents users or administrators from editing the audit log. (modifying, deleting or adding log entries)	Y	
32	Solution provides for software version controls to prevent outdated versions of software access to DBMS.	Y	
33	Solution generates outbound alerts and notifications. Explain what data is contained in said messages (e.g. email alerts, automated reports, SNMP traps).	Y	

34	If Solution's database is relational, referential integrity is enforced by the RDBMS	Y	
35	Solution prohibits users, developers, DBAs or system administrators from making changes to posted, completed or closed transaction records	Y	
36	Solution provides rollback processes incorporated into the database for all critical transactions	Y	
37	Solution ensures that sensitive data (data that falls under the scope of FSS 539.003, CJS, PII, SOX, HIPAA, and PCI requirements) is encrypted during transmission over the client's network (minimum AES 256-bit encryption)	Y	
38	If Cloud Hosted, Solution is hosted in an audited data center complying with ISO 27001, SAS 70, SSAE 16 or SOC2 v3 audit standards. (please provide copy of most recent audit)	Y	Solution is SaaS, not cloud-hosted. Securus utilizes co-location facilities for its data center services. Securus warrants that the leased space used in that co-located facility is FISMA certified. Securus is FISMA compliant, PCI-DSS compliant, and SOC 3 / SOC 2 Type 2 compliant.
39	If Cloud Hosted, Solutions has controls in place which prohibit Hosting or Solution's employees or 3rd party vendor technical support personnel access to or the ability to access, view or modify customer confidential data in compliance with FSS 536.003. Please describe controls used to ensure data confidentiality, including encryption and key storage mechanisms.	Y	Solution is not cloud-hosted.
40	If Cloud Hosted, Solution is a high availability solution with either active-active or active-passive failover between geographically diverse data centers	Y	Solution is SaaS, not cloud-hosted. Solution is active-passive failover between geographically diverse data centers (Dallas, Texas and Atlanta, Georgia)

41	If Cloud Hosted, System and data is physically located within the Continental United States.	Y	Solution is SaaS, not cloud-hosted. Systems and data are physically located within the Continental United States (Dallas, Texas and Atlanta, Georgia).
42	If Cloud Hosted, System is accessible from the County network and Proxy infrastructure	Y	Solution is SaaS, not cloud-hosted, and depending on Miami-Dade's network, should be able to access the Securus solution.
43	If Cloud Hosted, System encrypts all sessions from initiation to termination using validated encryption ciphers (TLS 1.2 or higher)	Y	Solution is SaaS, not cloud-hosted. All sessions, from initiation to termination, are encrypted using TLS 1.2 or higher.
44	If Cloud Hosted, Solution is scanned for vulnerabilities on a regular basis (monthly) using commercially available vulnerability scanners such as Nessus, Qualys etc. Monthly vulnerability reports must be shared with the County.	Y	Solution is SaaS, not cloud-hosted. Securus scans its workstations and servers on a monthly basis using commercially available vulnerability scanners. Reports are considered proprietary, and cannot be shared with clients.
45	Solution must be regularly patched with appropriate OS/database/application security patches within 30 days of vendor release.	Y	
46	Solution must have "Critical" security patches applied within 7 (seven) calendar days of release from vendor.	Y	
47	Solution must be maintained on current supported release of OS/database/applications. End of Life (EOL) versions will be upgraded prior to end of vendor support date.	Y	

48	Solution must be scanned for Application vulnerabilities on a regular basis (monthly) using commercially available vulnerability scanners such as HP Web Inspect, Veracode, or IBM, AppScan, or comparable.	Y	
49	If Cloud Hosted, Solution or solution will have change control processes implemented to provide application vulnerability scanning (PCI, OVA/SF top 20) prior to production migration of any changes. All Medium, Critical, and Severe vulnerabilities will be remediated prior to migration. Application vulnerability reports will be shared with the County.	Y	
50	Any API must use API key security (X-APKey) or demonstrate alternate security controls.	Y	
51	If Cloud Hosted, Solution is protected using Intrusion Detection and Prevention technology (IDS/IPS)	Y	
52	If Cloud Hosted, Solution is protected against Distributed Denial of Service (DDoS) Attack	Y	

**CONTRACT NO. RFP-02194  
ATTACHMENT H – DETAINEE COMMUNICATIONS SOLUTION FUNCTIONALITY**

**Contractor's compliance with system requirements shall conform to the Contractor's affirmations below.**

The acceptable codes are as follows:  
 "Y" – Will be FULLY met (without configuration or modification).  
 "C" – Will be met via configuration (without changing base source code).  
 "M" – Will be met via modification of the base source code.  
 "N" – Will not be met. If an alternative compensating control is being proposed, please provide a detailed explanation. A blank or N/A in any box will be interpreted as an "N".

Requirement No.	Functionality	Meet (Y/C/M/N)	Module / Detailed Explanation
<b>General Functionality:</b>			
1	Proprietary operating system (OS). Commercial tablets are not acceptable.	Y	
2	Detainee telephone calling from Tablets and Mobile/Stationary kiosks. Solution must prevent detainee from calling emergency services i.e., 911.	Y	
3	Detainee visitation management	Y	
4	Video Visitation capabilities.	Y	
5	Interface with Miami-Dade Public Library's digital content for detainees' consumption which is not in conflict with media offered by contractor.	Y	Will require development specific to Miami Dade Public Library.

6	Mobile and fixed device menus, online messaging and postings, inmate regular and medical requests, grievances, educational content, and etc., must be trilingual. The applicable languages are English, Spanish, and Creole. The ability to translate to additional languages is beneficial but not a requirement.	Y	New applications may require development for Creole.
7	Effectively, efficiently, and expeditiously interface with all current and future technology systems providing services to MDCR as requested by MDCR to reduce redundant data entry, avoid unnecessary duplication of services, and increase efficiencies.	Y	
<b>Industry Standards</b>			
1	Comply with all applicable Federal, State, and local Americans with Disabilities Act (ADA) standards to include DISABILITY RIGHTS FLORIDA, INC.; CASE NO.: 2019CA-2825 settlement agreement between Florida Department of Corrections and Disability Rights Florida	Y	
2	Deploy as a wireless network with the ability to wirelessly provide updates to Operating System, devices and applications, including security patches or fixes. Security updates shall be implemented within 30 days of release.	Y	
3	Provide a minimum of ten (10) Video Relay service devices to serve the hearing-impaired detainees.	Y	All fixed kiosks can operate as video relay service devices allowing access anywhere as directed by MDCR.
4	3. Provide a minimum of five (5) Ubuntu3 wireless devices or comparable device and/or software for MDCR staff to communicate with detainees who are deaf or hard of hearing.	Y	
<b>Administration/Operational Functionality</b>			
1	Allow read only Open Database Connectivity (ODBC) access to MDCR for custom analytic tools.	N	For security purposes, Securus does not use ODBC; however, all data is exportable for MDCR's review and use.

2	Communication monitor/investigative software	Y	
3	Ability to generate analytic reports for MDCR to respond to trends	Y	
4	Ability to block service to any particular detainee for any particular amount of time and to remotely power off tablets and kiosks(s)	Y	
5	Allow MDCR supervisory staff the ability to assign varying access rights to administrators based on their respective role.	Y	
6	Ability to receive/deliver secure privileged mail electronically.	Y	
7	Ability to scan existing detainee legal mail/documents and personal mail to digital format available via Detainee profile.	Y	
8	Ability to have Behavioral Rewards platform for Detainees to earn credits to purchase premium items based on behavior award system and completion of educational material.	Y	Securus can provide a program called EDOVO to MDCR at a cost to the County.
9	Ability to enable communications from a Detainee to the Contractor to resolve any questions, problems, or concerns regarding charges, refunds, or other financial inquiries. MDCR will not be involved in any financial matters.	Y	

10	Ability to take a photo of the Detainee at login. Cameras must be disabled via the software and are only active for video visits and when taking the Detainee's photo at login or for other security purposes.	Y	
11	Allow MDCR to conduct surveys and communicate/notify Detainees of new policies/statements/messages and keep track of acknowledgement or completion.	Y	
12	Content may be streamed or downloaded. Detainees shall not own any content.	Y	
13	Provide personal cloud storage at no cost that holds Detainees' files such as email, photos, and other document content. This feature shall provide Detainees with the ability to retrieve their digital content up to thirty (30) days post release from MDCR custody.	Y	
14	All data transferred to or from the tablets and kiosks must be wireless. No physically wired connection may be required to send messages or send and/or receive data.	Y	
15	Electronic messaging. Detainee must be able to receive a photo from friends and family after going through a vetting process.	Y	
16	Contain an approved library of music, e-books, movies, and games.	Y	
17	Provide the Detainee the ability to login to any tablet or kiosk to access their personal account.	Y	

18	Electronic submission and tracking of requests and grievances, including the ability to customize both systems to follow MDCR's current workflow.	Y	
19	Interface with the County's Mug shot System that provides photographs of all Detainees booked into custody in Miami-Dade County.	Y	
20	Controlled profile access; Detainees' profiles can only be accessed in their assigned cell location, to prevent unauthorized access to their profile.	Y	
21	Unlimited remote system access by users defined in MDCR based on Active Directory roles, broken down into multiple categories and capabilities, e.g., Super User – can record, view, download, burn, etc.	Y	
22	Radio Frequency transmitters for all unit televisions in all and future MDCR facilities. Radio frequency receivers shall be installed on all tablets and kiosks at no charge for usage.	Y	All detainees tablets have a receiver.
23	Various charging options, i.e., wall-mounted and rolling mobile charging stations.	Y	
24	Caption Telephone software to accommodate detainees who can speak but cannot hear on the telephone.	Y	
25	Wide range of Talking/audio Books to accommodate visually impaired Detainees.	Y	

26	Text-to-speech software and training on its use to accommodate visually impaired Dialers.	Y	
27	Solution must log and retain all dialer and administrator's logging and activity history for a given period. All changes to imml/administrator accounts shall be logged and retained.	Y	
<b>Network Security</b>			
1	Provide network and control Internet access.	Y	
2	Network appliances must have access control lists that are capable of a 1) deny all or 2) whitelst approach.	Y	
3	Network appliances must have stateful inspection with 1) attack checking and 2) automatically discard traffic initiated from the internet.	Y	
4	Network appliances must have firewall and content filter capabilities	Y	
5	Network appliances must deploy only with Contractor's circuit so that only the Contractor's engineers have access to firewall.	Y	

6	Ability to encrypt transmitted data and authentication information.	Y	
7	Support for Secure Socket Layer (SSL) 128 bit and 256-bit encryption.	Y	
8	Contractor shall conduct interference (including network, Wi-Fi, or radio systems) testing prior to deployment and provide results to MDCR.	Y	
<b>Application Security</b>			
1	Must be a custom solution to meet the needs of MDCR.	C	
2	Built into the Operating System layer to prevent removal.	Y	
3	Critical Kiosk settings must be controlled remotely.	Y	
4	Ability to disable any Kiosk setting.	Y	

5	Ability to shut down any kiosk or group of kiosks remotely.	Y	
6	Ability to remotely erase/wipe (brick) device.	Y	
7	Ability to alert if device is root killed (bricked).	Y	
8	Updated applications can be installed remotely.	Y	
9	Tablet and Kiosk applications can be removed remotely.	Y	
10	Provide the ability for each user to be uniquely identified by the existing Jail Number	Y	
11	Provide basic authentication through use of PIN/Passwords.	Y	
12	Provide the ability to enforce password expiration.	Y	

13	Provide the ability to require automatic password expirations when initially assigned or reset.	Y	
14	Provide ability to support and configure complex password parameters such as password lengths, upper/lower alpha numeric and special characters configurable by MDCR, and user access to expiration settings and other behaviors.	Y	
<b>Tablet/Kiosk Requirements</b>			
1	Be made of approved materials and shall meet specifications established and approved by MDCR. Kiosks shall be wall or floor mounted, locked, with no moving parts and equipped with industrial glass touch screen. Kiosks shall be made of non-breakable parts that cannot be fashioned into weapons. Kiosks should have tamper evident seals and/or door alarms to indicate if units have been tampered with or opened and be secured with security screws with unique unlocking tool.	Y	
2	Have floor and/or wall anchors. Contractor shall ensure that each kiosk can be easily unsecured from the floor or the wall by personnel authorized by the MDCR.	Y	
3	Be free of sharp edges.	Y	
4	Comply with all federal, state, and local ADA mandates to include DISABILITY RIGHTS FLORIDA, INC. - CASE NO.: 2019-CA-2825 settlement agreement between Florida Department of Corrections and Disability Rights Florida, Inc. for accessible design to ensure ease of access for individuals with disabilities.	Y	
5	Supply a minimum of ten (10) Stationary Kiosks with durable security-centered keyboards for compliance with ADA, specifically visually impaired Detainees who could not use the kiosks utilizing the touchscreen. Location of these ADA Compliant Kiosk will be determined by MDCR.	Y	

6	Privacy enclosure: The Contractor shall supply a minimum of sixty (60) soundproof video conferencing privacy enclosures for existing facilities as well as any future facilities opened during the term of this contract. The enclosures shall be same or similarly approved units comparable to Spaceworkx Duramate Single POD with wall mounted Kiosk installed inside each unit. These correction's grade privacy enclosures will serve Detainees while engaging in privileged communication with attorneys. Up to four of these units may be required to meet ADA standards. Similar units may be acceptable if approved by the County.	Y	
7	Be on a rigid cart with wheel castors, sufficiently sized to easily fit through thirty-six (36) inch doors and fit through the security flap.	Y	
8	The headset cord must be in armored flex tubing and must be permanently attached to the cart	Y	
9	Hardened, proven in the corrections environment device and not an off-the-shelf product.	Y	
10	Case should be either sealed or accessible only by security screws with unique unlock tool.	Y	
11	USB charging of tablets and mobile kiosks is not allowed. Preferred Sovered - magnetic charging - the charging port attaches to and charges the tablets and kiosks via a magnetic connection. Tablets and Mobile Kiosks must not be able to be used to charge other devices. Any access ports must not allow data transfer by the Detainee.	Y	
12	Flame Resistant	Y	

13	Military Drop Tested	Y	
14	At least 32GB of onboard RAM, a battery of at least 8000mAh	Y	
15	Minimum 7" Screen Size	Y	
16	Non-Removable Lithium Battery	Y	
17	A variety of Tablet and Mobile Kiosk Charging Systems Available (i.e., mobile cart, secured wall units)	Y	
18	No working speakers, audio can only be activated by the use of headphones. Contractor must supply all Detainees with a pair of headphones, additional headphones may be purchased by the Detainee through commissary.	Y	
19	E-skeleton with a clear view of tablet and mobile kiosk components (so facility staff can visually inspect devices for physical intrusion and/or hardware modification)	Y	
20	USB port should not recognize human interface devices (i.e., keyboards).	Y	Yes; however, devices can be configured to support a keyboard for use in classroom settings if requested.

21	USB port should not recognize Ethernet connections.	Y	
22	Locked bootloder (Only Operating Systems digitally signed by Contractor can be installed)	Y	
23	Custom OS that removes risky OS features such as safe boot, factory reset, command line access, blue tooth, wireless lehring, etc.	Y	
24	OS should be capable of remote management that is inaccessible to Dealers.	Y	
25	Should have custom software for communicating with tablets and mobile kiosks from a connected computer. Tablets and mobile kiosk should be devoid of any standard communication tools.	Y	
26	All installed applications should be evaluated and approved by certified security experts in the field.	Y	
27	Wireless security provides the ability to remotely monitor the airspace of the prison and all wirelessly connected devices for security breaches.	Y	
28	Contractor shall monitor wireless activity and provide tools for facility security staff to monitor all wireless activity.	Y	

29	System should be able to remotely measure signal strength and noise floor of all tablets and mobile kiosks.	Y	
<b>Communication Requirements</b>			
<b>A.Video Visitation Module/Application</b>			
1	Ability to support multiple onsite visitation centers.	Y	
2	Ability to provide multiple off-site visitation centers within Miami Dade County.	Y	
3	Ability for staff to enroll, schedule, and manage visitation sessions at each onsite/off-site facility and/or remote visits.	Y	
4	Ability for friends and family registration for video visitation to be verified utilizing a government identification	Y	
5	Ability to provide a unified system to manage both onsite and web-based visitation from within the same Client Application.	Y	
6	Ability to assign a configurable fee based on visitor type.	Y	

7	Ability to configure visitation time slots and visitation policy language.	Y	
8	Ability for visitation scheduling system to consider the following factors when allowing/denying visitation: detainee quotas, detainee classification/location, detainee visitation bans, visitor visitation bans, visitor categories, overall visitation time policy, blackout dates or configurable holidays, detainee unavailable due to court, medical, or other reasons.	Y	
9	9. Allow all stations and ancillary components of the system to continue to operate without County staff or Contractor intervention in the event of primary failure.	Y	
10	When fallover occurs, send an alert displayed to officers using the system.	Y	
11	Web-based visitation site that allows users to register, schedule visitation, and conduct web-based visitation.	Y	
12	Web-based visitation site that provides interfaces at a minimum in English, Spanish, and Creole.	Y	
13	Capability to deliver media to a large variety of devices/operating systems (e.g., computers, tablets, mobile devices, etc.) and platforms.	Y	
14	Recording and storage of all friends and families visits and strict non-recording of any privileged visits.	Y	

15	Ability to save recording and provide transcriptions of all friends and families visits in real time.	Y	
16	Ability to provide Officers with the capability to ban visitors either temporarily or indefinitely based on IP address.	M	
17	System automatically removes a ban upon its expiration without MDCR staff intervention.	Y	
18	Allow Attorney visitor records to be clearly distinguishable from other visitor records, via an icon on the record.	Y	
19	Allow "in custody" detainee details such as cell location, etc. to be periodically imported into the system.	Y	
20	When detainees are released from custody, allow the record to be retained along with the detainee's visitation history.	Y	
21	Detainees visit quotas that are configurable based on visits per day, per week, and visits per month.	Y	
22	Require the public to accept a visitation policy that is configurable by MDCR prior to scheduling visitation.	Y	

23	Allow the public to cancel a visit when the visit is within a predetermined time frame of the visit's start time (e.g., 24 hours), as configured by MDCR.	Y	
24	Ability to monitor all friends and family visits in real time.	Y	
25	Ability to easily terminate a session from the live monitor screen and input a reason for termination.	Y	
26	Headsets at each station to allow the officers to privately monitor and/or conference into a visitation session.	Y	
27	Ability to allow investigators to view historical visitation sessions.	Y	
28	Ability to define privileged/attorney visit sessions in order to prevent recording.	Y	
29	Ability to quickly flag visitation sessions for future investigation.	Y	
30	Ability to download certain recordings on an as needed basis.	Y	

31	Ability to allow officers to define custom messages that will display on the detainee and visitor screens during a visitation session, at the start and end of a session, each with different possible messages.	C	Yes, but for security reasons, custom messages must be pre-approved by the County and pre-defined in the NextGen system.
32	Ability for MDCR staff to customize an audible file that will play shortly after both parties connect to a visit and near the end of the visit. Ability to define holidays and limit visitation based on holiday schedules.	C	
33	Under no circumstance are privileged video visits to be recorded. Contractor will conduct quarterly self-audits to ensure that no privileged communication is recorded and provide reports to MDCR accordingly.	Y	
<b>B. Telephone Module/Application</b>			
1	Ability to require a secondary PIN prior to placing a phone call.	Y	Manual and Biometric Pins used to validate caller.
2	Combination PIN and/or biometric features with a 99% cumulative reliability rate - initialization of telephone account to occur at the time of booking, and deactivation at time of release.	Y	
3	An interface with the Miami-Dade County Criminal Justice Information System (CJIS), the Automated A-Form System, the Detainee Profile System, the Mugshot system to manage active jail numbers (records) in real time and any applicable Jail Management System.	Y	
4	Customized and comprehensive Call Detail Reports as defined by MDCR.	Y	

5	The ability to provide/receive an encrypted file to other law enforcement Agency or State Attorney's Office through a secure FTP site.	Y	
6	Perpetual Reverse Phone Number Look-up of all employee/volunteer/contractor phone numbers provided in MDCR's employee system of record database and ability to run large list of staff/contractors/ volunteers' phone numbers on demand. Ability to receive alerts regarding any staff/contractor/volunteers for receipt of detainee phone calls. The Contractor will ensure that the integrity of this information is protected in accordance with the exemptions stipulated in Florida State Statute 119 titled, "Public Records."	Y	
7	Redaction software with the ability to locate and permanently remove personal and sensitive data within the recorded telephone call, as well as the ability to encrypt and secure the file.	N	All data related to communications and detainees is automatically encrypted and stored in multiple data centers. To preserve the integrity of the data for chain of evidence purposes, redaction within the system is not allowed. However, information may be downloaded and redacted with commercial redaction software.
8	Enhanced security and alert features to show patterns of hotline or toll-free abuse or misuse.	Y	
9	Ability to exempt calls by phone number from recording and/or from billing, i.e., attorney's offices and the Public Defender – but with the ability to have a call record that the call was made, by whom, date, time, status, and duration of the call.	Y	
10	Ability to exempt phone numbers from billing of charges (toll free) with all other features of the phone system as defined by MDCR.	Y	
11	Automatic hours of operations - ability to schedule active and non-active phone service by facility, cellular, or system-wide.	Y	
12	Real-time back up of all data, recordings, and information maintained for the life of the Agreement on an active system.	Y	

13	Excellent call clarity and reception to ensure quality recordings and monitoring of information.	Y	
14	Recorded record retention in alignment with a schedule mutually agreed upon by the Contractor and MDCR to allow for manual and scheduled off-line archiving of recorded phone calls.	Y	
15	System must be capable of sealing and expunging records in compliance with Court Orders.	N	
16	A periodic update of the Florida Bar Directory.	Y	
17	A leave behind system of all historical recorded calls, with a solution for all authorized investigators to remotely access the information wherever the system is located.	Y	
18	Telephone Module should follow a pre-determined schedule established by MDCR, generally from 8:00 a.m. to 12:00 midnight, from Sunday to Thursday, and 8a.m. to 2a.m., from Friday to Saturday. An exception exists on Holidays when access to telecommunication services may be extended and during other timeframes as granted by MDCR. The exception to this policy is when detainees is in lockdown or on disciplinary confinement.	Y	
19	All calls are timed out at 15 minutes. This will not change unless otherwise requested by MDCR.	Y	
20	The Telephone Module phone calls must be capable of being monitored, recorded, and archived, with the exception of privileged communication.	Y	

21	The recordings of Detainee conversations are considered the property of MDCR. These recordings shall be transferred onto a leave behind system.	Y	
22	The Contractor shall flag and archive all Unauthorized Call attempts (incoming and outgoing) and shall generate alert reports to be made available to the MDCR.	Y	
23	The Telephone Module shall provide the ability to selectively monitor call activity in real time and initiate appropriate action as necessary.	Y	
24	The Telephone Module shall retrieve and generate Detainee Unauthorized Call activity logs for specified periods.	Y	
25	Recording and storage of all friends and families calls and strict non-recording of any privileged calls.	Y	
26	Ability to save recordings and provide transcriptions of all friends and families calls in real time.	Y	
27	The Telephone Module shall be designed for use by the hearing impaired. Provisions for the deaf must comply with Americans with Disabilities Act (ADA) and Telephone Devices for the Deaf (TDD) regulations and standards. A minimum of two (2) TDD Detainee Telephone Instruments are required at each MDCR Department Custody and Detention Facility.	Y	
28	The Contractor's automated operator shall be capable of prompting a caller to select the appropriate language by pressing the appropriate keypad digit. The Contractor's automated operator shall be capable of supporting English, Spanish, and Haitian Creole or other languages required by the MDCR Department. The visual training aid to learn how to use the telephone module shall be provided written, verbal, and a video supporting English, Spanish, and Haitian Creole or other languages required by the MDCR Department.	Y	



35	<p>The Contractor's automated operator shall provide free and unlimited calls to the Detainee's private attorney or public defender. Such calls shall not be monitored or recorded by the Telephone Module. Prior to completing a connection, the Telephone Module shall compare the dialed number with a list of telephone numbers known to be private attorneys and/or public defenders. This list shall be compiled from the Florida Bar Association and approved by the MDCR Professional Compliance Division and be capable of being updated or modified frequently. If a number appears on this list, the Telephone Module must automatically disable monitoring and recording of that call.</p>	Y	
36	<p>All requests received by the Contractor from attorneys for inclusion on the list of non-recorded numbers shall be forwarded to the MDCR Professional Compliance Division. MDCR Professional Compliance Investigative Unit personnel will have the option to physically input approved attorney telephone numbers. This electronic listing shall be maintained by the Contractor's System in such a manner that record of any additions, edits, and deletions are archived and able to be queried and immediately retrieved upon request by the County. The master listing and archived records shall be accessible via specified System Administrative Workstations by the MDCR Project Director and MDCR Project Manager and designated administrative and/or specified MDCR Professional Compliance Investigative personnel.</p>	Y	
37	<p>The Contractor's automated operator shall provide for Collect Calls and Pre-Paid Calls, as permitted in accordance with procedures authorized by the MDCR Project Manager or designee. The call recipient shall have the option to refuse calls from the Detainee, either by blocking the call by keypad entry or by written notification to the MDCR Project Manager or designee indicating that they do not wish to receive calls from the Detainee. Requests to unblock any currently blocked numbers shall be processed in accordance with procedures authorized by the MDCR Project Manager or designee.</p>	Y	
38	<p>The Contractor's Telephone Module must have ability to build a timetable for Pro Se calls that are on flexible timetable, with the ability to add specific telephone numbers, and allow recorded or not recorded call selections, which can be created by MDCR Project Manager, and designated administrative and/or specified MDCR Professional Compliance Investigative personnel.</p>	Y	
39	<p>The Contractor's automated operator shall prevent all incoming calls to tablets and mobile/stationary kiosks in MDCR Detention Facilities. Any attempted incoming calls shall be rejected, and appropriate information (if available) shall be recorded, archived and reported to the County Project Manager or designee.</p>	Y	
40	<p>The Contractor's Telephone Module must have ability to build a pre-approved phone number list.</p>	Y	
41	<p>The Contractor's automated operator shall maintain a database containing blocked telephone numbers. The Telephone Module shall be capable of blocking calls by area code, prefix, or destination numbers. A master listing of blocked numbers shall be available for query/review at any time electronically on System Administrative Workstations provided under this Scope of Work.</p>	Y	

42	The Telephone Module shall also afford a means for the MDCR Project Manager, and the designees, including Professional Compliance investigative staff to block numbers (in real time) electronically and independently via designated System Administrative Workstations provided under this Scope of Work.	Y	
43	The MDCR Project Manager or designee may also notify the Contractor of the telephone number(s) the County wishes to be blocked. The Contractor shall block telephone number(s) when requested as soon as practical, but under no circumstances greater than eight (8) hours after the initial request.	Y	
44	The Contractor's automated operator shall employ appropriate security safeguards to detect, and block attempted three-way calls with a 99% reliability rate to include, pre-detection and warnings embedded in the call in English, Spanish, and Creole. Appropriate information regarding any detected possible three-way call attempts shall be recorded, archived, and the County Project Manager alerted for possible Delainee call monitoring, recording, or other corrective action. When applicable, the Contractor's automated operator shall be capable of System sensitivity modifications and shall be configurable to prevent attempts at three-way calls. Unauthorized calls, while simultaneously preserving legitimate calls and avoiding erroneous disconnects. Failure to achieve a mutually agreed upon successful detection rate will result in the imposition of financial penalties.	Y	
45	The Contractor's automated operator shall detect, and block attempted Delainee calls to unauthorized telephone numbers. Unauthorized numbers shall include but are not limited to the following: Public officials; government agencies; businesses; news media; numbers blocked by family members; and any other numbers, or blocks of numbers, identified by the County or ordered by a court of law. A master listing of unauthorized numbers shall be available for query/review/modification by County at any time electronically on System Administrative Workstations provided under this Scope of Work.	Y	
46	The Contractor's automated operator shall detect, and block attempted Collect Calls to restricted numbers. A master listing of restricted numbers shall be available for query/review/modification by the County at any time electronically on System Administrative Workstations provided under this Scope of Work.	Y	
47	The Contractor's automated operator shall employ appropriate security safeguards to detect, and block attempted call forwarding of Delainee calls. Appropriate information regarding any detected Delainee call forwarding attempts shall be recorded, archived, and the concerned County Project Manager alerted for possible Delainee call monitoring, recording, or other corrective action.	Y	
48	At regular intervals, the Contractor shall keep the MDCR Project Manager or designee apprised of current sensitivity settings, any success, and/or perceived or actual negative affect on calls as a result of current settings. Prior to any System modifications in this area, which could affect the County, the Contractor shall apprise and receive written approval from the County Project Manager or designee.	Y	

49	<p>Detainee telephone calls to a live operator are absolutely prohibited. The Contractor's Detainee telephone module shall be limited solely to the placing of automated operator assisted Collected Calls and Pre-Paid calls.</p>	Y	
50	<p>The Contractor's automated operator shall detect and block all other types of Detainee calls including but not limited to local operator calls (0), Information (411), Emergency Services (911), time (555-1212), businesses or special services numbers (such as 1-700, 1-800, 1-800, 1-888, 1-800 and 1-876 numbers). No numeric sequences associated with other call carriers for operator services (such as 1-999 numbers, or as otherwise specified in this document) are allowed.</p>	Y	
51	<p>The Contractor's automated operator shall detect and block Detainee long distance telephone call attempts to bypass the County's Detainee telephone services, utilizing numeric access codes to alternative calling plans provided by other long distance service vendors.</p>	Y	
52	<p>The Contractor's automated operator shall detect and block Detainee telephone calls to 1-0-XXX, 1-0-XXX, or any other similar numeric sequences intended to reach another long-distance carrier. The Contractor's automated operator shall detect and block commercially available debit/calling cards.</p>	Y	
53	<p>The Contractor's automated operator shall detect and block Detainee telephone calls intended to cause a public nuisance. The candidate list of telephone numbers likely to be targets of public nuisance calls will be provided by the MDCR Project Manager or designee as needed.</p>	Y	
54	<p>The complete list of unauthorized telephone numbers to be blocked will be developed jointly by County and Contractor's staff and updated as needed. The Contractor shall prepare and maintain the list of blocked telephone numbers and submit the list to the MDCR Project Director or designee for review and written approval. This listing shall be available for query/view/modification by County at any time electronically on specified System Administrative Workstations provided under this Scope of Work.</p>	Y	
55	<p>Appropriate information regarding any detected Detainee call attempts to unauthorized telephone numbers shall be recorded, archived, and the MDCR Project Manager or designee alerted for possible Detainee call monitoring, recording, or other corrective action.</p>	Y	
56	<p>Contractor's automated operator shall provide capability to monitor Detainee telephone calls at MDCR Custody and Detention Facilities.</p>	Y	

57	Contractor's automated operator shall provide the capability to monitor any Detainee Telephone Instrument and any Detainee telephone calls, via laptops utilizing Web access, or via System Administrative Workstations.	Y	
58	The Contractor shall provide remote access via Virtual Private Network (VPN) for laptop access, to all program features to monitor calls, for MDCR personnel explicitly authorized by the MDCR Project Manager or designee.	Y	
59	Administrative Workstation for MDCR staff, as specified by the MDCR Project Manager for the purpose of monitoring and recording Detainee phone calls. The requirements for the System Administrative Workstation are described further in this document.	Y	
60	The Contractor shall supply a means to identify call recipient information associated with the dialed telephone numbers (e.g., Hanes reverse directory). When the call recipient information is confidential as determined by the Contractor, the Contractor shall have no obligation to reveal the information without a court order.	Y	
61	Contractor's automated operator shall provide capability to record Detainee telephone calls at MDCR Custodial and Detention Facilities. The Telephone Module must be capable of recording one hundred percent (100%) of all Detainee telephone calls. Calls must be recorded in their entirety, up to the thirty (30) minutes time limit for Detainee calls. Recordings must be selectable by Telephone Instrument, group of Telephone Instruments, facility or called number.	Y	
62	The Telephone Module shall capture unauthorized activities. System Administrative Workstations provided under this Scope of Work shall be capable of reporting unauthorized Detainee calls.	Y	
63	The Contractor's automated operator shall provide capability to archive and immediately retrieve via VPN access, or from System Administrative Workstation all recorded Detainee telephone calls. Once recorded, the content of the call must be stored by the Contractor and be available for immediate retrieval via method determined by the MDCR Project Manager or designee for a period of up to three (3) years and at the discretion of the MDCR Project Manager or designee. The Telephone Module must have the capability to transfer the recorded calls to an offline media for archiving, or review. (NOTE: The Telephone Module must be capable of preventing recording of calls in certain sections of the facilities as it pertains to Pro-Se Detainee, as the calls of Pro-Se Detainee are not recorded.)	Y	

	All recorded telephone calls (files) shall be accompanied by the following data: <ul style="list-style-type: none"> <li>-Salutatory call branding information.</li> <li>-Date and time the telephone call was placed.</li> <li>-Location from which the telephone call was placed.</li> <li>-Telephone number that was dialed.</li> <li>-Duration of the telephone call.</li> <li>-Time that the telephone call was terminated.</li> <li>-PIN, if applicable.</li> </ul>			
64		Y		
65	The Contractor shall copy, save, and store off-line data for archived Detainee calls in the agreed upon media format and retrieval rate.	Y		
66	The Telephone Module must continue to record calls, without interruption, while copying and saving previously recorded calls. The recorded call file format shall be compatible with Microsoft Windows 10 based personal computer, or another format to be determined by the County.	Y		
67	The Telephone Module shall provide the capability of naming each file, or automatically generating a file name. Each recorded telephone call or any copies shall be securely encoded, in order to detect any attempted alterations to the recorded telephone call.	Y		
68	The Detainee Telephone Module provides a secure login procedure, which guards against fraudulent user. The Telephone Module possesses a feature in which established passwords auto-expire at a period determined by the County. Levels of permissions exist which allow the County Project Managers or designees the ability to create, edit, or view user accounts and assign permissions. The Telephone Module provides detailed explanation as to System Administrator, user, or other definable levels of access.	Y		
69	The Telephone Module provides a feature, which allows users to attach "notes" which provide additional documentation to Call Records. Notes are logged by the username, and date and time of entry. Notes are capable of being printed or updated.	Y		
70	The Telephone Module is capable of displaying historical user data including, but not limited to, a list of users who opened the same call recording, when users were granted access to the System and by whom.	Y		

71	The Telephone Module is capable of displaying data on copied files containing each user's information including, but not limited to, username, date and time of each copy.	Y	
72	The Telephone Module allows users to print, e-mail, or export the current page of a report and to export in various file formats (i.e., PDF, Excel, RTF, TXT, or TIF).	Y	
73	The Telephone Module is capable of displaying attempted and successful user logon transactions for each logon username and includes, but is not limited to, date and time of attempt of logon and activity.	Y	
74	The Telephone Module allows users to view the call activities of each Detainee telephone located within a particular facility and listen to calls in real time.	Y	
75	The Telephone Module allows users to lock recordings. Locked recordings are not deleted or unlocked without the approval of the appropriate authorized user. Users may only lock files if there is a recording associated with that call detail record.	Y	
76	The Telephone Module allows users to monitor calls through workstation computer speakers or by sending calls to a designated telephone number (e.g., cell phone, home phone, or office phone without an extension).	Y	
77	The Telephone Module allows authorized users to disconnect any Detainee call as it is being monitored, immediately and without warning to parties participating in the conversation. The System allows the County Project Managers, or designees, the capacity to turn off (and on) individual, specified group, or all Detainee telephones from any authorized workstation.	Y	
78	The Telephone Module provides a means by which authorized users can add numbers to a destination number list. Numbers may be added to this list for various reasons including, but not limited to blocking the number, adding privileged numbers, creating a calling schedule, selecting a number for no recording or creating an alert. Once a phone number is blocked, no Detainee telephone calls to that destination number will be allowed from any Detainee telephone.	Y	

79	The Telephone Module provides a thorough complement of search and sort features both investigative and administrative which includes, but is not limited to, played calls, recorded calls, completed calls, incomplete calls, copied or downloaded calls, calls with notes, note content, locked calls, call duration, manner in which call was initiated, manner in which call was terminated, type of call, three-way calls, and rate type.	Y	
80	The Telephone Module provides a report which tracks the total number of calls by both origination number (Detailee telephone) and call destination number (number dialed by the Detailee). Information in this report includes, but is not limited to, the origination number, location of the Detailee telephone within the facility, number of calls attempts from the Detailee telephone, number of accepts (calls accepted by the called party from this Detailee telephone), destination number (number dialed by the Detailee), the number of attempts to the destination number, and the number of accepted calls at the destination number.	Y	
81	The Telephone Module provides a report indicating activities associated with destination numbers placed on an alert list provided by the County. Calls to specified destination numbers are monitored each time they are dialed by a Detailee. This report contains call detail information including, but not be limited to, if call was recorded, if call had notes attached, if call was locked, facility, destination, dateline of alert, call length, cost of call and manner in which the call started and ended.	Y	
82	The Telephone Module provides a means which allows investigators to utilize "bookmarks" or "timeline markers" to tag a particular location, in time, within a recording for future reference and enter comments or notes within the bookmark. Bookmarks are not retained unless a voice-recording file is downloaded or saved.	Y	
83	The Telephone Module provides a security method for verifying authenticity of recordings. Completed Detailee calls stored for retrieval are protected from fraud and tampering throughout the storage term.	Y	
84	The Telephone Module provides a means of immediately alerting a collection of user-defined phone numbers attached to an individual or group with monitoring rights. Each time a Detailee places a call to a designated destination number, the Telephone Module begins dialing the specified contact phone numbers immediately, one by one, in the succession specified. If contact cannot be established (i.e., busy or unanswered) at a called number, the Telephone Module moves on to the next number, respectively, until contact is made with a member of the group, at which time the dialing may cease. If no contact is made after exhausting the list, the System repeats the list, in succession, until contact is made.	Y	
85	The Telephone Module provides a means for compressing "dead space" in recorded Detailee phone calls where no voice is detected, to be eliminated, leaving only the actual voice recordings in a compressed/uncompressed form. Such feature does not alter the Telephone Module capacity to retain the original file with security envelope.	Y	

86	Under no circumstance are privileged communications/phone calls be recorded. Contractor will conduct quarterly self-audits to ensure that no privilege communication is recorded and provide MDCR reports accordingly.	Y	
<b>Standard Package</b> Contractor shall provide a wide variety of standard content to keep Detainees occupied in meaningful and self-improving activities to help Detainees satisfy social and emotional needs. At a minimum, Contractor shall provide the following content and services to all Detainees at no charge to either the Detainee or the County.			
<b>A. Communication</b>			
<ul style="list-style-type: none"> <li>Ninety (90) minutes of phone calls per day</li> </ul>		Y	
<ul style="list-style-type: none"> <li>Two (2) hours of video visitation per week</li> </ul>		Y	
<ul style="list-style-type: none"> <li>Five (5) electronic messages per week</li> </ul>		Y	