



## Professional Services Agreement

This is an Agreement between Ramsey County, a political subdivision of the State of Minnesota, on behalf of Sheriff's Office, Sheriff's Office, Law Enforcement Center: 425 Grove Street, Saint Paul, MN 55101 ("County") and Network Communications International Corporation, 607 East Whaley Street, Longview, TX 75601, doing business as (DBA) NCIC Correctional Services, registered as a S Corporation in the State of Minnesota ("Contractor").

### 1. Term

#### 1.1.

The original term of this Agreement shall be from June 24, 2025 through June 23, 2027 and may be renewed for up to three (3) additional one year period(s).

The full term of this agreement (including renewals) is 5 year(s), 0 month(s) and 0 day(s).

#### 1.1.1.

Contract renewals shall be made by way of a written Amendment to the original contract and signed by authorized representatives.

### 2. Scope of Service

The County agrees to purchase, and the Contractor agrees to furnish, services described as follows:

#### 2.1.

The Contractor's Proposal response dated June 25, 2024 (the "Proposal") is incorporated by reference herein. The County's Request for Proposals RFP-SHRF-22703 entitled Inmate Communication Services dated May 8, 2024 (the "RFP") is incorporated by reference herein. The Contractor and the County shall mutually agree upon a kick-off meeting within a month from the execution of the Agreement on June 24, 2025. The Contractor shall conform to a ninety (90) day or less installation and system go-live.

#### A. GENERAL

The Contractor shall provide for all supplies, equipment, materials, labor, and services necessary or incidental for the installation, maintenance, repair, replacement, and operation of inmate phone calling services, video visitation services with the capability for both in-house and remote video visitation via the internet from a visitor's home or other off-site location, and tablet services. This includes Contractor provision of a secure, separate network, which is not part of the County managed network and/or internet for the System, which includes build, installation and

ongoing maintenance of the Contractor provided network and/or internet. In the event that the System hardware or software is removed, in whole or in part, during or at the completion of the contract term, the Contractor shall pay all expenses associated directly or indirectly with the removal of the System hardware and software.

#### **B. RAMSEY COUNTY SECURE TECHNOLOGY SOLUTIONS**

As a government entity Ramsey County has a responsibility to ensure safe and secure technology solutions. To accomplish this, we expect our Contractors to use industry best practices for security and compliance controls. Therefore, the Contractor shall:

- 1) Agree and represent that it currently maintains information data and content protection practices and procedures ("Security Program") that complies with industry best practice and applicable privacy laws.
- 2) Demonstrate compliance with industry best practice Critical Security Controls. Methods to demonstrate this are via an SSAE 18, SOC 2 report, externally certified report, etc. for your company and all sub-tier suppliers, as applicable.
- 3) Undergo an annual vulnerability assessment (internal and external) via an independent third party.
- 4) Demonstrate adherence to an industry standard continuous monitoring program which includes real time monitoring, logging, timely review and remediation of events. The monitoring program will support a defined incident management policies and procedures that is aligned with industry best practices.

The Contractor and the System shall comply with the *Ramsey County Secure Technology Solutions* that was submitted by Contractor as part of its proposal response to the County's Request for Proposals RFP-SHRF-22703 entitled Inmate Communication Services dated May 8, 2024.

#### **C. TECHNICAL QUESTIONNAIRE**

The Contractor and the System shall comply with the Ramsey County Technology Questionnaire that was submitted by Contractor as part of its proposal response to the County's Request for Proposals RFP-SHRF-22703 entitled Inmate Communication Services dated May 8, 2024.

#### **D. RAMSEY COUNTY SECURITY EXHIBITS**

The Contractor and the System shall comply with the *County's Hosting Security Exhibit* attached hereto and made a part of this Agreement as **Attachment A** and the *County's Information Security Exhibit* attached hereto and made a part of this Agreement as **Attachment B**.

#### **E. SYSTEM FEATURES**

The Contractor and the System shall conform to all of the mandatory and preferred features and system requirements set forth in the *Phone Calling System Requirements and Questionnaire* attached hereto and made a part of this Agreement as **Attachment C**, *Video Visitation System Requirements and Questionnaire*, attached hereto and made a part of this Agreement as **Attachment D** and *Tablet System Requirements and Questionnaire* attached hereto and made a part of this Agreement as **Attachment E**.

#### **F. PRICING INFORMATION**

The Contractor shall conform to the *Pricing Schedule* attached hereto and made a part of this Agreement as **Attachment F**.

Additionally, the Contractor understands and agrees to the following:

- 1) Services for on-site video visitation (general, legal, and others) shall be provided at no cost.
- 2) Off-site video visitation for legal visitation with the Courts and the Public Defender's Office shall be provided at no cost. Cost for all other attorneys and professional services is established in the *Pricing Schedule*.
- 3) Contractor shall be required to handle all financial transactions from the utilization of off-site video visitation services and report all financial data to the County. County personnel shall also have access to reports.

The Contractor shall communicate all cost information in an open and transparent manner at all times.

#### **G. PROJECT SERVICES**

##### **1) Project Management**

The Contractor shall implement the System in phases, where necessary, using a traditional project management approach. The Contractor shall provide project management services throughout the entire Project consistent with project management best practices, to ensure that the Project's goal is met and that deliverables are submitted and approved within the defined budget and timeline.

##### **2) Documentation**

All documents including project plans, phase documentation, training materials and System documentation delivered to the County shall be provided in Microsoft Office formats; native formats where applicable and acceptable by the County. Copies may be printed by the County for its own internal use.

##### **3) Project Phases**

###### **Phase I – Planning**

Within a mutually-agreed to time period after execution of the Agreement with the County, the Contractor will organize and hold a Kick-Off Meeting, provide a high-level Project Schedule / Work Plan with key tasks, dates, milestones, deliverable

descriptions and Contractor and County staffing requirements that are necessary to ensure a successful “go live” date.

Deliverables: Kick-Off Meeting, Project Schedule/Work Plan.

#### Phase II – Design

Design documents should consist of a Fit/Gap Analysis that describes any development or configuration that is needed to meet the requirements of the Agreement as well as an Interface / Integration Plan and a Data Conversion / Migration plan.

Deliverables: Design documents that consist of a Fit / Gap Analysis that identify any development or configuration needed to the System, Interface/Integration Plan, and a Data Conversion / Migration plan.

#### Phase III – Development

This Phase shall cover configuration, customization (if required) and development of the System. During this Phase the Contractor shall develop all modifications from Phase II – Design and create all documentation listed below. Deliverables: A fully developed and configured System ready for testing, test plan, training plan, implementation plan, operations and maintenance transition plan, system functionality documentation, and converted legacy data. All deliverables identified herein shall be delivered to the department prior to System testing.

#### Phase IV - System Testing and Acceptance

1) Upon determination by the Contractor that the System has been successfully installed in a test environment and all environments perform in accordance with the provisions of the Agreement, including the System documentation, the County shall commence a mutually agreed to System Testing and Acceptance period (“Testing Period”).

2) The County will notify the Contractor of any defects or deficiencies identified during the Testing Period and the Contractor will correct the defects and deficiencies or present a plan acceptable to the County that addresses the deficiencies in a time period agreed to by the parties.

3) Upon resolution of all defects and deficiencies identified during the Testing Period, completion of training, and receipt of training and System materials and documentation, the County will provide written System Acceptance to the Contractor.

Deliverables: User Acceptance Test (usually completed by the County) completely developed and configured System installed in a Test Environment; Testing Defect Report with all defects showing fixed, passed and accepted by the County; updates to System Functionality and Training documentation; fully migrated, tested and accepted legacy system data.

#### Phase V – Training

After the Contractor certifies that the System is ready for use in a Production Environment and prior to “go live”, the Contractor shall provide County approved training both for system administrators and end users, approximately one hundred (165) in total. All training courses provided by the Contractor will be taught by experienced trainers. Training materials will be delivered to County before training begins. Training will be conducted by the Contractor. A Web-based environment will be provided for ongoing training for all licensed / administrative users.

The Contractor shall provide on-site “train the trainer” training sessions for managers on the use of the System. This training will at minimum include creating and managing accounts, managing/recording/downloading content, and other related topics as requested by the County.

The Contractor shall provide ongoing training in the event of a significant software or hardware update as deemed necessary by the County. This will be at no cost to the County.

Deliverables: System administrator training, end user training, train the trainer training, online assistance along with training manuals.

#### Phase VI – Deployment

Upon receipt of County’s System Acceptance and upon completion of training and all other pre- deployment services, the Contractor will fully deploy the System in a production environment.

Deliverables: Successful deployment of the System in the production environment.

#### 4) Deliverable Acceptance Process

All Deliverables identified in the resulting agreement will be subject to the following Deliverables Acceptance Process:

a) When a Deliverable is submitted for review and acceptance, the County has ten (10) business days or a mutually agreed upon period to review the Deliverable and provide written notice to the Contractor of acceptance or of any defects or deficiencies in the Deliverable. The County may reject a Deliverable that does not meet the requirements of the Agreement. Written acceptance will be provided to the Contractor in the form of a *Notice of Acceptance* (“NOA”), a sample of which was attached to the RFP. The Contractor shall have a period of ten (10) business days to correct the deficiency. If the Contractor fails to correct the deficiency within the time period, the County may treat the failure as “cause” for termination of the Agreement.

b) Partial or incomplete Deliverables submitted for review will not be considered by the County unless the partial or incomplete submission has been requested by the County.

5) County Ownership

All right, title and interest to the System Deliverables created by Contractor under the Agreement shall be owned by the County. Deliverables under the Project Services include but are not limited to: Project Documentation, Project Schedule/Work Plan, Interface/Integration Plan, System Test Plan, Training Plan, Implementation Plan, Operations & Maintenance Transition Plan, User Acceptance Test, System Documentation, County Training Plan and County Training Materials.

**H. POST-DEPLOYMENT TRAINING**

The Contractor shall make available annual refresher training and shall provide the County updated training materials whenever revised.

**I. WARRANTY**

1) The County requires a warranty beginning upon final deployment and System Acceptance that the System will operate in accordance with the provisions of the Agreement and the System documentation. Warranty services shall be consistent with the requirements described in **Section K. Support**.

2) The Contractor must warrant that all warranty services shall be performed by qualified personnel with that degree of skill and judgment normally exercised by recognized professional firms performing the same or substantially similar services and that the Contractor will devote adequate resources to meet its obligations under the Agreement.

3) Contractor acknowledges that time is of the essence with respect to Contractor's obligations under the Agreement and must agree that prompt and timely performance of all services and other Contractor obligations in accordance with the Agreement is strictly required.

4) During the term of the Agreement, the Contractor warrants that all services will be performed with the highest standard of professional service, that all Deliverables will be free from defects or deficiencies, and that services and Deliverables will conform to all requirements of the Agreement. Nonconforming goods or services will be replaced, corrected or re-performed at the Contractor's expense. Any services corrected or re-performed or Deliverables corrected will be covered by this warranty.

5) The Contractor must warrant that its System will not infringe any United States patent or copyright or violate any third-party trade secret and Contractor will indemnify and defend Ramsey County against any award of damage and costs made against the Contractor by a final judgment of a court of competent jurisdiction.

6) The Contractor must warrant that as provided by Contractor, the System will not at any time during term of the Agreement contain any: (a) virus, Trojan horse, worm, backdoor or other software or hardware devices that effect of which is to permit unauthorized access to, or to disable, erase, or otherwise harm, any computer, systems or software; or (b) time bomb, drop dead device, or other software or hardware device designed to disable a computer automatically with the passage of

time or under the control of any individual or organization, or otherwise deprive the County of its lawful right to use the System.

7) The Contractor must warrant that the System will be operational and available 99.5% of the time in any calendar month, including planned downtime, following System Acceptance. Contractors must agree to a service level credit for less than 99.5% availability, which will be specified and agreed to during contract negotiations and included in the Agreement. The County will also have the right to terminate services, without penalty and include the right for the County to recover costs from the Contractor associated with re-procurement of such terminated services.

#### **J. MAINTENANCE SERVICES**

1) The Contractor will provide all services, materials, equipment and personnel to maintain its system components that are located off-site, including all software and hardware, in full operating condition and keep it available for use in accordance with the provisions of the Agreement.

2) Routine System maintenance shall be conducted at times agreed to in advance by both parties and shall include but not be limited to periodic inspections, tests and adjustments. Contractor shall provide the County with a minimum of forty-eight (48) hour notice for non-service impacting maintenance. Contractor shall provide a minimum seven (7) days' notice for planned maintenance which will impact the County's availability to the System.

3) Software releases, updates and upgrades shall be provided on the general release of such releases, updates and upgrades and installed by the Contractor as agreed to by the parties at no additional charge. Contractor must warrant that no release, update or upgrade will have a material adverse effect on the functionality or operability of the System.

#### **K. SUPPORT**

1) The Contractor shall conform to the *Service Level Agreement* attached hereto and made a part of this Agreement as **Exhibit 4**.

2) The Contractor must provide support staff contact information, hours of operations and after hours support procedures. Such information must be published and be kept current.

3) The Contractor will not change its software support and hardware maintenance policies to adversely impact the County without providing the County at least twelve (12) months advance written notice.

4) The County reserves the right to require the Contractor to escrow its software source code at no cost to the County.

#### System failures are defined as:

5) Critical issues are issues that affect the functionality or critical data of the system that do not have a work-around and prevent the county from conducting business

practices. This is to include loss of connection to the contract network, facility wide outage to the video visiting kiosk, loss of ability to schedule, and collection of applicable rates and fees.

Non-critical issues affect minor functionality of system and have an easy work-around.

6) The Contractor shall provide a method to resolve critical system failures remotely within one (1) hour or employ a technician that can arrive at the facility within four (4) hours from the time the initial call or email to technical support is made.

7) The technical support solution offered by the Contractor must be approved by the Adult Detention Center administrator or designee. Should the solution offered by the Contractor be deemed unacceptable to the ADC administrator or designee, the Contractor must find another solution that is acceptable to the Adult Detention Center administrator or designee. Failure of the Contractor to find an acceptable solution to a technical problem may be cause for termination of the contract.

8) Any temporary solution shall not be used for more than forty-eight (48) consecutive hours unless approved by the Adult Detention Center administrator or designee.

9) Routine System maintenance shall be conducted at times agreed to in advance by the parties and shall include but not be limited to periodic inspections, tests and adjustments.

10) Failure by the Contractor to respond and resolve technical issues promptly and completely to the satisfaction of the County may be cause for termination of the Agreement.

#### **L. BACKGROUND CHECKS**

The Contractor shall comply with the following screening and security requirements:

1) All Contractor employees working on-site at the Adult Detention Center shall successfully pass a background check before first entering the facility. The background check will be conducted by and at the expense of the Ramsey County Sheriff's Office. Failure to comply may result in immediate termination of the Agreement. Any subcontractors, if authorized by the Sheriff's Office administrators or designee, must also pass a background check as described.

2) The Sheriff's Office administrator or designee shall have the sole right, at any time, to reject any such employee who it determines in its sole discretion poses a risk or potential risk to the security or operations of the Adult Detention Center.

3) All Contractor employees shall complete an orientation as defined by the Sheriff's Office administrator or designee. The Contractor and its employees will comply with all rules and regulations, policies and procedures, as well as any directives and/or orders by the Sheriff's Office administrators and staff. Any Contractor employee or subcontractor failing to comply with the aforementioned rules, regulations, policies,



procedures, or directives may be escorted from the building and such action may be cause for termination of the Agreement.

**M. QUALITY CONTROL**

The Contractor shall comply with the following requirements to ensure quality goods and services are provided to the County:

- 1) The Contractor shall meet monthly in-person or via conference call with the Adult Detention Center administrator or designee to discuss the quality of service and to ensure that the Contractor is meeting their contractual obligations.
- 2) The Contractor shall meet monthly for no less than the first six (6) months of the contract and may be adjusted to quarterly meetings after the six (6) months at the discretion of the Adult Detention Center administrator or designee.
- 3) Failure of the Contractor to participate in these meetings may be cause for termination of the Agreement.

**N. REPORTS**

- 1) The Contractor shall provide or make accessible reports to the County of revenue, fees, usage, and commission.
- 2) The County reserves the right to request additional reports as needed.

**O. CONTRACT MANAGEMENT**

The following contacts are the point of contact for contract management:

**County:**

Megan Schaefer, Planning Manager  
Ramsey County Sheriff's Office  
Law Enforcement Center  
425 Grove Street  
Saint Paul, Minnesota 55101  
Office: 651-266-9374  
Mobile: 651-775-6469  
Email: megan.schaefer@co.ramsey.mn.us

**Contractor:**

Scott Baniecke, Midwest Sales Director  
Office: 903-757-4455  
Mobile: 651-425-1601  
Email: scott.baniecke@ncic.com

Craig Storer, Director of Marketing  
Mobile: 903-699-2505  
Email: craig.storer@ncic.com

**2.2.**

During the term of the contract, the County reserves the right to add similar in scope goods/services, via written amendment, to accommodate accidental omissions, unanticipated needs, or new offerings.

**2.3.**

The Contractor shall make every reasonable effort to provide services in a universally accessible, multi-cultural and/or multi-lingual manner to persons of diverse populations.

**2.4.**

The Contractor agrees to furnish the County with additional programmatic and financial information it reasonably requires for effective monitoring of services. Such information shall be furnished within a reasonable period, set by the County, upon request.

**3. Schedule**

The Contractor shall provide services as and if requested by the County, it being understood that the County might not purchase any services under this Agreement.

**4. Cost**

**4.1.**

The County shall pay the Contractor the following unit rates:

The County and the Contractor shall conform to the *Pricing Schedule* attached hereto and made a part of this Agreement as **Attachment F**.

**Modifications to Equipment Counts**

Upon execution of this Agreement and throughout the original term and any renewal options, the County and the Contractor agree to review the phone calling, video visitation, and tablet services equipment on a quarterly basis in order to add, delete, or modify the equipment counts.

**Post Award Pricing**

Subject to rules and regulations that may be modified from time to time by governing authorities such as the FCC, pricing will not change during the first twelve (12) months after the commencement date of the Agreement. After the initial twelve (12) months, and annually thereafter on the anniversary of the Agreement a price change request may be submitted to the County. All price change requests must be submitted in writing to the County forty-five (45) days prior to the date the requested changes will take effect and must be accompanied by appropriately documented market justification. Price changes will only be granted with written approval from the County. Any adjustments must be negotiated on an annual basis between the Contractor and the Adult Detention Center administrator or designee.

### **Usage by Other Ramsey County Departments**

Other Ramsey County departments utilizing this Agreement shall designate a point of contact for the County for each Purchase Order and/or Statement of Work, with responsibilities, but not limited to invoicing, providing any necessary information, handling communications between the County and the Contractor for the Purchase Order/Statement of Work. Other Ramsey County departments will be responsible for receiving a quote from the Contractor for their project to ensure existing rates are used.

## **5. Special Conditions**

### **5.1.**

The Contractor will be authorized to subcontract the installation and removal of the existing equipment. Additionally, at the completion of the life cycle of the contract, the Contractor will also be authorized to subcontract for the removal of all related equipment. All use of subcontractors during the installation and removal process must be approved by the facility administrator or designee.

### **5.2** The order of Governance regarding the Terms and Conditions shall be:

- 1) Ramsey County Professional Services Agreement RC-000660
- 2) Attachment A – Hosting and/or Cloud Services and Security Standards
- 3) Attachment B – County’s Information Security Exhibit
- 4) Exhibit 1 – Business Associate Agreement
- 5) Exhibit 2 - CJIS Security Addendum
- 6) Exhibit 3 – CJIS Security Addendum Certification
- 7) The County’s Request for Proposals RFP-SHRF-22703 entitled Inmate Communication Services dated May 8, 2024
- 8) The Contractor’s Proposal response dated June 25, 2024
- 9) Exhibit 4 –Service Level Agreement

## **6. County Roles and Responsibilities**

The County shall provide a staff member(s) who will serve as the contact for project management. Access to County subject matter experts will be provided as determined necessary by the County.

## **7. Contracting for Equity**

### **7.1. Commitment to Advancing Racial Equity**

The county is committed to advancing racial equity for its residents. The commitment is captured in the county's Advancing Racial Equity policy which states that "Racial equity is achieved when race can no longer be used to predict life outcomes, and outcomes for all are improved."

Consistent with the Advancing Racial Equity policy, contractors will take all reasonable measures to advance racial equity during contract performance. Contractors will recognize and acknowledge this requires deconstructing barriers and changing systems, structures, policies and procedures. Contractors will be equitable, inclusive, transparent, respectful and impactful in serving and engaging residents. Contractors will have meaningful and authentic engagement with community and employees to strengthen the administration, development and implementation of policies and procedures to advance racial equity and ensure that all residents in need have awareness of and access to contracted services.

Please review Ramsey County's [Advancing Racial Equity policy](#) to learn more about Ramsey County's commitment to racial equity.

## **7.2. Non-Discrimination (In accordance with Minn. Stat. § 181.59)**

Contractors will comply with the provisions of Minn. Stat. § 181.59 which require:

*"Every contract for or on behalf of the state of Minnesota, or any county, city, town, township, school, school district, or any other district in the state, for materials, supplies, or construction shall contain provisions by which the contractor agrees:*

*(1) that, in the hiring of common or skilled labor for the performance of any work under any contract, or any subcontract, no contractor, material supplier, or vendor, shall, by reason of race, creed, or color, discriminate against the person or persons who are citizens of the United States or resident aliens who are qualified and available to perform the work to which the employment relates;*

*(2) that no contractor, material supplier, or vendor, shall, in any manner, discriminate against, or intimidate, or prevent the employment of any person or persons identified in clause (1) of this section, or on being hired, prevent, or conspire to prevent, the person or persons from the performance of work under any contract on account of race, creed, or color;*

*(3) that a violation of this section is a misdemeanor; and*

*(4) that this contract may be canceled or terminated by the state, county, city, town, school board, or any other person authorized to grant the contracts for employment, and all money due, or to become due under the contract, may be forfeited for a second or any subsequent violation of the terms or conditions of this contract."*

## **7.3. Equal Employment Opportunity and Civil Rights**

### **7.3.1.**

Contractors agree that no person shall, on the grounds of race, color, religion, age, sex, sexual orientation, disability, marital status, public assistance status, criminal record (subject to the exceptions contained in Minn. Stat. §§299C.67 to 299C.71 and Minn. Stat. §144.057), creed or national origin, be excluded from full employment rights in, participation in, be denied the benefits of, or be

otherwise subjected to discrimination under any program, service, or activity under the provisions of any and all applicable federal and state laws against discrimination, including the Civil Rights Act of 1964. Contractors will furnish all information and reports required by the county or by Executive Order No. 11246 as amended, and by the rules and regulations and orders of the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations and orders.

**7.3.2.**

Contractors shall comply with any applicable licensing requirements of the Minnesota Department of Human Services in employment of personnel.

**7.3.3.**

Contractors shall agree that no qualified individual with a disability as defined by the Americans with Disabilities Act, 42 U.S.C. §§12101-12213 or qualified handicapped person, as defined by United States Department of Health and Human Services regulations, Title 45 Part 84.3 (j) and (k) which implements Section 504 of the Rehabilitation Act of 1973, 29 U.S.C. §794, under Executive Order No. 11914 (41FR17871, April 28, 1976) shall be:

**7.3.3.1.**

Denied access to or opportunity to participate in or receive benefits from any service offered by contractors under the terms and provisions of this agreement; nor

**7.3.3.2.**

Subject to discrimination in employment under any program or activity related to the services provided by contractors.

**7.3.3.3.**

If it is discovered that a contractor is not in compliance with applicable regulations as warranted, or if the contractor engages in any discriminatory practices, as described above, then the county may cancel said agreement as provided by the cancellation clause of this agreement.

**7.4. Diverse Workforce Inclusion Resources**

For information and assistance in increasing the participation of women and minorities, contractors are encouraged to access the websites below:

1. <http://www.ramseycounty.us/jobconnect>
2. <http://www.ramseycounty.us/constructionconnect>

Job Connect and the Construction Connect provide a recruiting source for employers and contractors to post job openings and source diverse candidates.

Ramsey County's Job Connect links job seekers, employers and workforce professionals together through our website, networking events and community outreach. The network includes over 10,000 subscribed job seekers ranging from

entry-level to highly skilled and experienced professionals across a broad spectrum of industries.

Employers participate in the network by posting open jobs, meeting with workforce professionals and attending hiring events. Over 200 Twin Cities community agencies, all working with job seekers, participate in the network.

Ramsey County's Construction Connect is an online and in-person network dedicated to the construction industry. Construction Connect connects contractors and job seekers with employment opportunities, community resources and skills training related to the construction industry. Construction Connect is a tool for contractors to help meet diversity hiring goals. Additional assistance is available through [askworkforcesolutions@ramseycounty.us](mailto:askworkforcesolutions@ramseycounty.us) or by calling 651-266-9890.

## **8. General Contract/Agreement Terms and Conditions**

### **8.1. Payment**

#### **8.1.1.**

No payment will be made until the invoice has been approved by the County.

#### **8.1.2.**

Payments shall be made when the materials/services have been received in accordance with the provisions of the resulting contract.

### **8.2. Application for Payments**

#### **8.2.1.**

The Contractor shall submit an invoice monthly upon completion of services..

#### **8.2.2.**

Invoices for any goods or services not identified in this Agreement will be disallowed.

#### **8.2.3.**

Each application for payment shall contain the order/contract number, an itemized list of goods or services furnished and dates of services provided, cost per item or service, and total invoice amount.

#### **8.2.4.**

Payment shall be made within thirty-five (35) calendar days after the date of receipt of a detailed invoice and verification of the charges. At no time will cumulative payments to the Contractor exceed the percentage of project completion, as determined by the County.

**8.2.5.**

Payment of interest and disputes regarding payment shall be governed by the provisions of Minnesota Statutes §471.425.

**8.2.6.**

The Contractor shall pay any subcontractor within ten days of the Contractor's receipt of payment from the County for undisputed services provided by the subcontractor. The Contractor shall pay interest of 1 1/2 percent per month or any part of a month to the subcontractor on any undisputed amount not paid on time to the subcontractor. The minimum monthly interest penalty payment for an unpaid balance of \$100.00 or more is \$10.00. For an unpaid balance of less than \$100.00, the Contractor shall pay the actual penalty due to the subcontractor. A subcontractor who prevails in a civil action to collect interest penalties from the Contractor must be awarded its costs and disbursements, including attorney's fees, incurred in bringing the action.

**8.3. Independent Contractor**

The Contractor is and shall remain an independent contractor throughout the term of this Agreement and nothing herein is intended to create, or shall be construed as creating, the relationship of partners or joint ventures between the parties or as constituting the Contractor as an employee of the County.

**8.4. Successors, Subcontracting and Assignment**

**8.4.1.**

The Contractor binds itself, its partners, successors, assigns and legal representatives to the County in respect to all covenants and obligations contained in this Agreement.

**8.4.2.**

The Contractor shall not assign or transfer any interest in this Agreement without prior written approval of the County and subject to such conditions and provisions as the County may deem necessary.

**8.4.3.**

The Contractor shall not enter into any subcontract for performance of any services under this Agreement without the prior written approval of the County. The Contractor shall be responsible for the performance of all subcontractors.

**8.5. Compliance With Legal Requirements**

**8.5.1.**

The Contractor shall comply with all applicable federal, state and local laws and the rules and regulations of any regulatory body acting thereunder and all licenses, certifications and other requirements necessary for the execution and completion of the contract.

**8.5.2.**

Unless otherwise provided in the agreement, the Contractor, at its own expense, shall secure and pay for all permits, fees, charges, duties, licenses, certifications, inspections, and other requirements and approvals necessary for the execution and completion of the contract, including registration to do business in Minnesota with the Secretary of State's Office.

**8.6. Data Practices**

**8.6.1.**

All data collected, created, received, maintained or disseminated for any purpose in the course of the Contractor's performance under this Agreement is subject to the provisions of the Minnesota Government Data Practices Act, Minn. Stat. Ch. 13, any other applicable state statutes, any state rules adopted to implement the Act and statutes, as well as federal statutes and regulations on data privacy.

**8.6.2.**

The Contractor designates William Pope as its Responsible Designee, pursuant to the Minnesota Government Data Practices Act, Minnesota Statutes Chapter 13.02 Subdivision 6, as the individual responsible for any set of data collected to be maintained by Contractor in the execution of this Agreement.

**8.6.3.**

The Contractor shall take all reasonable measures to secure the computers or any other storage devices in which County data is contained or which are used to access County data in the course of providing services under this Agreement. Access to County data shall be limited to those persons with a need to know for the provision of services by the Contractor. Except where client services or construction are provided, at the end of the Project all County data will be purged from the Contractor's computers and storage devices used for the Project and the Contractor shall give the County written verification that the data has been purged.

**8.7. Security**

**8.7.1.**

The Contractor is required to comply with all applicable Ramsey County Information Services Security Policies ("Policies"), as published by Information Services Information Security. The Policies are posted at <https://www.ramseycounty.us/businesses/doing-business-ramsey-county/contracts-vendors/information-security-policies-vendors>.

**8.7.2.**

Contractors shall report to Ramsey County any privacy or security incident regarding the information of which it becomes aware. "Security Incident"



means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with System operations in an information system. "Privacy incident" means violation of the Minnesota Government Data Practices Act (MGDPA) and/or the HIPAA Privacy Rule (45 C.F.R. Part 164, Subpart E), including, but not limited to, improper and/or unauthorized use or disclosure of protected information, and incidents in which the confidentiality of the information maintained by it has been breached. This report must be in writing and sent to the County not more than 7 days after learning of such non-permitted use or disclosure. Such a report will at least: (1) Identify the nature of the non-permitted use or disclosure; (2) Identify the data used or disclosed; (3) Identify who made the non-permitted use or disclosure and who received the non-permitted or violating disclosure; (4) Identify what corrective action was taken or will be taken to prevent further non-permitted uses or disclosures; (5) Identify what was done or will be done to mitigate any deleterious effect of the non-permitted use or disclosure; and (6) Provide such other information, including any written documentation, as the County may reasonably request. The Contractor is responsible for notifying all affected individuals whose sensitive data may have been compromised as a result of the Security or Privacy incident.

**8.7.3.**

Contractors must ensure that any agents (including contractors and subcontractors), analysts, and others to whom it provides protected information, agree in writing to be bound by the same restrictions and conditions that apply to it with respect to such information.

**8.7.4.**

The County retains the right to inspect and review the Contractor's operations for potential risks to County operations or data. The review may include a review of the physical site, technical vulnerabilities testing, and an inspection of documentation such as security test results, IT audits, and disaster recovery plans.

**8.7.5.**

All County data and intellectual property stored in the Contractor's system is the exclusive property of the County.

**8.8. Payment Card Industry (PCI) Compliance**

**8.8.1.**

All Point of Interaction (POI) devices must meet the Payment Card Industry (PCI) PIN Transaction Security (PTS) requirements and be included in the PCI PIN transaction devices list. In order for these devices to transmit cardholder data on the Ramsey County network these devices must meet the PCI Point-To-Point Encryption (P2PE) standards.

## **8.9. HIPAA Compliance**

### **8.9.1.**

The Contractor agrees to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA, public law #104-191) and its amendments. The Contractor also agrees to comply with the HIPAA Privacy requirements, the HIPAA Standards for Electronic Transactions, the HIPAA Security requirements, the HIPAA Enforcement Rule, the HIPAA Breach Notification requirements, and any other applicable HIPAA laws, standards and requirements now or as they become law, including any future guidance issued by the Secretary of Health and Human Services.

### **8.9.2.**

Because the Contractor's function or service, described in Section I, Scope of Services, will involve the disclosure of Protected Health Information (PHI) by the County, or the creation, use or disclosure of PHI by the Contractor on behalf of the County, the County (Covered Entity) is required to enter into a separate Business Associate Agreement (BAA) with the Contractor (Business Associate). The BAA ensures that the Contractor's performance under this contract (the Covered Agreement) complies with the privacy and security requirements under HIPAA and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH ACT). Consequently, the Contractor agrees to the terms and conditions of the BAA, attached hereto and incorporated herein by reference as Exhibit 1, and the parties further agree that the electronic approval of this contract also constitutes approval of the BAA.

## **8.10. Indemnification**

The Contractor shall indemnify, hold harmless and defend the County, its officials, agents, and employees against any and all liability, losses, costs, damages, expenses, claims or actions, including reasonable attorney's fees, which the County, its officials, agents, or employees may hereafter sustain, incur or be required to pay, arising out of or by reason of any act or omission of the Contractor, or its subcontractors, and their officers, agents or employees, in the execution, performance, or failure to adequately perform the Contractor's obligations pursuant to this Agreement.

## **8.11. Prison Rape Elimination Act (PREA)**

Contractor and staff will comply with the Prison Rape Elimination Act of 2003 (42 U.S.C. § 15601 *et seq.*), which establishes a zero-tolerance standard against sexual assault, and with all applicable PREA Standards including background checks, county policies related to PREA and county standards related to PREA for preventing, detecting, monitoring, investigating, and eradicating any form of sexual abuse with Facilities/Client Services owned, operated or contracted. Contractor acknowledges that, in addition to "self-monitoring requirements" the county will conduct announced or unannounced, compliance monitoring to include "on-site" monitoring. Failure to comply with PREA, including PREA Standards and county PREA policies may result in termination of the Agreement.

## **8.12. Contractor's Insurance**

### **8.12.1.**

The Contractor shall purchase and maintain such insurance as will protect the Contractor from claims which may arise out of, or result from, the Contractor's operations under this Agreement, whether such operations are by the Contractor or by any subcontractor, or by anyone directly employed by them, or by anyone for whose acts or omissions anyone of them may be liable.

### **8.12.2.**

Throughout the term of this Agreement, the Contractor shall secure the following coverages and comply with all provisions noted. Certificates of Insurance shall be issued to the County contracting department evidencing such coverage to the County throughout the term of this Agreement.

### **8.12.3.**

Commercial general liability of no less than \$1,000,000 per occurrence, \$2,000,000 general aggregate, \$2,000,000 products/completed operations total limit, \$1,000,000 personal injury and advertising liability.

#### **8.12.3.1.**

All policies shall be written on an occurrence basis using ISO form CG 00 01 or its equivalent. Coverage shall include contractual liability and XCU. Contractor will be required to provide proof of completed operations coverage for 3 years after substantial completion.

### **8.12.4. Workers' Compensation**

Contractor certifies it is in compliance with Minnesota Statutes Ch. 176 (Workers' Compensation). The Contractor's employees, subcontractors and agents will not be considered County employees. Contractor must provide Workers' Compensation insurance for all its employees and, in case any work is subcontracted, Contractor will require the subcontractor to provide Workers' Compensation insurance in accordance with the statutory requirements of the State of Minnesota.

Required minimum limits of \$500,000/\$500,000/\$500,000. Any claims that may arise under Minnesota Statutes Ch. 176 on behalf of these employees, subcontractors or agents and any claims made by any third party as a consequence of any act or omission on the part of these employees, subcontractors or agents are in no way the County's obligation or responsibility.

If Minnesota Statute 176.041 exempts Contractor from Workers' Compensation insurance or if the Contractor has no employees in the State of Minnesota, Contractor must provide a written statement, signed by an authorized representative, indicating the qualifying exemption that excludes Contractor from the Minnesota Workers' Compensation requirements. If during the course of the contract the Contractor becomes eligible for Workers' Compensation, the

Contractor must comply with the Workers' Compensation Insurance requirements herein and provide the County with a certificate of insurance.

**8.12.5. Cyber Liability**

Contractor shall obtain and maintain Network Security and Privacy Liability Insurance, including first-party and third-party costs, for any privacy breach or security failure arising out of Contractor's performance of its services under this Contract that compromises Ramsey County data.

\$2,000,000 – per occurrence  
\$5,000,000 – annual aggregate

If the policy is claims-made, the retroactive/prior acts date of such coverage shall be prior to the effective date of this Contract and Contractor shall maintain such insurance for a period of at least three (3) years following completion of the work.

**8.12.6.**

An umbrella or excess liability policy over primary liability insurance coverages is an acceptable method to provide the required commercial general liability and employer's liability insurance amounts. If provided to meet coverage requirements, the umbrella or excess liability policy must follow form of underlying coverages and be so noted on the required Certificate(s) of Insurance.

**8.12.7.**

The Contractor is required to add Ramsey County, its officials, employees, volunteers and agents as Additional Insured to the Contractor's Commercial General Liability, Auto Liability, Pollution and Umbrella policies with respect to liabilities caused in whole or part by Contractor's acts or omissions, or the acts or omissions of those acting on Contractor's behalf in the performance of the ongoing operations, services and completed operations of the Contractor under this Agreement. The coverage shall be primary and non-contributory.

**8.12.8.**

If the contractor is driving on behalf of the County but not transporting clients as part of the contractor's services under this contract, a minimum of \$500,000 combined single limit auto liability, including hired, owned and non-owned.

**8.12.9.**

The Contractor waives all rights against Ramsey County, its officials, employees, volunteers or agents for recovery of damages to the extent these damages are covered by the general liability, worker's compensation, and employers liability, automobile liability, professional liability and umbrella liability insurance required of the Contractor under this Agreement.

**8.12.10.**

These are minimum insurance requirements. It is the sole responsibility of the Contractor to determine the need for and to procure additional insurance which may be needed in connection with this Agreement. Copies of policies and/or certificates of insurance shall be submitted to the County upon written request and within 10 business days.

**8.12.11.**

Certificates shall specifically indicate if the policy is written with an admitted or non-admitted carrier. Best's Rating for the insurer shall be noted on the Certificate, and shall not be less than an A-.

**8.12.12.**

The Contractor shall not commence work until it has obtained the required insurance and if required by this Agreement, provided an acceptable Certificate of Insurance to the County.

**8.12.13.**

All Certificates of Insurance shall provide that the insurer give the County prior written notice of cancellation or non-renewal of the policy as required by the policy provisions of Minn. Stat. Ch. 60A, as applicable. Further, all Certificates of Insurance to evidence that insurer will provide at least ten (10) days written notice to County for cancellation due to non-payment of premium.

**8.12.14.**

Nothing in this Agreement shall constitute a waiver by the County of any statutory or common law immunities, defenses, limits, or exceptions on liability.

**8.13.Audit**

Until the expiration of six years after the furnishing of services pursuant to this Agreement, the Contractor, upon request, shall make available to the County, the State Auditor, or the County's ultimate funding source, a copy of the Agreement, and the books, documents, records, and accounting procedures and practices of the Contractor relating to this Agreement.

**8.14.Notices**

All notices under this Agreement, and any amendments to this Agreement, shall be in writing and shall be deemed given when delivered by certified mail, return receipt requested, postage prepaid, when delivered via personal service or when received if sent by overnight courier. All notices shall be directed to the Parties at the respective addresses set forth below. If the name and/or address of the representatives changes, notice of such change shall be given to the other Party in accordance with the provisions of this section.

**County:**

Megan Schaefer, Planning Manager, Law Enforcement Center, 425 Grove Street, Saint Paul, MN 55101, Email: [megan.schaefer@co.ramsey.mn.us](mailto:megan.schaefer@co.ramsey.mn.us)

**Contractor:**

William Pope, CEO, 607 East Whaley Street, Longview, TX 75601, Email: [bill.pope@ncic.com](mailto:bill.pope@ncic.com)

**8.15.Non-Conforming Services**

The acceptance by the County of any non-conforming goods/services under the terms of this Agreement or the foregoing by the County of any of the rights or remedies arising under the terms of this Agreement shall not constitute a waiver of the County's right to conforming services or any rights and/or remedies in respect to any subsequent breach or default of the terms of this Agreement. The rights and remedies of the County provided or referred to under the terms of this Agreement are cumulative and not mutually exclusive.

**8.16.Setoff**

Notwithstanding any provision of this Agreement to the contrary, the Contractor shall not be relieved of liability to the County for damages sustained by the County by virtue of any breach of the contract by the Contractor. The County may withhold any payment to the Contractor for the purpose of setoff until such time as the exact amount of damages due the County from the Contractor is determined.

**8.17.Conflict of Interest**

The Contractor shall comply with all conflict of interest laws, ordinances, and regulations now in effect or hereafter to be enacted during the term of this Agreement. The Contractor warrants that it is not now aware of any facts that create a conflict of interest. If the Contractor hereafter becomes aware of any facts that might reasonably be expected to create a conflict of interest, it shall immediately make full written disclosure of such facts to the County. Full written disclosure shall include, but is not limited to, identification of all persons implicated and a complete description of all relevant circumstances. Failure to comply with the provisions of this subparagraph shall be deemed a material breach of this Agreement.

**8.18.Respectful Workplace and Violence Prevention**

The Contractor shall make all reasonable efforts to ensure that the Contractor's employees, officers, agents, and subcontractors do not engage in violence while performing under this Agreement. Violence, as defined by the Ramsey County Respectful Workplace and Violence Prevention Policy, is defined as words and actions that hurt or attempt to threaten or hurt people; it is any action involving the use of physical force, harassment, intimidation, disrespect, or misuse of power and authority, where the impact is to cause pain, fear or injury.

### **8.19.Force Majeure**

Neither party shall be liable for any loss or damage incurred by the other party as a result of events outside the control of the party ("Force Majeure Events") including, but not limited to: war, storms, flooding, fires, strikes, legal acts of public authorities, or acts of government in time of war or national emergency.

### **8.20.Unavailability of Funding - Termination**

The purchase of goods and/or labor services or professional and client services from the Contractor under this Agreement is subject to the availability and provision of funding from the United States, the State of Minnesota, or other funding sources, and the appropriation of funds by the Board of County Commissioners. The County may immediately terminate this Agreement if the funding for the purchase is no longer available or is not appropriated by the Board of County Commissioners. Upon receipt of the County's notice of termination of this Agreement the Contractor shall take all actions necessary to discontinue further commitments of funds to this Agreement. Termination shall be treated as termination without cause and will not result in any penalty or expense to the County.

### **8.21.Termination**

#### **8.21.1.**

The County may immediately terminate this Agreement if any proceeding or other action is filed by or against the Contractor seeking reorganization, liquidation, dissolution, or insolvency of the Contractor under any law relating to bankruptcy, insolvency or relief of debtors. The Contractor shall notify the County upon the commencement of such proceedings or other action.

#### **8.21.2.**

If the Contractor violates any material terms or conditions of this Agreement the County may, without prejudice to any right or remedy, give the Contractor, and its surety, if any, seven (7) calendar days written notice of its intent to terminate this Agreement, specifying the asserted breach. If the Contractor fails to cure the deficiency within the seven (7) day cure period, this Agreement shall terminate upon expiration of the cure period.

#### **8.21.3.**

The County may terminate this Agreement without cause upon giving at least thirty (30) calendar days written notice thereof to the Contractor. In such event, the Contractor shall be entitled to receive compensation for services provided in compliance with the provisions of this Agreement, up to and including the effective date of termination.

## **8.22. Interpretation of Agreement; Venue**

### **8.22.1.**

The Agreement shall be interpreted and construed according to the laws of the State of Minnesota. All litigation regarding this Agreement shall be venued in the appropriate State or Federal District Court in Ramsey County, Minnesota.

### **8.22.2.**

The provisions of this Agreement are severable. If any part of this Agreement is rendered void, invalid or unenforceable, such rendering shall not affect the validity and enforceability of the remainder of this Agreement.

## **8.23. Warranty**

The Contractor warrants that it has the legal right to provide the goods and services identified in this Agreement and further warrants that the goods and services provided shall be in compliance with the provisions of this Agreement.

## **8.24. Infringement**

### **8.24.1.**

Complementary to other "hold harmless" provisions included in this Agreement, the Contractor shall, without cost to the County, defend, indemnify, and hold the County, its officials, officers, and employees harmless against any and all claims, suits, liability, losses, judgments, and other expenses arising out of or related to any claim that the County's use or possession of the software, licenses, materials, reports, documents, data, or documentation obtained under the terms of this Agreement, violates or infringes upon any patents, copyrights, trademarks, trade secrets, or other proprietary rights or information, provided that the Contractor is promptly notified in writing of such claim. The Contractor will have the right to control the defense of any such claim, lawsuit, or other proceeding. The County will in no instance settle any such claim, lawsuit, or proceeding without the Contractor's prior written approval.

### **8.24.2.**

If, as a result of any claim of infringement of rights, the Contractor or County is enjoined from using, marketing, or supporting any product or service provided under the agreement with the County (or if the Contractor comes to believe such injunction imminent), the Contractor shall either arrange for the County to continue using the software, licenses, materials, reports, documents, data, or documentation at no additional cost to the County, or propose an equivalent, subject to County approval. The acceptance of a proposed equivalent will be at the County's sole discretion. If no alternative is found acceptable to the County acting in good faith, the Contractor shall remove the software, licenses, materials, reports, documents, data, or documentation and refund any fees and any other costs paid by the County in conjunction with the use thereof.



## **8.25. Ramsey County Cooperative Contract**

This is a Ramsey County Cooperative Contract available to all Ramsey County departments.

## **8.26. Cooperative Purchasing**

Public entities that have a purchasing Joint Powers Agreement with Ramsey County may purchase under this Agreement after having received written permission from the Contractor. Such public entities shall execute their own contract directly with the Contractor. Ordering and payment shall be the sole responsibility of such public entity and in no manner shall be the obligation, liability or responsibility of the County.

## **8.27. Contract Provisions for Non-Federal Entity Contracts Under Federal Awards**

### **8.27.1.**

Contracts and subcontracts for more than the simplified acquisition threshold, which is the inflation adjusted amount determined by the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council (Councils) as authorized by 41 U.S.C. 1908, shall address administrative, contractual, or legal remedies in instances where contractors violate or breach contract terms, and provide for such sanctions and penalties as appropriate.

### **8.27.2.**

Resulting contracts and subcontracts in excess of \$10,000 shall address termination for cause and for convenience by the non--Federal entity including the manner by which it will be effected and the basis for settlement.

### **8.27.3.**

**Debarment and Suspension (Executive Orders 12549 and 12689)**--A contract award at any tier (see 2 CFR 180.220) shall not be made to parties listed on the government-wide exclusions in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR part 1986 Comp., p. 189) and 12689 (3 CFR part 1989 Comp., p. 235), "Debarment and Suspension." SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549.

### **8.27.4.**

**Rights to Inventions Made Under a Contract or Agreement.** If the Federal award meets the definition of "funding agreement" under 37 CFR § 401.2 (a) and the County or the Contractor wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that "funding agreement," the County or the Contractor shall comply with

the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

#### 8.27.5.

**Byrd Anti--Lobbying Amendment (31 U.S.C. 1352)**--Contractors that apply or bid for an award exceeding \$100,000 shall provide the required Contractor Certification Regarding Lobbying for Contracts, Grants, Loans and Cooperative Agreement form. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier shall also disclose any lobbying with non--Federal funds that takes place in connection with obtaining any Federal award. Such disclosures shall be forwarded from tier to tier up to the non--Federal awardee, Ramsey County.

#### 8.27.6.      **48 CFR § 52.203-16 PREVENTING PERSONAL CONFLICTS OF INTEREST (JUN 2020)**

(a) **Definitions.** As used in this clause -

*Acquisition function closely associated with inherently governmental functions* means supporting or providing advice or recommendations with regard to the following activities of a Federal agency:

- (1) Planning acquisitions.
- (2) Determining what [supplies](#) or services are to be acquired by the Government, including developing statements of [work](#).
- (3) Developing or approving any contractual documents, to include documents defining requirements, incentive plans, and evaluation criteria.
- (4) Evaluating contract proposals.
- (5) Awarding Government contracts.
- (6) Administering contracts (including ordering [changes](#) or giving technical direction in contract performance or contract quantities, evaluating contractor performance, and accepting or rejecting contractor products or services).
- (7) Terminating contracts.
- (8) Determining whether contract costs are reasonable, allocable, and allowable.

*Covered employee* means an [individual](#) who performs an [acquisition function closely associated with inherently governmental functions](#) and is --

- (1) An [employee](#) of the contractor; or
- (2) A [subcontractor](#) that is a self-employed [individual](#) treated as a [covered employee](#) of the contractor because there is no employer to whom such an [individual](#) could submit the required disclosures.

*Non-public information* means any Government or third-party [information](#) that --

- (1) Is exempt from disclosure under the [Freedom of Information Act \(5 U.S.C. 552\)](#) or otherwise protected from disclosure by statute, [Executive](#) order, or regulation; or
- (2) Has not been disseminated to the general public and the Government has not yet determined whether the [information](#) can or will be [made](#) available to the public.

*Personal conflict of interest* means a situation in which a [covered employee](#) has a financial [interest](#), personal activity, or relationship that could impair the [employee's](#) ability to act impartially and in the best [interest](#) of the Government when performing under the contract. (A de minimis [interest](#) that would not "impair the [employee's](#) ability to act impartially and in the best [interest](#) of the Government" is not covered under this [definition](#).)

- (1) Among the sources of personal conflicts of [interest](#) are -
  - (i) Financial [interests](#) of the [covered employee](#), of close family members, or of other members of the [covered employee's](#) household;
  - (ii) Other employment or financial relationships (including seeking or negotiating for prospective employment or business); and
  - (iii) Gifts, including travel.
- (2) For example, financial [interests](#) referred to in paragraph (1) of this [definition](#) may arise from --
  - (i) [Compensation](#), including wages, salaries, commissions, professional fees, or fees for business referrals;
  - (ii) Consulting relationships (including commercial and professional consulting and service arrangements, scientific and technical advisory board memberships, or serving as an expert witness in litigation);

(iii) Services [provided](#) in exchange for honorariums or travel expense reimbursements;

(iv) Research funding or other forms of research support;

(v) Investment in the form of stock or bond ownership or partnership [interest](#) (excluding diversified mutual fund investments);

(vi) Real estate investments;

(vii) Patents, copyrights, and other intellectual [property](#) interests; or

(viii) Business ownership and investment interests.

**(b) Requirements.** The Contractor shall --

(1) Have procedures in place to screen covered [employees](#) for potential personal conflicts of [interest](#), by -

(i) Obtaining and maintaining from each [covered employee](#), when the [employee](#) is initially assigned to the task under the contract, a disclosure of [interests](#) that might be affected by the task to which the [employee](#) has been assigned, as follows:

(A) Financial [interests](#) of the [covered employee](#), of close family members, or of other members of the [covered employee](#)'s household.

(B) Other employment or financial relationships of the [covered employee](#) (including seeking or negotiating for prospective employment or business).

(C) Gifts, including travel; and

(ii) Requiring each [covered employee](#) to update the disclosure statement whenever the [employee](#)'s personal or financial circumstances change in such a way that a [new personal conflict of interest](#) might occur because of the task the [covered employee](#) is performing.

(2) For each [covered employee](#) --

(i) Prevent personal conflicts of [interest](#), including not assigning or allowing a [covered employee](#) to perform any task under the contract for which the Contractor has identified a [personal conflict of interest](#) for the [employee](#) that the Contractor or [employee](#) cannot satisfactorily prevent or mitigate in consultation with the contracting [agency](#);

(ii) Prohibit use of [non-public information](#) accessed through performance of a Government contract for personal gain; and

(iii) Obtain a signed non-disclosure agreement to prohibit disclosure of [non-public information](#) accessed through performance of a Government contract.

(3) Inform covered [employees](#) of their obligation --

(i) To disclose and prevent personal conflicts of [interest](#);

(ii) Not to use [non-public information](#) accessed through performance of a Government contract for personal gain; and

(iii) To avoid even the appearance of personal conflicts of [interest](#);

(4) Maintain effective oversight to verify compliance with personal conflict-of-interest safeguards;

(5) Take appropriate disciplinary action in the case of covered [employees](#) who fail to comply with policies established pursuant to this clause; and

(6) Report to the Contracting Officer any personal conflict-of-interest violation by a [covered employee](#) as soon as it is identified. This report shall include a description of the violation and the proposed actions to be taken by the Contractor in response to the violation. [Provide](#) follow-up reports of corrective actions taken, as necessary. Personal conflict-of-interest violations include --

(i) Failure by a [covered employee](#) to disclose a [personal conflict of interest](#);

(ii) Use by a [covered employee](#) of [non-public information](#) accessed through performance of a Government contract for personal gain; and

(iii) Failure of a [covered employee](#) to comply with the terms of a non-disclosure agreement.

**(c) Mitigation or waiver.**

(1) In exceptional circumstances, if the Contractor cannot satisfactorily prevent a [personal conflict of interest](#) as required by paragraph (b)(2)(i) of this clause, the Contractor may submit a request through the Contracting Officer to the Head of the Contracting Activity for -

(i) Agreement to a plan to mitigate the [personal conflict of interest](#); or

(ii) A waiver of the requirement.

(2) The Contractor shall include in the request any proposed mitigation of the [personal conflict of interest](#).

(3) The Contractor shall --

(i) Comply, and require compliance by the [covered employee](#), with any conditions imposed by the Government as necessary to mitigate the [personal conflict of interest](#); or

(ii) Remove the Contractor [employee](#) or [subcontractor employee](#) from performance of the contract or terminate the applicable [subcontract](#).

(d) **Subcontracts.** The Contractor shall include the substance of this clause, including this paragraph (d), in [subcontracts](#) --

(1) That exceed the simplified acquisition threshold, as defined in Federal Acquisition Regulation [2.101](#) on the date of [subcontract](#) award; and

(2) In which [subcontractor employees](#) will perform acquisition functions closely associated with inherently governmental functions (i.e., instead of performance only by a self-employed individual).

## 8.28. Debarment and Suspension

Ramsey County has enacted Ordinance 2013-330 [Ramsey County Debarment Ordinance](#) that prohibits the County from contracting with contractors who have been debarred or suspended by the State of Minnesota and/or Ramsey County.

## 8.29. Alteration

Any alteration, variation, modification, or waiver of the provisions of this Agreement shall be valid only after it has been reduced to writing and signed by both parties.

## 8.30. Entire Agreement

The written Agreement, including all attachments, represent the entire and integrated agreement between the parties hereto and supersede all prior negotiations, representations or contracts, either written or oral. No subsequent agreement between the County and the Contractor to waive or alter any of the provisions of this Agreement shall be valid unless made in the form of a written Amendment to this Agreement signed by authorized representatives of the parties.

# 9. Special Contract Terms and Conditions

## 9.1.

### 1) Payment Card Industry Compliance

In addition to section 8.8.1 above, the Contractor, and their merchant services provider, shall at all times maintain compliance with the most current Payment Card Industry Data Security Standards (PCI DSS). Contractor shall provide a current copy of the attestation of compliance (AOC) and shall provide annually.

### 2) Contractor's Personnel

Contractor shall ensure that during the term of the Agreement, it has adequate staff of

competent personnel to perform the services and provide the Deliverables set forth in the Agreement. The County may, at any time, request in writing, the withdrawal or replacement of any personnel assigned to an SOW and such request shall not be unreasonably refused by the Contractor. The Contractor shall not replace or withdraw any personnel assigned to the Agreement without prior written consent of the County.

### **3) Identity of Subcontractors**

The identity of all subcontractors who will work on the Project shall be disclosed in the Contractor's Proposal. If during the performance of the Agreement, the Contractor intends to enter into any further subcontracts it shall only be with the prior written approval of the County, and subject to such conditions and provisions as the County may deem necessary.

### **4) CJIS Requirements**

The County has electronic access to state and federal databases containing unencrypted and confidential Criminal Justice Information ("CJI"). These databases are managed by the Minnesota Bureau of Criminal Apprehension ("BCA") which requires that anyone who could have 'logical and physical access to CJI' must submit to a fingerprint-based record check ("Covered Individuals"). This includes not only those who actually have authorization to access CJI from their desktop computers, but also includes those who receive the CJI for any reason and those who do not receive CJI but are or could be in the general physical proximity of those who do receive it. This includes both a Contractor's employees and sub-contractors.

Covered Individuals must contact the BCA at [BCACJISSATScreening@state.mn.us](mailto:BCACJISSATScreening@state.mn.us) to complete the vendor screening program. Covered Individuals must complete the program and obtain approval prior to accessing any CJIS data under this Agreement.

Additionally, Contractor and all applicable employees and/or subcontractors must be in compliance with all applicable data security rules and regulations. Contractor must maintain an overall understanding and provide the current level of compliance with Federal Bureau of Investigation's Criminal Justice Information Services (FBI CJIS) Security Policy 5.4, and related security policy(ies) or its successor version(s), including the *CJIS Security Addendum*, **Exhibit 2** and the *CJIS Security Addendum Certification*, **Exhibit 3** as well as the Minnesota Bureau of Criminal Apprehension's Minnesota Justice Information Services (BCA MNJIS) security requirements outlined in FBI CJIS requirements document(s) and BCA Security Policy 5050, or its successor version(s). **Exhibit 2** and **Exhibit 3** are attached and made a part of the Agreement.

**Professional Services Agreement #: RC-000660**  
**Attachment A – County’s Hosting Security Exhibit**

1. **Virtual Infrastructure/Cloud Services.** In addition to the Contractor responsibilities listed in the Agreement by and between the Parties, Contractor acknowledges and agrees to assume the following additional responsibilities:
  - 1.1. **Connectivity.** Contractor will provide the connectivity as described in in the Agreement.
  - 1.2. **Load Balancing.** Contractor will load balance the County applications to meet the needs of the County’s operations, as may be further described in the County’s system architecture specifications, or as mutually agreed to by the Parties.
  - 1.3. **Security.** Contractor will implement reasonable and appropriate systems and procedures sufficient to ensure the security and confidentiality of the County Data, as further specified herein. County Data is defined as the data described in the Data Practices section of this Professional Services Agreement.
  - 1.4. **SOC 3.** Contractor will provide the Services utilizing a SOC 3 compliant data center located in the continental United States. Contractor will perform periodic audits (SOC 3 or other industry equivalent standard mutually agreed to by the Parties) of Contractor’s security controls (i.e., physical and logical security, network configuration, change/problem and vulnerability management and recovery services), and make available to the County a copy of such SOC 3 report and, upon the County’s request, written reports regarding such audits. In the event of any qualified statements in such reports that materially impact the County, the County may immediately terminate the Agreement for material breach without further period to cure.
  - 1.5. **Back-up Services.** Contractor will perform the backup services at the following intervals: Contractor will back-up the servers containing County Data one time each day to a storage area network (SAN), and Contractor will keep each such daily back-up for seven days; Contractor will back-up the servers containing County Data one time each week to a back-up tape. Each week, the back-up tape will be encrypted and stored offsite at a SOC 3 facility located in the continental United States. Contractor will retain one back-up tape per week for seven years. In addition, Contractor will fulfill restoration requests as directed by the County due to site failures. Restoration will be performed within the interval of two to four hours depending on the urgency of the request; and the agreed upon location of the desired back-up media; and if the location is expected to be down for more than 24 hours, Contractor will immediately transfer appropriate back-up data and re-establish all hosting operations in an appropriately functioning secondary server or location.
  - 1.6. **Anti-Virus Software.** Contractor will install and maintain industry standard anti-virus and anti-spyware software for all physical and virtual servers used to provide the Services.
  - 1.7. **Fix Errors.** Contractor will use Contractor’s best efforts to promptly remedy any failure of the Services.
2. **Multi Factor Authentication.** Contractor will utilize a secure, multi-factor method of remote authentication and authorization to access the system(s).



**Professional Services Agreement #: RC-000660**  
**Attachment A – County’s Hosting Security Exhibit**

**3. Monitoring Services.** Contractor will provide the following additional Services with respect to system monitoring:

**3.1. Access.** Contractor will provide access to Contractor’s client portal, monitoring and alerting of the County’s servers, as well as the processes and services being executed by such servers by Contractor’s Network Operations Center on a 24 x 7 x 365 basis. In addition, the County will be provided with access to Contractor’s Network Operations Center, which allows for 24x7x365 access to support requests, open ticket status, reporting and a knowledge base of previous County issues and projects.

**3.2. Monitoring and Detection.** Contractor will provide monitoring and alerting by Contractor’s Network Operations Center on a 24 x 7 x 365 basis of Services.

**3.3. Equipment Monitored.** The County requests that the Services be provided to cover the computer related items detailed on any network and infrastructure equipment inventory list maintained by Contractor in any County provided disaster recovery guidelines.

**3.3.1 Additional Equipment.** If the County has or purchases additional equipment, the monthly fee for Services will automatically be increased at the beginning of the following month to cover the additional equipment. Additional equipment must be inspected and certified as “fit for purpose” by Contractor before it is covered under this Hosting Security Exhibit.

**3.3.2 Equipment Retirement.** If the County retires equipment that is not replaced in kind, the monthly fee for Services will automatically be decreased at the beginning of the next month to account for the decrease in the need for support. The County must notify Contractor of the equipment retirement date via e-mail.

**3.3.3. County To Provide Access.** The County will provide full and complete access, including admin usernames and password, to all equipment covered under this Hosting Security Exhibit.

**3.4. Notification.** Contractor will notify the County of disruption in any Services for which Contractor is providing monitoring. To the extent not specified, Contractor will provide the County with weekly reports of Contractor’s monitoring results.

**3.5. Fix Issues.** Contractor will promptly apply a fix to any disruption in the Services.

**3.6. Communication with Network Operations Center.** The County may communicate with the Network Operations Center via telephone, email, or client portal ticket 24 hours a day, seven days a week and 365 days a year.

**3.7. Initiation of Client Portal Tickets.** Unless stated otherwise, client portal tickets are initiated or escalated within 15 minutes of receipt..

**4. Operating System Patch Services.** Contractor will provide the following Services with respect to operating system Patches:

**4.1. Patch Monitoring Services.** Contractor will monitor recommendations from software vendors relating Patches (defined below) to software used in one or more Services.

**Professional Services Agreement #: RC-000660**  
**Attachment A – County’s Hosting Security Exhibit**

- 4.2. Installation Services.** Contractor will install Patches at a time appropriate to their risk level, which may include considering the following factors: any possible disruption to the Services, and the urgency of the need to install the Patch.
- 4.3. Notification.** Contractor will notify the County of Patch management installations in accordance with the notification requirements agreed upon by the County and Contractor in any Patch Management and Monitoring. To the extent not specified, Contractor will provide the County with weekly reports of Contractor’s Patch recommendations and/or installations.
- 4.4. Definition of Patch.** For the purposes of this Hosting Security Exhibit, the term “Patch” means platform and applications software security and anti-virus updates and other software fixes and updates issued by and recommended for installation by software vendors for Software used in one or more Services.
- 5. Security Standards.** Contractor shall comply with all security measures and policies as outlined in the Agreement as well as Contractor’s data privacy, security policies, client guide and/or Information Security Policy, and security procedures that apply to county data, which have been provided to the County and are herewith included herein by reference. The Contractor shall not modify data privacy and security policies absent the County’s express consent. In the event Contractor materially degrades the information security standard during any such modification, such degradation shall constitute a material breach by Contractor under the Agreement Contractor will comply with applicable U.S. laws and regulations concerning information security, the US-EU Privacy Shield Framework as established by the United States Department of Commerce and conduct SSAE 16 audits (or SOC 2) at least annually, or in the event it is superseded, the resultant SSAE 16 equivalent.
- 6. Security Program.** Contractor agrees and represents that it currently maintains information protection practices and procedures (“Security Program”) that complies with industry best practice and applicable privacy laws. Contractor’s Security Program includes, at a minimum:
- 6.1.** Appropriate administrative, technical, and physical safeguards and other security measures designed to ensure the security and confidentiality of County Data;
  - 6.2.** A security design intended to prevent any compromise of Contractor’s own information systems, computer networks or data files by unauthorized users, viruses, or malicious computer programs which could in turn be propagated to County;
  - 6.3.** Appropriate internal practices including, but not limited to, encryption of data in transit and at rest; using appropriate firewall and antivirus software; maintaining these countermeasures, operation systems and other applications with up-to-date virus definitions and security patches so as to avoid any adverse impact to County’s systems or information; appropriate logging and alerts to monitor access controls and assure data integrity and confidentiality; installing and operating security mechanisms in the manner intended sufficient to ensure County government operations must not be disrupted; permitting only authorized users access to systems and applications; and preventing unauthorized access to County systems via the Contractor’s networks and access codes; and

**Professional Services Agreement #: RC-000660**  
**Attachment A – County’s Hosting Security Exhibit**

**6.4.** All persons with authorized access to County Data must have a documented genuine need-to-know prior to access;

**6.5.** Contractor warrants that the services and deliverables will not contain, and Contractor, its employees or Contractor’s Agents will not introduce through data transmission or any other means, any virus, ransomware, malware, spyware, bomb, worm, trap door, back door, Trojan horse, malicious logic, drop dead device, software lock, disabling code or any other contaminant, program routine or disabling device, including without limitation, any key, timer, clock, counter, local shared object/flash cookies or other self-enacting device or limiting routines, codes, commands, or instructions or other feature that may have the effect or that could be used to access, track activity on, alter, delete, damage, deactivate, interfere with, disable or otherwise harm any service or deliverable or the County owned, licensed and/or leased computer hardware, software, code, systems, data, compilations of data, or other property.

**7. Source Code Protection.** Contractor will have in place and will maintain an industry standard security program which protects Contractor’s source code from a compromise by Contractor’s subcontractors or any other third party.

**8. Audit.** County may conduct a security review of Contractor’s Security Program when determined as reasonably required by County. Contractor will provide County copies of its data privacy and security policies and procedures that apply to County Data. Subject to reasonable notice, Contractor shall provide County an opportunity to conduct a privacy and security audit of Contractor’s Security Program and systems and procedures that are applicable to the Services provided by Contractor to County. Such audit may be conducted on-site by County personnel or County’s contracted third party assessors or through surveys and interviews, at the option of County. In the event that Contractor has any security audits or review of its own systems performed by Contractor or a third party, including vulnerability and penetration assessments, it will give County notice of any current findings that are likely to adversely impact County Data and will keep County timely informed of its remediation efforts. If the audit reveals any vulnerability, Contractor shall correct such vulnerability at its sole cost and expense and shall certify the same in writing to County. Contractor shall use best efforts to correct all vulnerabilities and provide County a report explaining corrective actions immediately but no later than within thirty (30) days of completion of the audit, unless County agrees in writing otherwise. Contractor’s failure to procure audits or to complete corrections in a timely manner will be a material breach of the Agreement.

**9. Mobility and Transfer of Data.** No Confidential Information, CPI, CPM or County Data shall be stored, transported, or kept on a laptop or any other mobile device or storage media, including USB, “thumb drives,” DVDs, CDs, unless encrypted using an encryption methodology approved in writing by County. All electronic data transfers of County Data must be via secure FTP or other County approved protocol and/or in approved encrypted form. Any physical removal or transfer of County Data from County’s or Contractor’s facilities shall be conducted only according to controls developed or approved by County.

**Professional Services Agreement #: RC-000660**  
**Attachment A – County’s Hosting Security Exhibit**

**10. Security Certification.** Contractor must maintain a level of security certification or assessment consistent with best practices and by a qualified third party reasonably acceptable to County. Such certifications shall be provided to County as reasonably requested by County.

**11. Segmentation.** Contractor warrants that all County Data is maintained so as to preserve segmentation of County Data from data of others.

**12. Controls.** The County agrees that Contractor is solely responsible for all testing and auditing, including port scanning and penetration testing, of Contractor security controls. Contractor shall provide results of such testing as requested by the County.

**13. Penetration Testing.** Penetration testing of the Contractor’s architecture is included at a frequency of one per year at no additional cost. Contractor will coordinate with the current Contractor penetration testing vendor and shall use best efforts to remedy any issues identified immediately but no later than within thirty (30) days of reporting. At the County’s request Contractor will provide the final report to the County once it has been verified it does not contain information related to any other clients. Contractor’s failure to remedy and report the remedy in a timely manner will be a material breach of the Agreement. Additional penetration tests or the County specific penetration tests will be at the expense of the County and will be arranged through Contractor’s vendor for penetration testing.

**14. Security Policies.** Contractor’s security policy is posted [Insert URL] and is made up of the following documents:

- Acceptable Use Policy
- Access Control Policy
- Business Continuity Policy
- Data Destruction and Retention Policy
- Data Security Policy
- Disaster Recovery Policy
- Email Use Policy
- Encryption Policy
- Exception Request Policy
- Incident Management policy
- Internet Security Policy
- Mobile Device Policy
- Network Security Policy
- Password Policy
- Patch Management Policy
- Personnel Security and Termination Policy

**Professional Services Agreement #: RC-000660**  
**Attachment A – County’s Hosting Security Exhibit**

- Physical Security Policy
- Privacy Policy
- Physical Security Policy
- Server Security Policy
- Scanning and Security Policy
- Server Audit Policy
- Third Party Access Policy

**15. Hosting Security Standards.** The hosting security standards for the Contractor or Contractor’s Agent’s data center(s) (the “Data Center”) include:

- Physical Security
  1. Video cameras
  2. Motion sensors
  3. Fire sensors
  4. Locked doors with controlled access
  5. Manned reception area
  6. Visitor log

There are no external windows in the Data Center. In the Data Center, all physical equipment is owned or leased by Contractor and/or Contractor’s Agent and is subject to terms herein for all such hosting services including without limitation the secure management and monitoring of all components of the Services provided. Exterior perimeter walls, doors, windows and the main interior entry door to the raised floor environment are constructed of materials that afford UL rated ballistic protection. Vegetation and other objects within the Data Center are maintained such that an intruder would not be concealed.

Physical access mechanisms (e.g. access cards, biometric devices, man-traps and portals) have been implemented and are administered by local operations staff to help ensure that only authorized individuals have the ability to access the Data Center. Portals and Tdar man-traps have been installed as an anti-tailgating measure in the Data Center lobby. All access into and out of the Data Center is through either a portal or Tdar man-trap. The portal/man-trap bypass doors are only to be used in the event an individual is unable to use the portal or man-trap. Examples include handicap, phobia or other restrictions on a case-by-case basis. Tours and emergency Data Center security operations crews will be permitted to use the Portal bypass door, when necessary. All security systems have dedicated 24x7 UPS systems and standby emergency power support.

The Data Center incorporates video cameras, motion sensors, fire sensors, locked doors with controlled access, manned reception area, visitor log, and glass break sensors in the Data Center. There are no external windows in the Data Center. Video cameras are used in the front entrances, emergency exits, secure areas, main lobby, elevators, general employee areas, within the Data Center and monitoring the grounds and parking lots around the Data Center. Security monitoring is recorded to digital files with a 90 day retention. Tapes are rotated every 30 days and are stored offsite. Motion sensors are located on the

**Professional Services Agreement #: RC-000660**  
**Attachment A – County’s Hosting Security Exhibit**

roof and are armed 24x7. The Data Center utilizes on-site and remote monitoring centers and both are manned 24x7.

The Data Center requires a key-card for entry. Only three designated employees are permitted to open the door to accept shipments or greet visitors. The Data Center is staffed from 6 a.m. to 7 p.m. weekdays. Security guards patrol the building during unstaffed hours. Video cameras are positioned in the areas surrounding the Data Center. All visitors must sign in and be escorted at all times.

All persons requesting access into the Data Center must be positively identified. This process requires the requesting person to submit valid (unexpired) Government issued photographic ID at the desk and sign in and out of the Data Center. Visitors must be approved by Contractor’s personnel prior to arriving at the Data Center. The Data Center incorporates secure badges, secure visitor badges, and biometrics. All visits must be arranged in advanced, and all visitors are escorted at all times.

- Network Security
  1. Every connection to an external network is terminated at a firewall.
  2. Network devices are configured to prevent communications from unapproved networks.
  3. Network devices deny all access by default.
  4. Security patches are regularly reviewed and applied to network devices.
  5. Contractor follows a strict change management process which incorporates Change Advisory Board review and approvals.
  6. Communication through a network device is controlled at both the port and IP address level.
  7. There is a documented standard for the ports allowed through the network devices.
  8. Contractor prevents unauthorized devices from physically connecting to the internal network.
  9. There is an approval process to allow the implementation of extranet connections.
  10. There are regular scans for rogue wireless access points.
  11. Contractor manages a SIEM (Security Information and Event Management) tool to review any potential security, infrastructure and vulnerabilities.
  12. Contractor subscribes to Contractor’s Agent’s dedicated NIDS service and 24 x 7 incident response to monitor and respond to intrusion attempts.
  13. The Data Center is compliant with SOC-1 and SOC-2.

**16. Backup.** Contractor uses daily on-site backups that are transferred offsite weekly. On-site backups are in a secured tape library within the data center. The tapes travel to a secure facility in locked storage. All of the County Data will be contained in a distinct database that will follow the backup process set forth in the Agreement. Some systems are not backed up because they do not contain any useful data and the recovery process is to rebuild these systems.

**Professional Services Agreement #: RC-000660**  
**Attachment A – County’s Hosting Security Exhibit**

- Full backups of the County’s repositories are performed daily at 11:30 p.m. CT.
- Incremental backups are performed every hour.
- The backups are sent to tape every evening.
- Backup tapes are tracked in the Data Center where the backup takes place.
- Tapes are in locked containers before going offsite.
- The containers are tracked in the offsite facility and are stored for thirty (30) days.

**17. Disaster Recovery.** Contractor’s Disaster Recovery plan is structured in a recovery team format. This format increases the efficiency by allowing departments to be recovered concurrently. The plan provides critical recovery solutions, information and specific steps required to be followed by each team member to ensure successful recovery. Contractor has a Crisis Manager and leadership identified with responsibilities clearly assigned. Alternates for each critical team member are identified to be involved in the event that the team member is not available. The Disaster Recovery Plan is tested and updated at least annually or when major changes warrant updating. A report of each Disaster Recovery test is completed and any identified gaps and lessons learned are shared with leadership. Any major gaps are prioritized and mitigated where ever possible. At the County’s request, Contractor will provide the final report once it has been verified it does not contain information related to any other clients.

Contractor also includes Business Continuity Plans (BCP) as part the annual testing efforts. This includes a full BCP tabletop exercise with leadership engagement. A report of the annual BCP test is generated and reviewed with leadership. Any gaps identified are prioritized by leadership and are assigned and mitigated where ever possible before the next BCP test if not before. At the County’s request, Contractor will provide the final report once it has been verified it does not contain information related to any other clients.

**18. County Data.** The Contractor shall provide the County with all County Data upon termination or at any earlier time in the format reasonably requested by the County at no additional cost to the County. In addition, to the extent the County requests Transition Services, the Contractor will provide such Transition Services as provided below. The return of the County Data will either be provided once Transition Services are completed, or earlier, as requested by the County. The Contractor shall not destroy the County Data until such time as the County has confirmed successful access to the returned County Data.

**18.1.** “Transition Services” means those Services that are provided by Contractor to County at the time of expiration or termination of the Agreement, Service Order, SOW, or any other termination of Services, along with any new services that County may require to transfer County Data, and the affected Services to County or to any third party designated and authorized by County.

**18.2.** “Transition Services Period” means a period of six (6) months, or as otherwise described in the Agreement, Service Order or SOW, for the orderly transition of Services

**Professional Services Agreement #: RC-000660**  
**Attachment A – County’s Hosting Security Exhibit**

and transfer of any County Data to County or another service provider, beginning upon the expiration of the Agreement, Service Order, SOW, or other termination of Services.

**18.3.** “Transition Services Plan” is the written methodology and approach, including Deliverables and timelines that Contractor will use to deliver the Transition Services during the Transition Services Period.

**18.4.** Transition Services. In connection with the expiration or termination of the Agreement, any Service Order, or SOW, for any reason, and notwithstanding any dispute between the Parties, Contractor will provide Transition Services for the Transition Services Period, or as otherwise agreed upon between the Parties as follows: (i) Applicable Requirements and Access. At no additional cost Contractor will provide County and any designated Third Party Service Provider in writing, to the extent applicable, applicable standards, policies, operating procedures, and other Documentation relating to the affected Services; (ii) Development of Transition Services Plan. If requested by County, at Contractor’s expense, Contractor will assist County and its designated Third Party Service Provider in developing a Transition Services Plan; (iii) Comparable Fees. Contractor shall provide the Transition Services during the Transition Service Period at fees that are no greater than fees charged County for comparable services prior to termination or if comparable services were not performed for County prior to termination or expiration, then at fees no greater than the fees charged by Contractor to other similarly situated customers or fair market value, whichever amount is less; (iv) Post Transition Services Period. For up to three (3) months after the Transition Services Period, at no cost to County, Contractor will answer all reasonable and pertinent verbal or written questions from County regarding the Services on an “as needed” basis as agreed to by the Parties, and deliver to the County any County owned reports materials and information including without limitation any Confidential Information, CPI, CPM, and County Data that might still be in the possession of Contractor; and (v) Absolute Obligation. Contractor agrees that it has an absolute and unconditional obligation to provide County with Transition Services and Contractor’s quality and level of performance during the Transition Service Period will continue to adhere to all requirements of the Agreement.

**19. Data Retention.** Contractor may continue to keep or maintain any County Data obtained in the course of performance of the Services so long as the Agreement and the relevant Service Order or SOW remains in effect and such use shall not extend beyond the termination of the Agreement or the relevant Service Order or SOW except with respect to providing Transition Services, provided that Contractor will provide a copy of the County Data upon termination or expiration of the Agreement in accordance with Section XX or at any time requested by County.

**20. Warranties.**

**20.1.** Contractor warrants that the Services and Deliverables will not contain, and Contractor, its employees or Contractor’s Agents will not introduce through data transmission or any other means, any virus, ransomware, malware, spyware, bomb, worm, trap door, back door, Trojan horse, malicious logic, drop dead device, software lock, disabling code or any other contaminant, program routine or disabling device, including without limitation, any key, timer, clock, counter, local shared object/flash



**Professional Services Agreement #: RC-000660**  
**Attachment A – County’s Hosting Security Exhibit**

cookies or other self-enacting device or limiting routines, codes, commands, or instructions or other feature that may have the effect or that could be used to access, track activity on, alter, delete, damage, deactivate, interfere with, disable or otherwise harm any Service or Deliverable or the County owned, licensed and/or leased computer hardware, software, code, systems, data, compilations of data, or other property.

**20.2.** Contractor warrants that (a) all Services and Deliverables will strictly comply, function and perform in accordance with the functional requirements and specifications of County or as otherwise identified in any and all specifications, criteria, requirements and documentation specified or referred to in the applicable Service Order(s) and/or SOW(s), (b) the Documentation, if any is to be provided, will be accurate, complete and sufficient in detail to enable the End Users to use all of the functionality of the Services and Deliverables without assistance from Contractor or any third party, (c) no information transferred through or stored in or on the Services or Deliverables, while in the possession or under the control of Contractor, will be subject to any loss of accuracy or integrity or corruption, and (d) all Services or Deliverables will comply, function and perform in accordance with all applicable laws and regulations. In the event that the County discovers that any Services or Deliverables do not conform to and perform in accordance with the specifications and requirements of the County, the County shall promptly notify Contractor in writing of such nonconformance, and Contractor shall, at Contractor’s sole cost and expense, promptly re-perform Services to modify such Services or Deliverable to make it conform, time being of the essence. In the event Contractor is unable to qualitatively and functionally re-perform the Services or correct a Deliverable within five (5) business days of County notice of the nonconforming Service or Deliverable, County may seek and obtain a refund for the defective Services or Deliverable. Contractor’s failure to properly remedy any failed warranty outlined above shall not preclude County from exercising any other remedies available to it under the Agreement or at law or equity.

**20.3.** Contractor represents and warrants that all third party materials required to operate and fully utilize the Services or Deliverables will be fully disclosed to the County and are commercially available to the County and unless otherwise identified in a Service Order or SOW, no additional license fee or other costs will be incurred by County for use of the Services. Contractor shall and hereby does assign and pass through to the County all warranties, representations and indemnities granted to Contractor by third parties in and with respect to such third party materials, or any component thereof, and all remedies for breach of such warranties, representations and indemnities.

- 1. County Policies, Procurements & Requirements.** Contractor will perform Services in accordance with the Agreement and any County policies, procedures, and any requirements specifically provided to Contractor. If policies, procedures or standards are updated or changed, County will provide reasonable advance notice when feasible to Contractor. If Contractor is unable or unwilling to comply with the updated or changed County policies, procedures and requirements within thirty (30) days of notice of such update or change, the Agreement may be terminated for cause without a further period of time to cure. If Contractor performs Services through Contractor's Agent, Contractor shall ensure that such Contractor's Agent shall perform such Services in accordance with the terms of the Agreement, including any County provided policies, procedures and requirements.
- 2. Multi Factor Authentication.** Contractor will utilize a secure, multi-factor method of remote authentication and authorization to access the system(s).
- 3. Security Program.** Contractor agrees and represents that it currently maintains information protection practices and procedures ("**Security Program**") that complies with industry best practice and applicable Privacy Laws. Contractor's Security Program includes, at a minimum:

  - A.** Appropriate administrative, technical, and physical safeguards and other security measures designed to ensure the security and confidentiality of County Data;
  - B.** A security design intended to prevent any compromise of Contractor's own information systems, computer networks or data files by unauthorized users, viruses, or malicious computer programs which could in turn be propagated to County;
  - C.** Appropriate internal practices including, but not limited to, encryption of data in transit and at rest; using appropriate firewall and antivirus software; maintaining these countermeasures with up-to-date virus definitions and security patches so as to avoid any adverse impact to County's systems or information; appropriate logging and alerts to monitor access controls and assure data integrity and confidentiality; installing and operating security mechanisms in the manner intended sufficient to ensure County government operations must not be disrupted; permitting only authorized users access to systems and applications; and preventing unauthorized access to County systems via the Contractor's networks and access codes; and
  - D.** All persons with authorized access to County Data must have a documented genuine need-to-know prior to access.
- 4. Training and Supervision.** Contractor conducts appropriate and reasonable background checks or other investigations of its job candidates or Contractor's Agents prior to such persons' employment or access to County Data. Contractor represents that it maintains adequate training and education programs to ensure that its employees and Contractor's

Agents are aware of and adhere to its Security Program. Contractor shall exercise necessary and appropriate supervision over its employees and Contractor's Agents to maintain appropriate confidentiality and security of County Data.

- 5. Third Parties.** Contractor shall not share, transfer, disclose or otherwise provide access to any County Data, to any third party unless it is a Third Party Service Provider or Contractor's Agent and County has authorized Contractor to do so in writing. Contractor will ensure that any Contractor's Agent it may desire to perform any of the services required by its Agreement with County shall be obligated to have a Security Program equivalent to that required of the Contractor. Further, regarding any Data Incident, Contractor shall contractually preserve for County all such rights as County has above. Regarding audit rights, Contractor shall contractually preserve for County all such rights as County has in the section below. Contractor shall not share County Data with any other third party, without prior written approval, or if required, to comply with legal process, only after notice to County. Contractor shall only retain Contractor's Agents that are capable of performing the delegated obligations in accordance with the Agreement.
- 6. Source Code Protection.** Contractor will have in place and will maintain an industry standard security program which protects Contractor's source code from a compromise by Contractor's subcontractors or any other third party.
- 7. Audit.** County may conduct a security review of Contractor's Security Program when determined as reasonably required by County. Contractor will provide County copies of its data privacy and security policies and procedures that apply to County Data. Subject to reasonable notice, Contractor shall provide County an opportunity to conduct a privacy and security audit of Contractor's Security Program and systems and procedures that are applicable to the Services provided by Contractor to County. Such audit may be conducted on-site by County personnel or County's contracted third party assessors or through surveys and interviews, at the option of County. In the event that Contractor has any security audits or review of its own systems performed by Contractor or a third party, including vulnerability and penetration assessments, it will give County notice of any current findings that are likely to adversely impact County Data and will keep County timely informed of its remediation efforts. If the audit reveals any vulnerability, Contractor shall correct such vulnerability at its sole cost and expense and shall certify the same in writing to County. Contractor shall use best efforts to correct all vulnerabilities and provide County a report explaining corrective actions immediately but no later than within thirty (30) days of completion of the audit, unless County agrees in writing otherwise. Contractor's failure to procure audits or to complete corrections in a timely manner will be a material breach of the Agreement.

- 8. Security Certification.** Contractor must maintain a level of security certification or assessment consistent with best practices and by a qualified third party reasonably acceptable to County. Such certifications shall be provided to County as reasonably requested by County.
- 9. Security Standards.** Contractor shall comply with all security measures and policies as outlined in the Agreement as well as Contractor's client guide and/or Information Security Policy which have been provided to the County and are herewith included herein by this reference. The Contractor shall not modify its client guide and/or Information Security Policy absent the County's express consent. In the event Contractor materially degrades the information security standard during any such modification, such degradation shall constitute a material breach by Contractor under the Agreement and this Information Security Exhibit. Contractor will comply with applicable U.S. laws and regulations concerning information security, the US-EU Privacy Shield Framework as established by the United States Department of Commerce and conduct SSAE 16 audits (or SOC 2) at least annually, or in the event it is superseded, the resultant SSAE 16 equivalent.
- 10. Controls.** The County agrees that Contractor is solely responsible for all testing and auditing, including port scanning and penetration testing, of Contractor security controls. Contractor shall provide results of such testing as requested by the County.
- 11. Penetration Testing.** Penetration testing of the Contractor's architecture is included at a frequency of one per year at no additional cost. Contractor will coordinate with the current Contractor penetration testing vendor and shall use best efforts to remedy any issues identified immediately but no later than within thirty (30) days of reporting. At the County's request Contractor will provide the final report to the County once it has been verified it does not contain information related to any other clients. Contractor's failure to remedy and report the remedy in a timely manner will be a material breach of the Agreement. Additional penetration tests or the County specific penetration tests will be at the expense of the County and will be arranged through Contractor's vendor for penetration testing.
- 12. Anti-Malware Warranty.** Contractor warrants that the Services and Deliverables will not contain, and Contractor, its employees or Contractor's Agents will not introduce through data transmission or any other means, any virus, ransomware, malware, spyware, bomb, worm, trap door, back door, Trojan horse, malicious logic, drop dead device, software lock, disabling code or any other contaminant, program routine or disabling

device, including without limitation, any key, timer, clock, counter, local shared object/flash cookies or other self-enacting device or limiting routines, codes, commands, or instructions or other feature that may have the effect or that could be used to access, track activity on, alter, delete, damage, deactivate, interfere with, disable or otherwise harm any Service or Deliverable or the County owned, licensed and/or leased computer hardware, software, code, systems, data, compilations of data, or other property.

**13. Mobility and Transfer of Data.** No County data shall be stored, transported, or kept on a laptop or any other mobile device or storage media, including USB, "thumb drives," DVDs, CDs, unless encrypted using an encryption methodology approved in writing by County. All electronic data transfers of County Data must be via secure FTP or other County approved protocol and/or in approved encrypted form. Any physical removal or transfer of County Data from County's or Contractor's facilities shall be conducted only according to controls developed or approved by County.

**14. Security Policies.** Contractor's security policy is posted [Insert URL] and is made up of the following documents:

- Acceptable Use Policy
- Access Control Policy
- Business Continuity Policy
- Data Destruction and Retention Policy
- Data Security Policy
- Disaster Recovery Policy
- Email Use Policy
- Encryption Policy
- Exception Request Policy
- Incident Management policy
- Internet Security Policy
- Mobile Device Policy
- Network Security Policy
- Password Policy
- Patch Management Policy
- Personnel Security and Termination Policy
- Physical Security Policy

**Professional Services Agreement #: RC-000660**

**Attachment B - Information Security for On Premise Solutions ("Information Security Exhibit")**

- Privacy Policy
- Physical Security Policy
- Server Security Policy
- Scanning and Security Policy
- Server Audit Policy
- Third Party Access Policy

**15. Disaster Recovery.** Contractor's Disaster Recovery plan is structured in a recovery team format. This format increases the efficiency by allowing departments to be recovered concurrently. The plan provides critical recovery solutions, information and specific steps required to be followed by each team member to ensure successful recovery. Contractor has a Crisis Manager and leadership identified with responsibilities clearly assigned. Alternates for each critical team member are identified to be involved in the event that the team member is not available. The Disaster Recovery Plan is tested and updated at least annually or when major changes warrant updating. A report of each Disaster Recovery test is completed, and any identified gaps and lessons learned are shared with leadership. Any major gaps are prioritized and mitigated wherever possible. At the County's request, Contractor will provide the final report once it has been verified it does not contain information related to any other clients.

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660****ATTACHMENT C - PHONE CALLING SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION		Y	N	COMMENTS
<b>A. COMPLIANCE</b>					
1. FCC Compliance/Data Privacy	The system is compliant with all federal, state, and local laws, statutes, ordinances, rules, regulations, and standards for data privacy and the Federal Communications Commission (FCC).	M	Y		NCIC is fully compliant with Federal, State or local laws, statutes, etc., and all equipment meets or exceeds applicable FCC licensing, rules and certification regulations. FCC FRN# and other certification-related documents are available upon request.
2. ADA Compliance	The system is compliant with the Americans with Disability Act (ADA) and accessible to hard of hearing individuals.	M	Y		NCIC's proposed system is fully compliant with the Americans with Disability Act.
3. FBI CJIS and BCA MNJIS Compliance	The contractor and system is compliant with federal and state laws and regulations, including the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) and the Minnesota Bureau of Criminal Apprehension (BCA) Minnesota Justice Information Services (MNJIS).	M	Y		NCIC and the proposed system is compliant with all applicable Federal and State laws and regulations associated with the FBI, CJIS, BCA and MNJIS.
4. Minnesota Government Data Practices Act	The contractor and system is compliant with the Minnesota Government Data Practices Act.	M	Y		NCIC and the proposed system is fully compliant with Minnesota Government Data Practices Act
<b>B. GENERAL TECHNICAL</b>					
5. Hosting	The system is a hosted solution.	M	Y		The proposed ITS deploys a centralized soft switch platform utilizing VoIP (Voice over Internet Protocol) technology. Each of the telephone stations will connect back to a central telephone communications room within the Jail via twisted pair cable. There is no line concentration, so all phones can be used simultaneously, which increases customer satisfaction and reduces complaints. A robust MPLS (Multi-Protocol Label (Switching) network will be

**KEY:** M = Mandatory P = Preferred Y = Yes

No = No

Page 1 of 14

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660****ATTACHMENT C - PHONE CALLING SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION		Y	N	COMMENTS
					installed to establish a VPN (Virtual Private Network) to the Jail and the central software host platforms. At the Network Operations Center (NOC) level, one of ten SIP registration servers handle the secure authentication and registration of each of the VoIP routers within the inmate facility. When an inmate initiates a phone call at a jail facility, that call is handled by one of several dozen Asterisk-based call processing servers.
6. Active Directory	The system is capable of using Active Directory.	P	Y		The proposed system is capable if using Active Directory.
7. Architecture Integrations	The system supports open system/service-oriented architecture for integrations.	P	Y		The proposed system is completely open in architecture to allow for a variety of system integrations.
8. Reverse Directory	The system has an internet reverse directory look up of subscribers' information via several providers of dialed number upon selecting the dialed number on the computer screen.	P	Y		Our integrated Reverse Lookup feature allows County / Facility users to see name and billing addresses of called party with a convenient link to Google Maps allowing the user to pinpoint the address and see a "Street view" of the particular address associated to their phone, whether landline or cellphone.
9. Power Tolerance	The system is protected against and tolerant of line transients, momentary surges, and short duration drops	M	Y		All equipment is connected to a network-enabled Uninterruptable Power Supply (UPS) backup in order to prevent down-time during power failures or during conversion from power to generator.
10. Power Supply	The system is equipped with a back-up power supply for use during power failures.	P	Y		The UPS units allow backup power as well as for remote power management by our NOC and will power all inmate phones, via telephone line, with no additional power source for up to four (4) hours.
11. Automation	The system has fully automated inmate calling without the need for live operator intervention.	M	Y		The proposed system provides fully automated inmate calling and at no time will inmates communicate with a live operator.
12. Telephone Instruments	The system is capable of connecting to any standard telephone instrument with a hook switch, handset, and 12-button	M	Y		The proposed system is completely capable of connecting to all specified telephones listed herein. Several handset options are available.

**KEY:** M = Mandatory P = Preferred Y = Yes

No = No

Page 2 of 14



**PROFESSIONAL SERVICES AGREEMENT #: RC-000660****ATTACHMENT C - PHONE CALLING SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION		Y	N	COMMENTS
	keypad including the type of telephones specified herein.				
13. Tablet Devices	The system has the capability to connect to tablet devices for the purpose of phone calling.		Y		The proposed system has the capability to place a phone call via the telephone or a tablet for the purpose of phone calling.
14. Connectivity	The system is capable of connecting via a commercially available, reliable, high-speed local area network (LAN)	M	Y		The proposed system is capable of connecting via a commercially available LAN.
<b>C. INTEGRATIONS; INMATE INFORMATION &amp; IDENTIFICATION</b>					
15. Jail Management System Integration	The system provides an interface with the current Jail Management System (JMS) and capability to interface with future JMS and/or upgrades to be used to identify an inmate information.	M	Y		NCIC has existing interfaces built with numerous JMS companies and will be readily available to approach the current vendor to assist in this interface. NCIC will cover any costs associated with developing an interface with the County's current or future JMS provider.
16. Commissary and Vending System Integration	The system provides an interface with the current commissary/vending system and capability to interface with future system and/or upgrades to be used to identify an inmate account balances.	M	Y		NCIC has existing interfaces built with numerous commissary/vending systems and will be readily available to assist with this interface to ensure that critical data for the inmate account balances are imported through the interface with the County's current or future commissary/vending system.
17. Inmate Information and Identification	The system shall store: <ul style="list-style-type: none"> <li>• Last Name</li> <li>• First Name</li> <li>• Middle Name</li> <li>• Date of Birth (DOB)</li> <li>• Inmate Status (E.g., Active or released)</li> <li>• Living Unit (Dorm)</li> </ul>	M	Y		NCIC's proposed system is capable of storing all listed demographic information requested by the County.
<b>D. VOICE PROMPTS; ACKNOWLEDGEMENTS; MESSAGES</b>					

**KEY:** M = Mandatory P = Preferred Y = Yes

No = No

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660****ATTACHMENT C - PHONE CALLING SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION		Y	N	COMMENTS
18. Voice Prompts: English and Spanish	The system provides clear and concise voice prompts and messages in English and Spanish	M	Y		The proposed platform allows inmates to select the preferred language of either English or Spanish, by default. The prompts and greetings are pre-recorded in both English and Spanish.
19. Voice Prompts: Other Languages	The system provides clear and concise voice prompts and messages in other languages. Please list.	P	Y		The proposed system provides additional other languages as requested by the County to guide callers and the called party through the calling process. Following is a partial list of additional available languages: Arabic, Mandarin Chinese, Russian, Vietnamese, French, Tagalog (Filipino), Haitian Creole, German, Portuguese, Korean, Italian, Japanese, Urdu, Bengali, Punjabi, Polish, Dutch, Turkish, Thai, Romanian, Greek, Gujarati, Telugu, Malayalam, Kannada, Tamil, Marathi, Oriya (Odia), Assamese, Malay, Indonesian, Farsi (Persian), Pashto, Swahili, Amharic, Somali, Yoruba, Igbo, Hausa, Zulu, Afrikaans, Servo-Croatian, Czech, Slovak, Hungarian, Ukrainian, Lithuanian, Latvian.
20. Professional Recording	The system has professionally produced voice prompts given in short sentences with meaningful instructions.	M	Y		The proposed system provides professionally produced prompts with easy to follow instructions. These are fully customizable to meet the needs of the County.
21. Facility and Inmate Identification	The system announces to a called party, and any conferenced-in third party, they are receiving a call from a correctional facility. The inmate's recorded voice name also be announced.	M	Y		The proposed system provides pre-recorded customizable announcements to the called party including the name of the facility.
22. Inmate Acknowledgement	The system provides for and demands a proactive and documented response from an inmate which affirms that the inmate understands and accepts the conditions of the telephone call, e.g. "calls may be monitored and recorded."	P	Y		The proposed system provides both the inmate and / or the called party including "All calls are subject to monitoring and recording."
23. Call Recipient Acknowledgment	The system permits a call to be accepted only after a call recipient	M	Y		The inmate and called party cannot communicate until the called party has positively and actively accepted the initial call. Active

**KEY:** M = Mandatory P = Preferred Y = Yes

No = No

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660****ATTACHMENT C - PHONE CALLING SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION		Y	N	COMMENTS
	acknowledges receipt by dialing a recognized digit on a touch-tone telephone.				acceptance requires that the called party press a "1" on their keypad.
24. Signal Line Noises	The system must distinguish signal from line noises such as "pops" or "clicks" (i.e. answering machines). Voice recognition is not an acceptable form of acceptance.	M	Y		The proposed system uses a sophisticated answer detection algorithm which can distinguish between standard and artificial telephone tones, standard SIT tones, busy signals and even answering machines / voicemail to ensure accurate call answering, prevent erroneous billing and subsequent complaints.
25. Editing Authority	The system allows editing authority over all system messages and the ability to add its own messages.	M	Y		The proposed system allows for editing authority by users with appropriate permissions, including customizable messages that can be broadcast to specific inmates or the entire population.
26. Prerecorded Messages	The system allows for the facility to configure pre-recorded messages on paid and free calls.	P	Y		The proposed system allows pre-recorded and fully customizable messages at no cost to the County.
<b>E. SYSTEM CONTROLS</b>					
27. On/off Control	The system allows the facility control of the system to turn specific phones on or off at any time.	M	Y		NCIC's proposed system features include manual and automated on/off controls allowing authorized users to shut down individual telephones, blocks of telephones or the entire telephone system. The system can be manually switched on/off via the secured web page using any computer with internet access or by manual switches located in any area designated (Demarcation location, central control center, selected housing units, selected telephone) by the authorized personnel.
28. Emergency Disable	The system allows the facility to shut down/disable the inmate phone system as needed for emergencies or other purposes.	M	Y		The system allows users the ability to shutdown a complete facility, groups of phones or individual phones, via keystroke. Calls can either be terminated immediately or after any current call is finished.
29. Flexible Control	The system allows flexible control over the operating hours of each phone, with the ability to control phones or groups of phones with differing schedules.	M	Y		The proposed systems provide the ability to configure facility, inmates (or specific phones) to particular call duration/time limits, provides optional warning announcement for remaining time/security measures, calling patterns and time of day/on-off. Configurations are established during installation and can be

**KEY:** M = Mandatory P = Preferred Y = Yes

No = No

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660****ATTACHMENT C - PHONE CALLING SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION		Y	N	COMMENTS
					easily adjusted to meet the unique requirements of the County.
30. Time Limits – Free Calls	The system allows for the facility to set time limits on calls for free calls.	M	Y		The proposed system allows the option to set time limits on all calls, including free calls.
31. Time Limits – Paid Calls	The system allows for the facility to set time limits on calls for paid calls.	M	Y		The proposed system allows the option to set time limits for all paid calls.
32. Time Limits – Specific Numbers	The system allows the facility to limit the call time to specific numbers.	P	Y		The proposed system allows the option to set time limits for all paid calls.
33. Free and Non-recorded Calls	The system allows the facility to configure phone numbers that will be free and not be recorded for the purpose of protecting privileged communication.	M	Y		The proposed system allows the option to configure specific numbers as free and non-recorded for privileged communication purposes. NCIC is one of the only large inmate telephone providers that has not been a party to legal proceedings for mis-handling attorney-client (privileged) phone calls.
34. Blocked and Allowed Numbers	The system allows phone numbers to be blocked or allowed by phone, living unit, and inmate.	P	Y		The proposed system allows for numbers to be blocked or allowed by phone, living unit, and / or inmate.
35. Restricted Numbers	The system allows for the regulation or restriction of calls to numbers including but not limited to, e.g., 800, 888, and 900.	P	Y		The proposed system prohibits access to 800, 888, and 900 type services. There is a database of blocked numbers which is maintained by NCIC. A small but representative sample of the blocked number database includes 800, 888, 877, 900, 700, 911, 411, 311, 0, 950, 976, 555-1212 and 10-10xxx numbers. This database of blocked numbers is updated regularly.
36. Threshold Blocked Numbers	The system allows the facility to block or restrict phone numbers based on an individual inmate's attempted or completed calls (i.e., a predefined calling frequency threshold).	P	Y		The proposed system allows the facility to block frequently called numbers. A standard feature that is available includes use of an inmate's "Allowed Numbers" list that works in conjunction with the blocked call list; if a phone number has been set to "block all" no inmate at the Facility will be able to dial the phone number under any circumstances. Likewise, a phone number can be blocked for a specific inmate but allowed for others.
37. Limit Alerts	The system alerts users that have exceeded any limits before terminating calls.	M	Y		The proposed system provides a notification to both the inmate and the called party one minute ahead of the maximum allowed

**KEY:** M = Mandatory P = Preferred Y = Yes

No = No

ATTACHMENT C - PHONE CALLING SYSTEM REQUIREMENTS AND QUESTIONNAIRE

FEATURE	FUNCTION / DESCRIPTION		Y	N	COMMENTS
					time. This notification/warning is configurable based on the County's need(s).
<b>F. REPORTS; INVESTIGATIVE AND ANALYTICAL TOOLS; ALERTS</b>					
38. Standard Report	<p>The system can produce a consolidated standard report that includes, at a minimum, the following:</p> <ul style="list-style-type: none"> <li>• Time and date of each call</li> <li>• Name of inmate</li> <li>• PIN of caller</li> <li>• Phone location</li> <li>• Phone number dialed</li> <li>• Duration of the call</li> <li>• Amount charged (to the receiver of the call, debit card, or inmate's account)</li> </ul>	M	Y		The proposed system can produce consolidated standard report(s). The Call History Reporting page allows for searching, reporting, and sorting requirements. Call History reports allow searching by time/date, inmate name, phone location, complete and partial destination numbers, by call disposition such as answering machine, no answer, busy line, call denied by caller, call blocked by caller, invalid PIN (when inmates are trying to hack PINs), invalid destination number and over 20 more options. The Call Detail lists all calls placed/accepted in addition the report lists the date, time, and duration of all calls, local, or long distance and even calls to commissary.
39. Disconnected Call Report	The system can produce a report that lists all disconnected calls.	M	Y		The proposed system provides reports noting disconnected calls.
40. Ad Hoc Reports	The system provides the ability to generate ad hoc reports/queries via user-defined reports within the system boundaries.	M	Y		The proposed system produces ad hoc reports allowing for individuals to filter through reports seamlessly
41. Security Report	The system produces a security report, which includes all users of the system and their rights, excluding passwords.	P	Y		The proposed system provides a security report to authorized users for all users and their rights.
42. Financial and Utilization Reports	The system provides a method for facility staff to view financial and system utilization reports.	P	Y		At any time, the appropriate County personnel can access the same back-end web-based traffic reports that NCIC uses on a monthly basis to complete our commission calculations. Raw, unaltered Call Detail Records able to be accessed at any time, showing the details regarding all completed calls.

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660**

**ATTACHMENT C - PHONE CALLING SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION		Y	N	COMMENTS
					Monthly reports provided are detailed, yet easy to understand. A monthly Revenue/Commission report will be provided that clearly breaks down the total amount of revenue generated, split out by Call Type (Local, Intralata/Intrastate, Interlata/Intrastate, Interlata/Interstate, International) and Bill Type (Collect, Pre-Paid Collect, Debit, Pre-Paid Cards (if applicable). All Revenue/Commission reporting is able to be verified and validated through the monthly Call Detail Records which are able to be easily exported directly from the web-based platform at any time and can be scheduled to be sent at pre-configured intervals (such as at the beginning of each month, for the prior traffic month).
43. Schedule Reports	The system provides the ability to schedule reports to run on a regular basis and be distributed to designated parties electronically.	P	Y		The proposed system can generate daily, monthly, weekly reports and if requested by Ramsey County, these reports can be automated and delivered to designated authorized Ramsey County officials.
44. Data Export	The system provides the ability to export (extract) pre-defined set(s) of data.	M	Y		The proposed system allows a myriad of exportable pre-defined set(s) of data in order to provide required reports for the County.
45. Investigative and Analytical Tools	The system has investigative and analytical tools.	M	Y		The proposed system includes a range of powerful investigative reports as standard, including Commonly Called Numbers, Frequently Called Numbers, Seven Degrees of Separation, Visual Link Analysis, PIN Abuse Report, Multi-Speaker Report, etc. The system also includes investigative and analytical tools such as affiliations between inmates and destination numbers, innovative recording management, reporting capabilities, and alerts to calls of interest either prior to a call being connected or while a call is in progress.
46. Alerts	The system alerts or notifies an investigator when individual criteria are set by an investigator (e.g., an inmate places a phone call to a certain number, etc.).	M	Y		The proposed system is completely web-based, offering a powerful features providing the Authorized User access to the live-monitoring, investigative alerts, as well as other features such as search, reporting and sorting features to easily find any completed or attempted call. The system shows all live/current calls under the Live Monitoring tab and allows the authorized user to easily single-click on each call to hear the active call. Multiple users can

**KEY:** M = Mandatory P = Preferred Y = Yes

No = No



**PROFESSIONAL SERVICES AGREEMENT #: RC-000660**

**ATTACHMENT C - PHONE CALLING SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION		Y	N	COMMENTS
					monitor simultaneously, without affecting the performance of the system, and without the parties on the call being aware of the monitoring. Live calls can also be terminated in progress as needed.
47. Crime Reporting	The system has a method for inmates to confidentially report crimes or other incidents via phone call to a recorded message system.	M	Y		The proposed system can be configured to allow extra digits to specified dialed numbers as is the case with speed dials to specific numbers and designated voicemails for services such as PREA, Crime Tips, grievances, Public Defender, sexual assault/harassment, medical requests, etc. All such numbers will be configured at no cost to the County.
48. Voice Certification	The system uses voice certification for enrollment, call initiation, and security.	P	Y		Our Voice Biometric System (VBS) is capable of scanning voice prints and accurately identifying them as specific inmates, on a continuous automated level. This is performed automatically after each communication print is captured, meaning that our VBS is actively refining the collected data to verify and improve the accuracy of identified voice prints. Since our VBS does not require a manual enrollment of a person's voice at the time of the intake/booking process, Facility staff will be able to focus on other duties without having to be involved in a cumbersome voice registration process - with the added benefit being that inmates are not aware that the VBS is in operation at the facility.  Investigators will have the ability to search for any specific inmates of interest to determine any cases of PIN theft or sharing during a selected period of time. Our reporting system showcases the individual's PIN that was used to place a phone call and the detected voice that was found, side by side.
49. Voice Biometrics	The system uses voice biometrics to analyze completed calls for investigative purposes.	M	Y		
G. MONITORING & RECORDING; VIEWING					
50. Monitoring/Recording	The system provides a web-based application for users to manage monitoring, recording, and general operations including setting alerts and live-monitoring of calls and disconnecting calls.	M	Y		The proposed system is completely web-based, offering a powerful features providing the Authorized User access to the live-monitoring, investigative alerts, as well as other features such as search, reporting and sorting features to easily find any completed or attempted call. The system shows all live/current calls under the Live Monitoring tab and allows the authorized user to easily

**KEY:** M = Mandatory P = Preferred Y = Yes

No = No

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660****ATTACHMENT C - PHONE CALLING SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION		Y	N	COMMENTS
					single-click on each call to hear the active call. Multiple users can monitor simultaneously, without affecting the performance of the system, and without the parties on the call being aware of the monitoring. Live calls can also be terminated in progress as needed.
51. Detailed Monitoring Capability	The system provides remote viewing and monitoring with detailed real-time call monitoring and disconnect.	M	Y		NCIC's proposed system is a fully centralized, web-based Inmate Telephone System, written using the newest technology in web tools. The system is compatible with any Windows-based computer and various web browsers including Internet Explorer, Chrome (recommended), Safari and Firefox. All functions of the system are accessible 24/7/365 via any internet-enabled computer, tablet or smart-phone allowing authorized users access throughout the platform based on their level of access authorization.
52. Call Details	The system offers remote monitoring with call detail viewing capability and silent monitoring of selected conversations.	M	Y		Multiple users can simultaneously and covertly monitor all calls, both on site and remotely, without affecting the ability of the system to record calls, or the quality of the call audio for the sessions participants (inmate and called party/visitor). Live Monitoring on the platform allows for all recorded calls to be monitored and activity to be viewed in real-time. The Live Monitoring feature allows the authorized user to sort monitoring/call history by a large variety of search criteria. Authorized Users can single-click on each call to monitor the active call. Live monitoring information can be viewed chronologically and sorted in real time. The information is viewable through the system's Live Monitoring tab and Authorized Users will have the ability to pause a live recording as well as playing the call from the beginning.
53. Real-time Monitoring Alert	The system forwards in progress calls to an assigned person/preprogrammed phone numbers for real-time monitoring. Calls must be able to be selected by using an inmate's name or dialed number.	P	Y		The proposed system features an Alert system ("Hot Number Alerts") whereby alerts can be sent via email, text, or phone call, allowing investigators to receive real-time notifications and covertly listen to calls of interest. The proposed system alerts investigators to calls of interest either prior to a call being connected or while a call is in progress (this is configurable based on the needs of the Facility) so that investigators can listen to

**KEY:** M = Mandatory P = Preferred Y = Yes

No = No

Page 10 of 14



**PROFESSIONAL SERVICES AGREEMENT #: RC-000660**

**ATTACHMENT C - PHONE CALLING SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION		Y	N	COMMENTS
					and/or approve the call. Authorized Users can configure alert settings in the Alerts tab which allows the user to set up an alert based on a particular phone number, a particular inmate, particular inmate phone, or other variables. The user can receive an alert by email, text to cell phone, a phone call or the user can select all options.
54. User Activity Reports	The system provides reports of all user activity.	M	Y		All page views and modifications to the database are logged in to provide an audit trail in our User Logging report. With these checks in place, any views or changes are logged with the user's login information, timestamp and their location allowing the change to be tracked back to the user – in case any actions taken need to be reversed. All information is stored in multiple geographically separate, redundant locations to ensure 100% reliability.
55. In Progress Privileged Calls	The system does not allow live calls to be monitored that are subject to privileged communications.	M	Y		The proposed system does not permit monitoring or recording of a call made from any inmate telephone to any restricted or privileged number, such as attorney-client privilege.
56. Active Scan Mode	The system offers a scan mode of all active trunks and capability of recording or monitoring calls based on dialed number, inmate, or location.	M	Y		The proposed system offers a scan mode feature of all active trunks and the capability of recording/monitoring based on dialed / destination number, inmate, and/or location.
<b>H. RETENTION &amp; STORAGE</b>					
57. Back-up Capability	The system provides back-up provision and equipment to allow for retention of call detail and recordings.	M	Y		The proposed system is a fully integrated, custom-designed system comprised of both onsite and offsite network components to provide the utmost in network redundancy and higher security than standard cloud-based systems. All components for placing calls / video sessions, live monitoring, recording, and data collections are located in high security, fully redundant locations in Texas, with near real-time back up on NCICloud storage, designed using CEPH server clusters in a minimum of two, diverse locations. Each device endpoint is verified with Amazon Web Service's CrowdStrike and when approved, will be managed

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660**

**ATTACHMENT C - PHONE CALLING SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION		Y	N	COMMENTS
					by our communications platforms which are designed to host the most sensitive data, and address the most stringent security and PCI compliance requirements. All data is stored in a minimum of 2 separate locations and encrypted in AWS' proprietary encryption code. All records and system data are backed up in real-time and are immediately copied to NCICloud for off-site redundancy. Access to NCICloud services is limited to vetted account holders that must be held by our IT directors.
58. Storage	<p>The system provides for storage of call detail information as follows:</p> <ul style="list-style-type: none"> <li>Storage capacity for the entire length of the contract; call records are to include recorded conversations</li> <li>Maintain all recordings for a period of seven years after completion of the contract</li> <li>Report of stored activity</li> </ul>	M	Y		<u>All recordings are stored for the life of the contract (including any extensions) and longer up to a period of seven (7) years, or longer if required, and are available online for downloading at any time.</u> Retention of call recordings is completely configurable, based on the needs of Ramsey County.
59. Non-delete	The system will not allow a user to edit or delete a call.	M	Y		All records and system data are backed up in real-time and are immediately copied to NCICloud for off-site redundancy and cannot be deleted.
<b>I. USERS ADMINISTRATION</b>					
60. Roles	The system provides the ability to specify the role of each user (e.g., system administrator, supervisor, investigator).	M	Y		The proposed system establishes County personnel via the User Tab and accompanying detail settings. Once County officials provide authorization for staff / personnel, the individual is added based on level of authority. The proposed system supports multiple levels of password protected access, so all Authorized Users only have access based on their individual level of authority, and do not have access to the entire functionality of the systems.
61. Password Reset	The system provides the ability to reset passwords at the facility.	M	Y		The proposed system provides the ability to reset password by Authorized Users with proper permissions.

**KEY:** M = Mandatory P = Preferred Y = Yes

No = No

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660**

**ATTACHMENT C - PHONE CALLING SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION		Y	N	COMMENTS
62. Inactivity	The system, upon detection of inactivity, prevents further access to the system and timeouts.	M	Y		The proposed system times out after 20 minutes of inactivity and can be adjusted to accommodate the County's requirements.
<b>J. SEARCH AND DOWNLOADING OF CALLS</b>					
63. Search Feature	The system has a robust search feature that includes indexing of calls by user, date, location, and number call.	M	Y		The proposed system provides Call History tab with a powerful search feature that returns data based on calls by user, date, location, number called, time, and multiple other details. This powerful search feature is customizable and provided at no cost to the County.
64. Advanced Search Feature	The system has an advanced search feature that includes indexing of calls by keywords, specific areas of the call, or other criteria.	P	Y		<p>The proposed system provides Call History tab with a powerful search feature that returns data based on calls by keywords utilizing our Transcription and Keyword Searching feature. This powerful tool for correctional personnel and investigators helps correctional and law enforcement agencies gather actionable intelligence, helping prevent and solve more crime. NCIC's Transcription acts as a 'Workforce Multiplier' by alerting facility personnel and investigators to items of interest within recorded inmate conversations which may have otherwise go undetected. Additionally, it is an integrated part of the Inmate Call Engine ('ICE') investigative suite, with no separate login or any special software required. From directly with the ICE call player, investigators can simply click on the Transcription tab to access the transcribed conversation which has automatically been processed and is available immediately.</p> <p>The ICE call player transcribes sentence by sentence throughout the duration of the conversation, separating out the Destination and the Inmate sides of the conversation. By simply clicking anywhere in the transcribed text, the ICE call player will take the listener to that specific point of the call.</p> <p>If preferred by the investigator, the Transcription feature also offers the 'Higher Contrast' option which provides an alternative</p>

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660****ATTACHMENT C - PHONE CALLING SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION		Y	N	COMMENTS
					<p>view with more definition and greater distinction between the Destination and the Inmate sides of the conversation.</p> <p>NCIC's Transcription Service also allows for keyword detection, which automatically sifts through every call placed from your facility to detect keywords of interest. Investigators can search for multiple keywords of interest by simply entering them into the Keyword field (separated by a space).</p> <p>Investigators have the option of setting up automated / pre-scheduled Keyword Detection reports, which can be seamlessly delivered to their inbox at times / intervals specified by them.</p>
65. Download Format	The system allows individual or a selected number of calls to be downloaded in a universal format (e.g., wav, mp3, etc.) and a system protected format with a system supported software player.	M	Y		All recorded calls are available for retrieval/review for the duration of the Agreement including any renewals (or for as long as is specified by the County). All call recordings and associated data can be easily shared with other authorized recipients, downloadable to various forms of removable media, etc. Users can easily manage downloaded recordings for saving in .zip files, ISO files, .wav formats and .mp3 formats for listening on all devices, PC's, Macs, tablets, and smart phones. The user can also burn the files to a CD or DVD or ZIP file. Windows XP or newer has the capability to burn disks built in. Email access for outside users is also available, based on the parameters set by Ramsey County.
66. Download Media	The system allows downloads of calls to commonly available USB flash drives and DVD/CD discs.	M	Y		

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
<b>A. COMPLIANCE</b>					
1. FCC Compliance / Data Privacy	The system is compliant with all federal, state, and local laws, statutes, ordinances, rules, regulations, and standards for data privacy and the Federal Communications Commission (FCC).	M	Y		NCIC is fully compliant with Federal, State or local laws, statutes, etc., and all equipment meets or exceeds applicable FCC licensing, rules and certification regulations. FCC FRN# and other certification-related documents are available upon request.
2. ADA Compliance	The system is compliant with the Americans with Disability Act (ADA) and accessible to hard of hearing individuals.	M	Y		NCIC's proposed system is fully compliant with the Americans with Disability Act. VRS is being offered.
3. FBI CJIS and BCA MNJIS Compliance	The Contractor and system is compliant with federal and state laws and regulations, including the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) and the Minnesota Bureau of Criminal Apprehension (BCA) Minnesota Justice Information Services (MNJIS).	M	Y		NCIC and the proposed system is compliant with all applicable Federal and State laws and regulations associated with the FBI, CJIS, BCA and MNJIS.
4. Minnesota Government Data Practices Act	The Contractor and system is compliant with the Minnesota Government Data Practices Act.	M	Y		NCIC's proposed system is compliant with the Minnesota Government Data Practices Act.
<b>B. GENERAL TECHNICAL</b>					
5.	The system shall be web based and not require proprietary software or hardware for visitors using their home computers.	M	Y		The proposed system is fully web-based requiring no additional software or hardware.
6.	The system uses Windows Active directory for user authentication.	P		N	The proposed solution includes a secure User Password System that provides Ramsey County with complete control over who is interacting with the system. The User Password System is based on a Username (email)

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
					and Password that can provide a customized level of access for each user, based on their required level of access and daily duties. Authorized administrators can easily update user access rights on an as-needed basis, and add/remove users as needed.
7.	The system shall automatically assign the inmate's booking number as the primary key for each inmate.	P	Y		The proposed system provides for automatically assigned booking number as the primary key for the inmate and associated details are to be automatically loaded when interfaced with most JMS/Booking systems via a simple XML interface.
8.	The system has both public and internal graphical user interface (GUI) that will, at a minimum, the following:				
a.	The system must register different types of users for browser based video visiting.	P	Y		The proposed system accommodates multiple criteria for registering different types of users.
b.	The system is able to process payments by participants for remote visits.	M	Y		The proposed system provides management of remote visit payments and remote VVS sessions can be billed on a per-minute basis.
c.	The system has the ability to post and regularly update inmate and visitation information and rules.	P	Y		The proposed system is fully capable of providing updated inmate and visitation information and rules. Additional updates are able to be provided upon request.

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
d.	The system's communications must be available in multiple languages.	M	Y		NCIC's fully automated system provides inmates and the called party the option to select the desired language (English, Spanish or other languages as requested by the County) to guide callers and the called party through the calling process. Currently, English, and Spanish prompts are available by default and NCIC will commit to implementing any additional required languages into the System within thirty (30) days of request.
e.	The system has the ability to initiate on-site visitations conducted at the county without requirement payment.	P	Y		The proposed system is able to be configured to allow visitations without payment, if required.
f.	The system must allow other related information to be posted on the site.	P	Y		The proposed system is able to provide additional information and details for posting on site.
10.	The system has high definition video streaming capabilities.	P	Y		The proposed system offers high-definition video streaming capabilities.
11.	The system must perform at a rate of up to thirty (30) frames per second for 2-party visitations.	P	Y		NCIC prefers to allow 3mbps for each VVS station since both sides of the visit connect independently. NCIC always facilitates ample bandwidth for each VVS deployment based on the specifics of each deployment, but in all cases the amount of bandwidth is ample to accommodate video visitation



FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
					even if all VVS kiosks in the Facility are being used concurrently (which rarely happens).
12.	The system is able to white-list IP addresses.	P	Y		The proposed VVS is capable of white-listing specific user's IP addresses should the County require this function.
13.	The system has a web-enabled Dashboard for visitation	P	Y		The proposed solution is inclusive of a dashboard feature that can be configured to display various information, directly through the web-based platform.
14.	The system is able to furnish capabilities for the administrator of the system, at a minimum, the following:				
a.	Setup visitations designated by user type (standard or professional) with present conditions.	P	Y		The proposed VVS is able to designate visitations based on user type. The proposed VVS has been developed with customizability and configurability based on the unique needs and preferences of each agency.
b.	Begin and end meetings at will (Ad hoc visits).	P	Y		The proposed system allows for "at will" start and end times.
c.	Set a time duration for visitations that will automatically end them after the designated time.	P	Y		The proposed system allows for automated time durations ending visits at designated time.
d.	Blind monitor non-confidential visits so the participants are not aware of monitoring.	P	Y		The proposed system provides the blind monitor feature allowing covert sessions without participants aware.



FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
15.	The system shall be equipped with an automatic default mode that returns the system to normal operation without human intervention in case of a power failure.	P	Y		All equipment is connected to a network-enabled Uninterruptible Power Supply (UPS) backup in order to prevent down-time during power failures or conversations from power to generator. The UPS units allow for remote power management for up to four (4) hours.
16.	The system has the capability to provide videophone and video relay service calling for deaf or hard of hearing inmates.	P	Y		NCIC offers, as standard, access to the leading Purple Video Relay System ( <a href="https://www.purplevrs.com/">https://www.purplevrs.com/</a> ). NCIC and Purple have worked closely to introduce a fully secure, locked-down and web-based version of the Purple VRS which NCIC now offers on both our correctional-grade tablets and wall-mounted kiosks. Access to the Purple VRS application is restricted to only qualifying deaf or hearing-impaired inmates, so as to prevent abuse by other non-qualifying inmates.
<b>C. INTEGRATIONS; INMATE INFORMATION &amp; IDENTIFICATION</b>					
16. Jail Management System Integration	The system provides an interface with the current Jail Management System (JMS) and capability to interface with future JMS and/or upgrades to be used to identify inmate information.	M	Y		NCIC has existing interfaces built with numerous JMS companies and will be readily available to approach the current vendor to assist in this interface for identification of inmate information.

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
17. Commissary and Vending System Integration	The system provides an interface and capability to interface with future proposed system and/or upgrades to be used to identify inmate account balances.	M	Y		The proposed system will allow identification of inmate account balances.
<b>D. SECURITY CONTROLS</b>					
18.	The system provides and supports table driven security. This security schema is able to allow for a separation of access to functions including, but not limited to user id, type of user, location, transactions, etc.	P	Y		The proposed system provides such security levels including user id, location, etc. and the security schema multiple criteria, as listed.
19.	They system provides security at the field level. The system allows users to specify, using reference tables, the fields requiring security.	P	Y		The proposed system is entirely encrypted to ensure that all aspects are secure from unauthorized users and external threats. Should the County require additional security functions, we are capable of configuring those through the system's back end.
20.	The system provides security at the screen and transaction level.	P	Y		The proposed system provides screen and transaction level security.
21.	The system provides security to ad hoc queries to protect sensitive data.	P	Y		The proposed system provides security to ad hoc queries to protect sensitive data.
22.	The system provides security violation reports.	P	Y		The proposed system's security measures were configured using strong encryption practices resulting in the restriction of CJI access to those who are not in compliance with CJIS and BCA policies. If there are security violations, NCIC is alerted of such threats and will have detailed reports on the attack.

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
23.	The system will be permissions based to allow different users to have access to different privileges in the system as defined by the county.	P	Y		The proposed system is a permissions-based system requiring username / password in order to access. User permissions can be configured at a very granular lever and based on specific roles and job functions of each user.
24.	The system provides an automatic timeout for the application requiring a password to be re-entered.	P	Y		The proposed system provides automatic timeout and once in motion, login details are required to log back into the system.
25.	The system allows the facility to reset passwords upon identification.	P	Y		The proposed system allows authorized facility staff / personnel to reset passwords in this manner.
<b>E. REGISTRATION CONTROLS</b>					
26.	The system allows for the facility the ability to schedule specific visits to be recorded based on the inmate, visitor, or both via the web-based scheduling system.	P	Y		The proposed system, by default, allows for facility to schedule video sessions to ensure proper use of the video stations through the web-based access.
27.	The system allows for the facility to enter visitation appointments for visitors.	P	Y		Authorized users at Ramsey County are able to enter visitation appointments for visitors.
28.	The system allows for the facility to enter ad-hoc visits for any type of visit (professional or social) upon approval with no delay.	P	Y		The Facility is able to enter ad-hoc visits for multiple types of visits, including those listed here.

ATTACHMENT D - VIDEO VISITATION SYSTEM REQUIREMENTS AND QUESTIONNAIRE

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
29.	The system allows for the facility to approve registration and give authorization.	P	Y		The system provides approval and authorizations to the facility.
30.	The system allows for the visitor to register to visit more than one (1) inmate per day.	P	Y		The system provides registration for multiple visits to multiple inmates.
31.	The system allows for multiple visitors in one (1) visitation session.	P	Y		By default at most correctional agencies, NCIC does not allow more than 2 parties in visitation sessions for security purposes and to avoid three-way party communications. If this is a feature required by the County, NCIC has already began to develop this type of conferencing for special court/judge/attorney conferencing and can provide Ramsey County with this type of visitation as needed.
32.	The system allows for positive identification of visitors through the use of passwords and picture of driver's license or other government issued ID for authentication.	P	Y		The proposed system utilizes the method(s) listed for visitor identification and authentication.
33.	The system has the ability to reference blocked list for visitors.	P	Y		The proposed system has the ability to determine blocked list(s) for visitors.
34.	The system has the ability for positive identification of inmates through use of PIN, barcode, or other reliable identification means.	P	Y		The proposed system readily authorizes an inmate through use of PIN and other identification means (booking number, barcode, etc.). Additionally, identification can be authenticated through information mirrored by the

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
					JMS system at the Facility such as Social Security Number, FBI number, etc.
<b>F. SCHEDULING CONTROLS</b>					
35.	The system has a scheduling/calendaring module that will, at a minimum, the following:				
a.	Block out access to station times that are already scheduled.	P	Y		The proposed system allows Facility personnel to block or schedule a “no visitations” event as well as apply ‘block outs’ either at a global level, for specific housing areas, by individual visitor, or by individual inmate.
b.	Allow scheduling of visits only on terminals available at the requested time and in the requested location.	P	Y		The proposed system allows scheduling of visits only on available terminals, times, location.
c.	Allow online scheduling.	P	Y		The proposed system is web-based allowing online scheduling.
d.	Provide the ability for an inmate to decline or accept visits.	P	Y		The option to accept or decline visitation is available in the proposed system.
36.	The system allows the system administrator to, at a minimum, the following:				
a.	Review visitation requests made in a specific time frame.	P	Y		By default, the proposed system allows for inmates to schedule video visitation sessions ahead of time to ensure proper use of the video stations but is completely customizable if required by Customer.

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
b.	View a list of scheduled visits for specific stations or all stations.	P	Y		The proposed system provides the specified visitation for all stations or an individual station.
c.	Cancel scheduled visitation sessions and allow selection of the reason for the cancellation, which will be posted to the system database.	P	Y		The proposed system provides for cancellation and reason. This will be posted in the system.
d.	Ability to cancel visits based on inmate, station, housing unit or time frame.	P	Y		The proposed system allows administrators to cancel visits based on a specific inmate, station, housing units, or time frames. Identifying notes can be applied to cancelled / restricted visits that allow other users in the system to see why these restrictions have been implemented.
e.	Move visits when necessary.	P	Y		The proposed system allows users to move visits and reschedule them for a later time when necessary.
f.	Notify public visitors of an intervention made to a scheduled visit.	P	Y		The proposed system provides email/text notifications to visitors in the event a visit has been rescheduled or cancelled.
37.	The system tracks an inmate visitation status and restricts a visitation automatically, if the inmate's status does not allow for visitation.	P	Y		The proposed system features tracking restrictions for an inmate not allowed to receive visit(s). Additionally, the scheduler is built with sophisticated tracking to prevent scheduling over any restrictions.

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
38.	The system automatically cancels the visit if the inmate's status has changed or inmate is released.	P	Y		The proposed system automatically updates according to inmate releases and change in status.
39.	The system sends e-mail and voicemail cancellation notifications to the visitor if the scheduled visit has been cancelled to include a reason if specified.	P	Y		The proposed system sends notification of the cancellation to the visitor in the event of such a change.
40.	The system shall reflect all movement of inmates in conjunction with scheduled appointments. The system shall notify scheduled visitor when visit has been canceled due to inmate movement and a resource is not available to maintain schedule	P	Y		The proposed system provides various customizable criteria to reflect movement, notify visitors, and more, according to the requirements of Ramsey County.
41.	The system provides a methodology to provide notification to the inmate and housing unit officer of an approved, upcoming video visitation. Notification must provide the inmate name, date, time and visitor name.	P	Y		The proposed system provides this feature. The inmate information is customizable to provide name, date, time and visitor name, and other requested fields of information may be available upon request.
42.	The system provides a designation of general visitors and attorney / professional visitors.	P	Y		The proposed system allows for such designations as general, professional, and more, allowing control and flexibility for the Facility administration to manage.
43.	The system allows for the visitor the ability to cancel a visit and the facility shall be notified upon cancellation.	P	Y		The proposed system allows for an authorized visitor the ability to cancel which will provide notification to the facility.
44.	The system prevents overbooking of visitation resources.	P	Y		The proposed system's scheduler is built with sophistication features recognizing which kiosks are

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
					available, how many visits and any changes as they occur in real-time. This prevents the occurrence of scheduling conflicts and overbooking.
45.	The system provides time blocks for housing units that can be changed by facility staff as necessary.	P	Y		The proposed system provides time blocks at a global level, for specific housing areas, by visitor, by inmate, or kiosk and is accessible by authorized facility staff to apply changes as needed.
46.	The system provides time blocks that can be altered for holiday visitations to allow more visits for shorter or varied time periods.	P	Y		The proposed system provides such customization to allow altered time blocks based on the needs of Ramsey County, including Holiday visitations.
47.	The system provides a web-based visitor check-in module to assist the user in the visitation process.	P	Y		The proposed system is a proprietary, centralized, web-based application that allows for visitor check-in through any internet connected device, including desktop, laptop, table or mobile device.
48.	The system initiates and finalizes visits by checking visitors in/out after visit is complete.	P	Y		The proposed system provides finalization of check in / check out on visits.
49.	The system tracks incomplete visits.	P	Y		The scheduler's feature includes built in tracking that is able to provide information on incomplete visits.
<b>G. RECORDING AND MONITORING</b>					
50.	The system provides for real-time monitoring and interruption of visitations from any PC on the network	M	Y		The proposed system provides the Live Monitoring feature for



FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
	according to user security level.				authorized users. Additionally, the authorized user / staff are able to send warning messages to either party (or both parties) on the visitation session, in the event of unacceptable behavior.
51.	The system allows browser-based video conferencing between inmates and their visitors without the visitors having to download any proprietary software onto their computers to conduct the visit, other than one of the standard browsers.	M	Y		The proposed system is a proprietary, centralized, web-based application that allows for both on-site and off-site visitation, through a secure internet connection. NCIC recommend the use of Google Chrome (preferred) or Firefox, and also such browsers as Edge, or even Internet Explorer.
52.	The system provides a browser-based video visitation with VOIP.	P	Y		The proposed system deploys a platform that utilizes VoIP technology.
53.	The system provides a Real-time viewing of the audio and video visitations simultaneously and allows the user the ability to define requirements.	P	Y		The proposed system provides real-time viewing simultaneously and covertly by multiple users without affecting the ability or quality of the session.
54.	The system shall be capable of scanning the total number of active visits.	P	Y		The proposed system currently scans all active visits and limits 14 live visits to be viewed per page in order to prevent smaller images and icons. If there is a visit of interest, investigators may pin that visit to their screen so that it follows them to the next page of visits.

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
55.	The system provides the ability to interrupt the visit.	P	Y		The proposed system provides for visit interruptions.
56.	The system provides the ability to cancel the visit.	P	Y		As has been stated, yes, the system provides cancelation capabilities.
57.	The system provides the ability to start recording the visit.	P	Y		By default, unless customized according to specific County requirements, the proposed system immediately begins recording all visits with the exception of those set as privileged or indicated as do not record.
58.	The system provides the ability to turn recording off and on to facilitate legal visitation due to attorney / client privilege.	P	Y		Please refer to immediate previous response indication the exception(s) for attorney / client privilege.
59.	The system provides the ability of recording any and all inmate / visitor connection combinations.	P	Y		There is no limitation on the number of inmate units or video sessions that can be recorded.
60.	The system notifies both the inmate and visitor that visits are subject to monitoring and/or recording.	M	Y		The proposed system provides the warning statement for all calls, except attorney / client privilege, or others based on Ramsey County requirements. Both the caller and the called-party hear the warning statement that the call is subject to monitoring and/or recording.
61.	The system provides display notifications on the screens of visitors/inmates in both English and Spanish that their visits are being monitored and recorded. Other languages available should be listed in response.	M	Y		The proposed system provides English and Spanish by default. Additional other languages are available for notifications and information upon request.

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
62.	The system provides fully synchronized recordings with inmate and visitor side-by-side in a single file and system must utilize a real-time data and time stamp with proper security features to prevent tampering of the recording time/date. Further, the time and date stamp must be on the inmate's and visitor's captured video stream to provide the highest level of integrity. A single time and date stamp is not acceptable.	P	Y		The proposed system provides real-time side - by - side recordings that are securely encrypted with the appropriate, unique checksum value, date and time stamped, and stored along with the data associated with that specific session. These features maintain the integrity of each session to support the chain of evidence and ensure that our data and recordings withstand the highest degree of judicial scrutiny.
63.	The system records and stores basic visitation data such as inmate, date and time of visit, start and end times, persons who visited and location of visits for all visits.	M	Y		The proposed system records and stores all listed data and additional customization is available upon the County's request.
64.	The system allows authorized users (i.e., investigators, internal affairs, etc.) to query pending visits on specific victors or inmates and select such pending visitations for recordings.	P	Y		The proposed system provides authorized users the capability to query upcoming schedules and recordings via multiple criteria including pending visitations.
65.	The system stores all recorded visits for a minimum of sixty (60) days.	M	Y		The proposed system's recordings are stored for the life of the contract and any extensions. Storage retention is completely configurable based on the requirements of Ramsey County.
66.	The system allows authorized users to be able to stream the video visitation session on multiple types of devices.	M	Y		The proposed system is web-based, giving authorized users the ability to access video

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
					visitation sessions through a computer (laptop or PC), tablet, or smart phone.
67.	The system is software based and does not require third party video conferencing equipment to record and store recordings. The end user may require additional simultaneous recordings in the future and does not want to be limited, nor have to subscribe to third party recording equipment with port expansion limitations and associated costs. The system must utilize standard servers for processing and storing the records.	M	Y		The proposed system is completely configurable and customizable based on the specific requirements of Ramsey County. All recordings utilize standard servers for processing and storing recordings, unless configured as attorney / client or do not record.
68.	The system allows user authorization to perform various tasks (viewing, searching, saving to media, etc.) and shall be controlled by permissions (or roles) stored in the visitation system. The authorizations shall be under the control of authorized administrators in the Sheriff's Office. All changes, additions, and deletions of user permissions shall be recorded in an audit trail.	M	Y		All authorization for each user is controlled by specific permissions / privileges assigned based on the duties and functions of the staff / personnel. The User Logging report provides the audit trail to track all such changes, additions, deletions, and more.
69.	The system allows for stored video files be protected such that they are only accessible through the video visitation system and not through direct access to file shares.	M	Y		Video sessions can only be accessed and audited through the system by authorized users. Should a user download and export specific video sessions, the system makes a log of the user that did so, along with a date/time stamp.
70.	The system incorporates an audit trail to track who has viewed or downloaded a copy of a visit.	M	Y		Should a user download and export specific video sessions, the system makes a log of the user that did so, along with a date/time stamp.

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
71.	The system records must be downloadable to a readable format for court testimony or other evidentiary purposes.	M	Y		System records can be downloaded in readable formats.
72.	The system provides a visitation email and voice mail cancellation module. When a pre-arranged visit in the system is cancelled, the system shall automatically dial out (via a dedicated phone line) to the visitor and play a pre-recorded message letting them know that one or more of their visits has been cancelled with the respective inmate. The system shall dial the number that was provided by the visitor and send an email to the pre-provided email.	P	Y		The proposed system currently provides notification that a visit has been cancelled, by text and email. Notifications provide the end-user with reason as to why it was cancelled.
73.	The system allows visitation recording that will, at a minimum, the following:				
a.	Have automated management capabilities.	P	Y		The proposed system contains automated management capabilities.
b.	Be stored on secure cloud-based storage servers at no cost to the County.	M	Y		Storage retention of Video Visit Sessions and the associated Visit Detail Records is completely configurable based on the requirements of Ramsey County. The proposed VVS is a completely web-based, centralized system with no physical servers located on-site at the Jail facility. All data and recordings are stored in multiple, geographically separate locations in order to ensure redundancy and maximum protection.
c.	Have a method to determine if information was altered.	M	Y		Video visits and detail cannot be altered in the system due to the secure encryptions worked

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
					into the software. Should any data be corrupted or altered by threats or hacks, the system can pinpoint these instances.
d.	Be made available for use using proprietary and standard non-proprietary application(s).	P	Y		Authorized Users are able to view current, in-progress sessions as well as historical sessions (aside from privileged sessions) from directly within the proposed web-based application.
e.	Be accessible via a web portal.	P			
f.	Be searchable and sortable by a variety of fields including: ascending and descending date and time, name of inmate, name of visitors, visitation station and ID number.	P	Y		The proposed system is capable of searching and sorting through the fields described herein.
g.	Be downloadable for review and can be saved to other types of portable media.	M	Y		The proposed system allows for video visits to be downloaded and saved to external hard drives.
h.	Will be permission-based access to recordings and logging.	P	Y		The proposed system is a permissions-based system requiring username / password in order to access. User permissions can be configured at a very granular lever and based on specific roles and job functions of each user.
i.	Be date and time stamped.	M	Y		
j.	Have archiving capabilities.	P	Y		
<b>H. REPORTS</b>					

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
74.	Thy system can produce queries and creates reports on inmates and their visitors in HTML or PDF format.	P	Y		Custom reports can also be set up for automatic delivery. Reports can easily be downloaded in a variety of file formats including PDFs, XLS and CSV.
75.	The system can produce access to reports (hard copy or electronic) for the facility to make arrangements for inmate's pending scheduled visit.	P	Y		In addition to the wide range of standard 'canned' reports available from within the proposed system, NCIC's VVS team is prepared to work with Ramsey County in order to generate customized reports based on the specific requirements of Ramsey County.
76.	The system can produce reports that include, at a minimum, the following:				
a.	Inmates previous visitation history including date and time of visit, type of visit (on-site or off-site), the person who scheduled the visit, person who actually visited.	P	Y		The proposed VVS includes a comprehensive range of reporting capabilities, including a set of "canned" reports that are commonly used by Facility personnel. Reports are both investigative and managerial / financial in nature. Additionally, NCIC will deploy our experienced Reporting experts to design and make available any custom reports as required by Ramsey County. The following reports are available to authorized users from the proposed VVS application: • Visit History Reporting

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
					<ul style="list-style-type: none"> <li>• User Activity Reporting</li> <li>• Ticket Usage Log Reporting</li> <li>• Inmate Document Log Reporting</li> <li>• External Service Log Reporting</li> <li>• Inmate Message Log Reporting</li> </ul>
b.	Visitors visitation history including date and time of visit, type of visit, which inmate they visited, IP address used during the visit for at home visits.	P	Y		
c.	Daily, monthly and annual report of visits.	P	Y		The proposed system can generate these reports.
77.	They system can produce an audit trail to provide a means to search visitation data that include, at a minimum, the following:				
a.	How visit was scheduled.	P	Y		The proposed system is capable of auditing this information.
b.	Who scheduled visit.	P	Y		The proposed system is capable of auditing this information.
c.	When was visit scheduled.	P	Y		The proposed system is capable of auditing this information.
d.	When was visit canceled or changed.	P	Y		The proposed system is capable of auditing this information.
78.	The system provides access capability to the visitor database for custom report writing by the facility.	P	Y		NCIC will provide access to the reporting database to any required personnel and systems.
<b>I. EQUIPMENT</b>					
79.	Contractor shall specify all equipment needed and to be installed. Equipment in housing units must be of rugged construction and able to meet the needs in a correctional environment.	M	Y		The proposed VVS has been designed specifically for use in a correctional environment, sturdy, robust, with no exterior removable components. The top



FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
					surface of the kiosk is angled in order to prevent inmates from placing drinks and other items on top of the units, which are moisture resistant. Neither NCIC nor our Facility customers have encountered any limitations of the proposed VVS.
80.	Equipment shall include, at a minimum, the following: <ul style="list-style-type: none"> <li>• 15 Public Terminals</li> <li>• 29 Inmate Terminals</li> <li>• 20 Skype Kiosk (if separate from Terminals)</li> <li>• 1 Lobby Kiosk for scheduling purposes only</li> <li>• Ability to expand to 30 public terminals</li> <li>• Ability for inmates to visit without direct access to a fixed video visitation station</li> </ul>	M	Y		NCIC will provide all required equipment described herein.
81.	Handsets attached to the station and interfaced with audio and video on computer.	P	Y		
82.	Handsets made of heavy molded plastic with 18" armored cords.	P	Y		The NCIC video units employ a heavy-duty armored handset that is hearing-aid compatible, and has an anti-static receiver.
83.	Installation of cable, conduit and other materials must conform to the standards of the industry and the Ramsey County Sheriff's Office institutional security standards.	M	Y		NCIC will ensure that all of cable, conduit and other materials meet the standards of Ramsey County.
84.	All equipment shall be of heavy construction and considered vandal-proof by the Ramsey County Sheriff's Office institutional security standards. All screws shall be tamper-proof. Security phone sets shall be provided.	M	Y		All proposed VVS equipment is correctional-grade, robust, with no exterior moving parts, meeting or exceeding all requirements as stated herein.
85.	Contractor shall provide information on a screening mechanism to minimize views of facility for safety and security reasons and other new technology.	M	Y		

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
86.	Contractor shall provide a secure, separate network, which is not part of the County managed network and/or internet for the video visitation solution, which includes build, installation and ongoing maintenance of the Contractor provided network and/or internet.	M	Y		<b>NCIC will provide a secure, independent network that will run across all proposed video visitation stations and systems.</b>

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660**  
**ATTACHMENT E - TABLET SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
<b>A. COMPLIANCE</b>					
1. FCC Compliance / Data Privacy	The system is compliant with all federal, state, and local laws, statutes, ordinances, rules, regulations, and standards for data privacy and the Federal Communications Commission (FCC).	M	Y		NCIC is fully compliant with Federal, State or local laws, statutes, etc., and all equipment meets or exceeds applicable FCC licensing, rules and certification regulations. FCC FRN# and other certification-related documents are available upon request.
2. ADA Compliance	The system is compliant with the Americans with Disability Act (ADA) and accessible to hard of hearing individuals.	M	Y		NCIC's proposed tablet system is fully compliant with the Americans with Disability Act. Our tablets provide VRS capabilities,
3. FBI CJIS and BCA MNJIS Compliance	The contractor and system are compliant with federal and state laws and regulations, including the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) and the Minnesota Bureau of Criminal Apprehension (BCA) Minnesota Justice Information Services (MNJIS).	M	Y		NCIC and the proposed system is compliant with all applicable Federal and State laws and regulations associated with the FBI, CJIS, BCA and MNJIS.
4. Minnesota Government Data Practices Act	The contractor and System are compliant with the Minnesota Government Data Practices Act.	M	Y		NCIC's proposed system is compliant with the Minnesota Government Data Practices Act.
5. PCI Compliance	Inmate financial transactions must comply with PCI requirements.	M	Y		The proposed platform and billing system is fully PCI Compliant.
<b>B. GENERAL TECHNICAL</b>					
6. Ownership	Contractor owns the tablets and other related devices. If anything malfunctions, contractor is responsible for repairing and replacing.	M	Y		NCIC is the owner of the proposed tablet equipment and directly manages/repairs any faulty equipment for the lifetime of the agreement. At no time will NCIC use a third party manage and replace any of the proposed equipment for Ramsey County.
7. Case Color	The case for the tablets is bright in color for easy identification/locating.	P		N	As a standard, NCIC's proposed tablet exterior is black with a clear backing but if

**KEY:** M = Mandatory P = Preferred Y = Yes No = No

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660**  
**ATTACHMENT E - TABLET SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
					a brightly colored casing is required for tablets, NCIC will work to accommodate this requirement, if awarded.
8. Case Type	The case for the tablet is tamper-resistant.	M	Y		NCIC's tablets are comprised of a heavy-duty exterior which is specifically designed for a correctional environment, allowing it to withstand a shock and/or drop test onto concrete. NCIC has only allowed access to critical hardware buttons such as the power button, volume buttons, and the home button.
9. Charging	Contractor provided charging stations will accommodate multiple tablets simultaneously in a minimum space.	M	Y		All of the proposed tablets will be stored and charged in mobile charging carts allowing for secure storage and easy transport (or wall-mounted charging options are available, if preferred for certain areas of the Jail). Charging carts can be wheeled between pods to allow for maximum distribution of tablets in areas equipped with secured wireless connectivity. The charge cart itself simply plugs into a wall outlet when it is time to charge the tablet devices; otherwise, it can be rolled between pods without exposed cords or wiring. This prevents any inmate access to electrical components or wiring.
10. Charging Type	Tablets are charged wirelessly.	P	Y		NCIC is capable of providing charge carts that provide a wireless charge – tablets would simply be placed on top of a charging pad that is installed into the cart.
11. Display	Tablets have a minimum of a 7-inch highly durable and break-resistant display.	M	Y		NCIC has used similar grade materials to the kinds used in bullet resistant glass, windows in correctional facilities, military applications, etc., ensuring that the tablet is suitable for your Facility. This case protects

**KEY:** M = Mandatory P = Preferred Y = Yes No = No

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660**  
**ATTACHMENT E - TABLET SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
					the tablet from being tampered with, general damage, and contraband storage.
12. Device Quantity	Contractor shall provide a minimum of 475 tablets.	P	Y		NCIC will provide the required number of tablets listed herein, as well as an agreed upon number of spare tablets for quicker replacements of faulty equipment.
13. Usage Duration	Tablets can support 8 hours of continued use before having to be recharged.	M	Y		
14. Device Capability	Tablets have the ability for phone calling, electronic mail, e-messaging, and video visiting.	M	Y		The tablets operate on the same InTouch Suite platform as the Kiosk System, allowing for streamlined delivery of approved services and applications to the inmate population. The proposed Inmate Tablets are capable of offering video visitation services, standard inmate phone calling, messaging, grievances/ticketing, educational & rehabilitation program services, entertainment services, commissary ordering, inmate handbooks, law library, medical/mental health sick call requests; digital mail services; email messaging services, and various other services.
15. Content	Tablets can deliver entertainment, programming, educational, and law library content.	M	Y		
16. Facility Documents	Tablets can display Ramsey County Sheriff's Office uploaded documents and messages to inmates.	M	Y		The proposed InTouch Suite also offers the ability for Facility staff to upload custom Facility Documents to be displayed to inmate or public kiosks. Commonly used documentation includes information such as Inmate Rules, Jail Rules, Facility Handbooks, PREA information, etc., and the system does not provide limitations on uploading. Information can be uploaded in formats such as PDF documents, images, text, videos, and webpages.

**KEY:** M = Mandatory P = Preferred Y = Yes No = No

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660****ATTACHMENT E - TABLET SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
17. Network	Contractor provides a secure tablet Wi-Fi network that is self-contained and managed/maintained by the contractor. The network is completely independent from the Ramsey County network. Wi-Fi service and coverage is robust enough to support all devices simultaneously accessing content in every inmate area, including individual jail cells. Installed hardware is hardened and/or inaccessible to inmates to destroy, damage or modify.	M	Y		The proposed Inmate Tablet solution operates on a dedicated Wi-Fi network that does not allow access to external networks, websites, or applications. The tablet's wireless solution has various components that can be either wired to an extended switched ethernet network or can be fully meshed with other existing access points. At no time will inmates be able to access the Operating Systems of the proposed Inmate Tablet solution. Prior to being deployed in correctional facilities, the proposed Tablets are subject to strenuous Penetration Testing methodologies to ensure that they are suitable for deployment in a correctional environment. A Connect appliance is installed at each facility which manages the network and content distribution. This appliance maintains connectivity to the Private Cloud for continuous monitoring and content updates.
18. Splash Screen	There is a splash screen that is customizable by the Ramsey County Sheriff's Office.	M	Y		The proposed system allows for customized announcement prompts to be displayed on the video kiosks for both detainees and the public. These prompts can be displayed in any language required by the Facility and can be displayed either before or during a video session. These prompts are displayed on inmate kiosks without the requirement for them sign in to access displayed information. In addition, the proposed Kiosk solution allows for the entry of a customized digital banner, allowing Authorized Users / Facility administration

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660**  
**ATTACHMENT E - TABLET SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
					the ability to broadcast messages to the inmate population or to kiosks in the public lobby areas. Messages can either be broadcast at a facility-wide level, or to specific housing areas. This allows for “Message of the Day” functionality, such as changes in visitation hours, special menu updates, etc.
<b>C. GENERAL OTHER</b>					
19. Financial Proposals	Contractor proposes multiple financial options to include but not limited to, providing tablets at no cost to inmates, no cost to the County, and/or funded by inmate content purchases.	M	Y		NCIC can offer tablets at no cost to Facility staff or the inmate population. Our services and equipment are provided to Ramsey County at no cost for the life of the agreement. Our proposed system and content is also entirely free to the inmate population in order to promote access to free educational and rehabilitative content, in exchange for “awarded” time towards a variety of entertainment options such as games, movies, e-books, music, podcasts, and more.
20. Free Content	Inmates have access to programming, educational and law library content free of charge.	M	Y		NCIC Correctional Communications is thrilled to unveil our groundbreaking Learning Management System (LMS), designed to significantly enhance the rehabilitation and reentry preparation for incarcerated individuals. Named Schoolhouse, our educational platform is the culmination of years of meticulous planning and the assembly of high-quality learning materials, videos, and games. It operates using our proprietary RISE Method (Restoration through Incentives, Skills, and Education) model, aiming to actively engage and transform our students

**KEY:** M = Mandatory P = Preferred Y = Yes No = No

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660**  
**ATTACHMENT E - TABLET SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
					<p>into responsible citizens. Through this innovative method, learners can explore personal growth and skill development while earning rewards for their dedication. It offers a comprehensive range of over 900 courses and 400 books, covering academic subjects, vocational skills, and life-enhancing topics.</p> <p>NCIC is continuing to add new educational course content, as well as entertainment content, to the Schoolhouse system with the help of our full-time Curriculum Coordinator, who has a master's degree and various certifications in education. NCIC is constantly working with our customers and partners to generate new, custom content that suits the needs of our Facility customers, and incarcerated individuals. We find that engaging with our customers allows us to specifically target their specific requirements for reform and education of their incarcerated population.</p> <p>NCIC strongly believes in widespread accessibility of educational opportunities for those who are incarcerated. Because of this, we believe a truly impactful tablet program requires free and continuous access, irrespective of an incarcerated individual's ability to pay or socioeconomic status. There are many tablet programs that focus on a revenue generating model, requiring incarcerated individuals to "pay to play." These programs that charge their</p>



**PROFESSIONAL SERVICES AGREEMENT #: RC-000660**  
**ATTACHMENT E - TABLET SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
					<p>incarcerated population to access content and entertainment (such as movies, games, music, e-books, etc.) often see significantly lower engagement rates. NCIC's LMS also allows agencies to upload their own classes and content via URL's or SCORM files, which also can be added as part of our module allowing the students to earn rewards.</p> <p>The benefits that our Schoolhouse System provides an Agency, such as decreased incidences of violence, lowered recidivism, and better re-entry preparation, often far outweigh the potential revenue that may be generated from the devices. We want to stress that NCIC's educational platform and incentive-based entertainment comes at no additional cost to the incarcerated individuals, or their friends and family. Our Schoolhouse system helps students realize that incarceration is their opportunity to find a path forward instead of a brief pause from their struggles outside of your facility. These thoughtful courses were designed for incarcerated individuals struggling with mental health issues, grief, anxieties, and addictions. Your efforts to offer these meaningful programs will help your community curb recidivism by providing encouragement to your detainees and their families.</p> <p>Priority courses cover:</p> <ul style="list-style-type: none"> <li>• Anger Management – Over 120 classes</li> </ul>

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660**  
**ATTACHMENT E - TABLET SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
					<p>specifically help students control anger and emotions during heated moments.</p> <ul style="list-style-type: none"> <li>• Stress Management – Over 150 classes that help in overcoming stressful situations and lighten the mood of students.</li> <li>• Personal Finance – Money management, budgeting, understanding credit cards, debt management and personal checking.</li> <li>• Personal wellness – Over 250 classes of confidence building, social skills, meditation, mindfulness relaxation and self-awareness activities.</li> <li>• People skills – Interacting with others, dispute resolution, management techniques, communications skills, and reconnection with loved ones.</li> <li>• Work skills – Thousands of classes on computer / technical skills, how-to videos on construction, auto repairs, mechanical trades, etc.</li> </ul> <p>Additionally, NCIC is proposing a complete, comprehensive Law Library solution at zero cost to the County and inmates, which is accessible through kiosks or Tablets. NCIC has researched Law Library providers that also offer robust resources for Federal inmates, and by partnering with Fastcase (<a href="https://www.fastcase.com/">https://www.fastcase.com/</a>) for provision of legal resources for Ramsey County, ensuring inmates at the Facility will have optimal access to these resources. The application allows inmates to research past legal cases, constitutions, statutes,</p>

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660**  
**ATTACHMENT E - TABLET SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
					regulations, etc.
21. Tutorial	Tablets will have a usage tutorial accessible to inmates.	M	Y		The proposed tablet system is the same as the kiosk platform – NCIC will provide usage tutorials to Ramsey County to distribute to inmates, if needed.
22. Repair and Replacement	Contractor proposes multiple financial options for repair or replacement of tablet devices.	M	Y		<p>NCIC is proposing an entirely no cost service for repairs and replacement of tablet equipment, charging carts, and all other associated equipment installed at Ramsey County.</p> <p>NCIC has made it easy for the management of damaged or faulty tablets by allowing Authorized Users to prepare and submit a Return Merchandise Authorization (RMA) request, directly through the proposed InTouch Suite.</p> <p>By default, all Tablets are identified by using the individually assigned MAC address on the back of the casing. Specifications for individual Tablet are required in order for the RMA process to be initiated such as providing the MAC Address, a pre-selected issue, and a written description of the issue, in order to proceed. In the event that Facility staff would like to submit a long listing of faulty equipment, users will have the ability to either manually add each device or upload an Excel spreadsheet with all required detail.</p> <p>NCIC provides ticket information and resolution updates of RMAs by sending an email notification to the appropriate parties</p>

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660**  
**ATTACHMENT E - TABLET SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
					<p>throughout the process. Once an RMA has been submitted, it will be assigned a unique RMA identifier number so that facility staff and NCIC personnel can easily locate RMA requests. NCIC personnel can communicate with Facility staff by sending messages back and forth within the submitted RMA request, until the request has been resolved and closed.</p> <p>Once NCIC staff has logged all necessary details, replacement tablets with new MAC addresses will be boxed up and shipped to the Facility for next day or 2-day shipping arrival. Along with the tablets, NCIC will provide the Facility with a return label for staff to send back the faulty tablet equipment for us to refurbish.</p>
23. Inmate Fees	Any fees/charges to the inmates are minimal, transparent, and are subject to the County's approval.	M	Y		NCIC does not charge fees to inmates, aside from the communication rates for calling, video visits, and messaging. The only fees charged are government taxes applied to calls that are placed.
24. Staff Training	Ramey County Sheriff's Office team members have access to training on the administration and usage of the tablet system.	M	Y		NCIC provides free, comprehensive training to all customers and will provide free recurring training as needed and/or requested by Ramsey County. Facility Administrators, along with any County staff who will have access to the equipment and the system interface, are thoroughly instructed on how to use the proposed platform. Staff will receive hands-on training to ensure they are properly acquainted with the new system. Training can be provided over multiple days and

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660**

**ATTACHMENT E - TABLET SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
					shifts to ensure all Facility staff have a chance to participate, if needed. All staff will be provided with a detailed syllabus, as well as a training manual.
25. Spare Tablets	Replacement tablets are available on-site at the Adult Detention Center.	M	Y		NCIC will provide Ramsey County with the required number of tablets listed above, along with additional spare units in the event there are faulty tablets. After the initial units are provided, NCIC will work with the Facility to provide more tablet replacements on an as needed basis.
26. Sanitize Tablets	The contractor shall have a method to sanitize the tablets in between inmate usage.	M	Y		NCIC recommends having inmates wipe down their tablet with sanitizing wipes, prior to putting their used tablet back into the charging station. If required, NCIC will provide Ramsey County with sanitizing wipes.
<b>D. SECURITY CONTROLS</b>					
27. User Login	Tablets allows for secure authentication for inmate end-user login.	M	Y		<p>Inmates will have the ability to securely log onto the tablets using their inmate ID number (“PIN1”) and will be required to enter their “password” (PIN2), which they will have the capability to create themselves. This login is required in order for inmates to access any tablet features or applications.</p> <p>Additionally, on the “login” screen of NCIC’s tablets, the keypad is “scrambled” so that the numbers appear in different sequence / placement each time. This minimizes the probability that other residents are able to view / memorize the</p>

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660**

**ATTACHMENT E - TABLET SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
					input of an inmate's PIN1 or PIN2, further ensuring the integrity of resident accounts.
28. Content Control	Ramsey County Sheriff's Office has control over the content delivered.	M	Y		
29. Monitoring	Tablet system has the ability for Ramsey County Sheriff's Office to monitor content the inmates are viewing.	M	Y		The proposed Tablet system allows authorized users to monitor the content the inmates are viewing or interacting with through the tablets. Monitoring is covert and residents will not be aware that monitoring is taking place.
30. Content Accessibility	Tablets have device safeguards that prevent the inmate from accessing unauthorized content. All accessible content shall be Ramsey County Sheriff's Office authorized.	M	Y		All proposed Tablet content has been pre-filtered to show only positive and rehabilitative content. At no time will residents have access to external links or inappropriate content. Ramsey County will have the ability to pre-approve all content prior to tablet deployment, to ensure that only approved content is being accessed.
31. Tablet Control	Tablet system has ability to control and terminate the devices remotely.	M	Y		The proposed tablet application is entirely customizable and facility staff will have the ability to modify which applications will be available to residents. These modifications can be applied based on an individual tablet, group of tablets, or all tablets.
32. Usage Tracking	Tablet system can track and document inmate usage and completion of educational programming.	M	Y		<p>Our system offers robust reporting capabilities that are essential for tracking learning progress, engagement, and overall effectiveness of training programs. Here is a summary of some key reporting features that we can provide upon request:</p> <p>➤ <u>Custom Reports</u>: Allows the creation of custom reports based on specific criteria, which can then be saved,</p>

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660**  
**ATTACHMENT E - TABLET SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
					<p>scheduled, and distributed automatically.</p> <ul style="list-style-type: none"> <li>➤ <u>Predefined Templates</u>: Offers a variety of pre-configured report templates for common reporting needs.</li> <li>➤ <u>Dashboard Analytics</u>: Provides real-time analytics on the dashboard, giving administrators a quick overview of key metrics.</li> <li>➤ <u>User Tracking</u>: Enables detailed tracking of individual user progress, including course completion, grades, and activity engagement.</li> <li>➤ <u>Course Analytics</u>: Provides insights into course engagement and effectiveness, including data on participation, time spent, and course completions.</li> <li>➤ <u>Data Filters</u>: Allows users to sort and filter data based on different criteria, such as date ranges, user roles, or specific courses and activities.</li> <li>➤ <u>Data Export</u>: Capability to export reports in multiple formats like CSV, Excel, and PDF for further analysis or sharing.</li> <li>➤ <u>Dynamic Data</u>: Reports can be set to auto-update, ensuring stakeholders always have access to the most current data.</li> <li>➤ <u>Competency Reports</u>: Tracks skill and competency development across various learning programs</li> <li>➤ <u>Multi-Tenancy Support</u>: Allows for isolated reporting in multi-tenancy environments, providing different</li> </ul>

**PROFESSIONAL SERVICES AGREEMENT #: RC-000660**

**ATTACHMENT E - TABLET SYSTEM REQUIREMENTS AND QUESTIONNAIRE**

FEATURE	FUNCTION / DESCRIPTION	M or P	Y	N	COMMENTS
					<p>departments or organizations with their own specific reports.</p> <p>➤ <b>Audit Trails:</b> Keeps a log of all system activities, including user logins and course modifications, aiding in compliance and auditing processes.</p>
<b>E. INTEGRATIONS; INMATE INFORMATION &amp; IDENTIFICATION</b>					
35. Jail Management System Integration	The system provides an interface with the current Jail Management Systems (JMS) and capability to interface with future JMS and/or upgrades.	M	Y		<p>NCIC currently has multiple interfaces developed with major JMS and commissary companies, allowing inmate information to be imported on a real-time basis. All features of the interface will be automated, eliminating any need for County / Facility staff intervention in managing accounts.</p>
36. Commissary and Vending System Integration	The system provides an interface with the current commissary/vending system and capability to interface with future systems and/or upgrades.	M	Y		



**PROFESSIONAL SERVICES AGREEMENT # RC-000660**  
**ATTACHMENT F – PRICING SCHEDULE**

	PRICING
SERVICE TYPES	At Cost: No Cost to the County, Free, and Reduced Rates
<b>Correctional Telephone Service:</b>	<b>\$0.00 / phone / month</b>
All calls within United States, 10 minute limit on each call including all payment types (pre-paid collect, and debits)	2 free phone calls per day, 10 minute limit on each call, \$0.07 per minute for each additional call
Mexico/Canda including all payment types (pre-paid collect, and debits)	\$0.15 per minute
Cuba including all payment types (pre-paid collect, and debits)	\$0.99 per minute
Other International Calls including all payment types (pre-paid collect, and debits)	\$0.20 per minute
Inbound Voicemail (public users may leave up to a 3 minute voicemail message)	\$0.50 per voicemail (up to 3 minutes duration)
<b>Video Visitation:</b>	<b>\$0.00 / kiosk / month</b>
On-Site Video Visits (all on-site video visitation sessions will be provided at no cost)	Free
Remote Video Visits (between inmates and public users or private attorneys only, 20 minute maximum)	1 free remote visit per day, 20 minute limit, \$0.12 per minute for each additional visit
Remote Video Visits (between inmates and public defenders or court staff will be provided at no cost, 20 minute maximum)	Free
<b>Tablet / Entertainment Services:</b>	<b>\$0.00 / tablet / month</b>
1:1 Distribution Ratio with Charging Stations and Devices	Free, unlimited use
Premium Learn2Earn Educational Platform	Free, unlimited use
Paid Streaming Digital Content (still in beta testing but expected to role out within the year)	\$0.02 per minute Once rolled out-concurrent with Learn2Earn

	PRICING
SERVICE TYPES	At Cost: No Cost to the County, Free, and Reduced Rates
<b>Deaf and Hard of Hearing Services for ADA Compliance:</b>	
Video Relay Service (available on all video visitation kiosks and tablets)	Free calls / visits
<b>Fees:</b>	
All Fees Including, But Not Limited To: Funding Fees, Transaction Fees and Card Processing Fees	Live operator: \$5.95
	Automated operator and web transaction fee: \$3.00
	Refund Fee: \$0.00
<b>Commission:</b>	
Correction Telephone Service, Video Visitation and Secure Messaging, and Tablet-Educational and Entertainment Content	0%
<b>Additional Services:</b>	
Text Messages (up to 140-160 characters)	\$0.10 per message
Picture Attachments (inbound and outbound)	\$0.15 per photo
Video Messages (inbound and outbound, 30 seconds)	\$0.15 per message
GIFs	\$0.05 per GIF
Suicide and Crisis Lifeline Access	Included, no cost
Voice Biometrics, Call Transcription, and Investigative Keyword Alerts	Included, no cost
Learn2 Earn Educational Platform Via Tablets and Kiosks (free educational, rehabilitative and entertainment content)	Included, no cost
Video Relay Service (available on all video visitation kiosks and tablets)	Free calls / visits
Offsite Digital Mail	Included, no cost
County's Jail Management System, Commissary, and Related Systems Interfacing	Included, no cost
All Hardware with Installation and Software Upgrades	Included, no cost
24/7/365 Live, United States Based, Customer and Technical Support	Included, no cost
Commissary Ordering	Included, no cost

	PRICING
SERVICE TYPES	At Cost: No Cost to the County, Free, and Reduced Rates
Digital Law Library Access	Included, no cost
Detainee Forms and Documents (allows staff to share documents and allows attorneys to screen share discovery and e-sign documents)	Included, no cost
Internal Communications System with Grievance, Detainee Requests, and Medical Request Service	Included, no cost
Free Podcasts	Included, no cost
Free Library	Included, no cost
Paid Streaming Digital Content <i>(still in beta testing but expected to roll out within the year)</i>	\$0.02 per minute Once rolled out-concurrent with Learn2Earn
	Learn2Earn content – no cost
	Paid streaming content – reduced cost
Ear Buds	Ear Buds: \$2.00 per each Premium Ear Buds: \$3.00 per each
<b>Equipment Counts:</b>	
Regular Phones	54 each
Speaker Phones	5 each
Kiosks	46 Each
Tablets	520 each
Ear Buds	780 each
Charging Carts - 40 Port	10 each
Charging Carts - 20 Port	7 each

Exhibit 1  
**Business Associate Agreement**

This Business Associate Agreement (“BA Agreement”) is referenced by and incorporated within Professional Services Agreement # RC-000660 (the “Service Agreement”) between Ramsey County, Minnesota, a political subdivision of the State of Minnesota, on behalf of the Community Human Services Department, 160 E. Kellogg Blvd, St. Paul, MN 55101 AND/OR the St. Paul-Ramsey County Department of Public Health, 555 Cedar St., St. Paul, MN 55101 ("Covered Entity") and Network Communications International Corp., dba NCIC Correctional Services, 607 E. Whaley Street, Longview, Texas 75601 ("Business Associate") (each a "Party" and collectively the "Parties").

**Recitals**

- A. The Service Agreement identifies services between the Parties that require execution of a Business Associate Agreement as defined by the Health Insurance Portability and Accountability Act of 1996 as amended ("HIPAA") and the Privacy, Security, Breach Notification, Electronic Transactions, and Enforcement Rules at 45 C.F.R. Parts 160, 162, and 164 (HIPAA Rules).
- B. Ramsey County is a Covered Entity that is a Hybrid Entity as defined at 45 C.F.R. § 164.105.
- C. The Service Agreement identifies certain program areas/units of Covered Entity that are included in Covered Entity’s Health Care Component and in need of Business Associate’s services;
- D. In accordance with HIPAA Rules, which require Covered Entity to have a written contract or memorandum of understanding with its Business Associates, the Parties wish to establish satisfactory assurances that Business Associate will appropriately safeguard PHI and, therefore, execute this BA Agreement.

**NOW, THEREFORE**, intending to be legally bound, the Parties agree as follows:

- 1. **Definitions.** Terms defined in the Recitals and introductory paragraph of this BA Agreement are incorporated by reference. Capitalized terms used but not otherwise defined in this BA Agreement shall have the same meaning as those terms in the HIPAA Rules as amended from time to time.
  - (a) “Business Associate” shall generally have the meaning set forth in HIPAA Rules and also shall refer to the Party identified in this BA Agreement that serves as the Business Associate.
  - (b) “Covered Entity” shall generally have the meaning set forth in HIPAA Rules and also shall refer to the identified Health Care Components of the Party identified above as the Covered Entity, in accordance with the use of this term at 45 C.F.R. § 164.105(a)(2)(i)(A).
  - (c) Protected Health Information (PHI) shall generally have the meaning set forth in HIPAA Rules and also shall refer to PHI applicable to the relationship between the Parties under this BA Agreement and the Service Agreement.

2. **Representations, Acknowledgements, & Satisfactory Assurances of Business Associate.** Business Associate hereby represents and acknowledges: i) it has legal status as a Business Associate under HIPAA Rules as a direct result of its relationship with Covered Entity under the Service Agreement; ii) it has read and fully understands the extensive legal requirements of Business Associates under HIPAA Rules; iii) it has sufficient technical, legal, and monetary resources and know-how to comply with all Business Associate regulatory and contractual requirements for the full term of the Service Agreement, including any renewals or amendments it may execute; and iv) that the consideration identified in the Service Agreement is, in part, in exchange for obligations under this BA Agreement, which may be referenced or incorporated into the Service Agreement. Business Associate offers and Covered Entity accepts these representations and acknowledgments, along with other promises in this BA Agreement, as satisfactory assurances that Business Associate will appropriately safeguard PHI, including electronic PHI.
3. **Obligations of Business Associate.** Business Associate agrees and promises in good faith to do all of the following:
- (a) Comply with all Business Associate obligations and requirements under HIPAA Rules and, if uncertainty exists as to how to achieve compliance, request direction from Covered Entity.
  - (b) Comply with other requirements under HIPAA Rules that may apply to the Covered Entity, such as when Business Associate carries out one or more of the Covered Entity's obligations under HIPAA Rules.
  - (c) Use and disclose PHI only: (i) when required by law; ii) as set forth in this BA Agreement; or (iii) as set forth in the Service Agreement or, if the Service Agreement is ambiguous or incomplete, then only as permitted or required by the Covered Entity's Notice of Privacy Practices that was in effect when the information was collected from the individual.
  - (d) MINIMUM NECESSARY. Limit its use, disclosure, and requests for use or disclosure to the minimum amount necessary to accomplish the intended purpose in accordance with the requirements of the HIPAA Rules.
  - (e) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic PHI that it creates, receives, maintains, or transmits on behalf of the Covered Entity.
  - (f) Manage Security Incidents in compliance with 45 C.F.R. Part 164 Subpart C, including immediate notification to the Covered Entity of a Security Incident upon discovery.
  - (g) Upon discovery of a Breach as defined at 45 C.F.R. § 164.402, which is recognized by HIPAA Rules as a type of Security Incident, comply with 45 C.F.R. Part 164 Subpart D, which includes immediate notification to Covered Entity in a prescribed form and providing prescribed information. In addition to the requirements of HIPAA Rules, Business Associate shall:

- (1) Identify all known individuals or entities that caused or contributed to the occurrence of a Breach at Business Associate's expense; and
  - (2) Cooperate with Covered Entity to notify, at Business Associate's expense, all Individuals and media required to be notified under the HIPAA Rules; and
  - (3) Indemnify Covered Entity for any reasonable expenses Covered Entity may incur in connection with such Breach, including notification.
- (h) The parties acknowledge that the definition of Breach as set forth in the HIPAA Rules at 45 C.F.R. Part 164.402 excludes the following circumstances and therefore Breach notice requirements do not apply:
- (1) Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a Covered Entity or a Business Associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under 45 C.F.R. Part 164, Subpart E.
  - (2) Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same Covered Entity or Business Associate, or organized health care arrangement in which the Covered Entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under 45 C.F.R. Part 164, Subpart E.
  - (3) A disclosure of PHI where a Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
- (i) In accordance with 45 C.F.R. § 164.524, provide access to PHI in a Designated Record Set to an Individual at the request of Covered Entity and in the time and manner designated by Covered Entity. Provide immediate notice to Covered Entity when Business Associate receives a request for access from an Individual.
  - (j) In accordance with 45 C.F.R. § 164.526, make amendments to PHI in a Designated Record Set as directed by the Covered Entity or take other measures as necessary to satisfy Covered Entity's obligations regarding amendments. Provide immediate notice to Covered Entity when Business Associate receives a request for an amendment from an Individual.
  - (k) Make its internal practices, books and records, including policies, procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity available to the Covered Entity or to the Secretary or the Secretary's designee, in a time and manner designated by the requestor, for purposes of audit or determining Covered Entity's compliance with HIPAA Rules.
  - (l) In accordance with 45 C.F.R. § 164.528, document disclosures of PHI and information related to such disclosures as would be required for Covered Entity

to respond to a request by an Individual for an accounting of disclosures of PHI. Provide to Covered Entity or an Individual, in time and manner designated by Covered Entity, information required to provide an individual with an accounting of disclosures of PHI.

- (m) Implement written policies and procedures, conduct periodic security risk assessments and evaluations, and train employees who have access to PHI about the standards, obligations, policies and procedures required by HIPAA Rules.
- (n) Enter into a written agreement with each agent and subcontractor who has access to the PHI created, received, maintained, or transmitted by Business Associate in relation to Covered Entity and include in such agreement the same or parallel restrictions, requirements, and conditions that apply through this BA Agreement to Business Associate, including provisions with respect to reasonable and appropriate safeguards to protect electronic PHI.

4. **Obligations of Covered Entity.** Covered Entity shall not direct Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Covered Entity. Covered Entity agrees to provide Business Associate with:

- (a) the applicable notice of privacy practices that Covered Entity produces in accordance with 45 C.F.R § 164.520 and material changes to such notice over time;
- (b) any changes in, or revocation of, permission by an Individual to use or disclose PHI, if such changes affect Business Associate's permitted or required uses and disclosures; and
- (c) notice of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with HIPAA if such restrictions affect Business Associate's permitted or required uses and disclosures.

5. **Defense, Indemnification and Hold Harmless.** The Business Associate agrees to defend, indemnify, and save and hold the Covered Entity, its agents, officers, and employees harmless from all claims, fines, penalties, damages, and settlement amounts arising out of, resulting from, or in any manner attributable to any unauthorized use or disclosure of PHI by Business Associate, its subcontractors, agents and employees under this BA Agreement, including legal fees or disbursements paid or incurred to enforce the provisions of this BA Agreement.

6. **Term and Termination.**

- (a) **Term.** The Term of this BA Agreement shall be effective as of the Effective Date listed below, and shall continue until terminated as provided herein.
- (b) **Termination upon Termination of the Underlying Relationship.** This BA Agreement will terminate upon the termination of the Business Associate's relationship with Covered Entity under the Service Agreement.
- (c) **Termination for Cause.** Upon learning of a violation by Business Associate of a material term of this BA Agreement, Covered Entity shall provide Business Associate with notice to cure or end the violation by a specified time, which may

be different for each type of violation, but the default for which shall be two (2) business days. The Covered Entity will have the right to terminate this BA Agreement and the Service Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity; or the Covered Entity may immediately terminate this BA Agreement and the Service Agreement if the Business Associate has breached a material term of this BA Agreement and cure is not possible or is not in the best interest of Covered Entity, based on Covered Entity's sole determination.

(d) Upon Termination.

- (1) Except as provided in paragraph (2) of this section, upon termination of this BA Agreement for any reason, Business Associate shall immediately return or destroy, according to Covered Entity's instructions, all PHI that it created, received, maintained, or transmitted on behalf of or to or for Covered Entity to the extent that Business Associate still maintains such PHI in any form. Business Associate shall take the same action for all such PHI that may be in the possession of its subcontractors and agents. Business Associate and its subcontractors and agents shall not retain copies of any such PHI.
- (2) In the event that Business Associate knowingly cannot or does not return or destroy PHI as described in paragraph (1) of this section, it shall notify Covered Entity of the specific circumstances and continue to extend the protections of this BA Agreement to such PHI and take all measures possible to limit further uses and disclosures of such PHI for so long as Business Associate or its subcontractors or agents maintain such PHI. The Parties intend that the provisions of this section 6(d)(2) survive termination of this BA Agreement.

7. **Mutual Representations and Warranties of the Parties.** Each Party represents and warrants to the other Party that it is duly organized, validly existing, and in good standing under the laws of the jurisdiction in which it is organized, it has the full power to enter into this BA Agreement and to perform its obligations, and that the performance by it of its obligations under this BA Agreement have been duly authorized by all necessary corporate or other actions and will not violate any provision of any license, corporate charter or bylaws; and that neither the execution of this BA Agreement, nor its performance hereunder, will directly or indirectly violate or interfere with the terms of another agreement to which it is a party.
8. **Governing Law.** This BA Agreement will be governed by and construed in accordance with the laws of the State of Minnesota, without giving effect to the conflicts of laws principles thereof.



9. **Notices.** All demands, notices, requests and other communications hereunder must be in writing and will be deemed to have been duly given only if delivered personally or by registered or certified mail return receipt requested to the Parties at the following addresses:

if to Covered Entity, addressed to:

Karen Saltis  
Privacy Officer  
Ramsey County Community Human Services Dept.  
160 E. Kellogg Blvd., Rm. 9305  
St. Paul, MN 55101

OR

Chris Bogut  
Privacy Officer  
St. Paul-Ramsey County Department of Public Health  
555 Cedar St.  
St. Paul, MN 55101

if to Business Associate, addressed to:

William Pope  
CEO  
607 E. Whaley Street  
Longview, Texas 75601

or to such other address as a Party hereto will specify to the other Party hereto in writing in a notice which complies with this Section. Any party may give any Notice using other means (including personal delivery, expedited courier, messenger service, telecopy, telex, ordinary mail, or electronic mail), but no such Notice shall be deemed to have been duly given unless and until it is actually received by the intended recipient.

10. **Amendment and Modification.** No part of this BA Agreement may be amended, modified, supplemented in any manner whatsoever except by a written document signed by the Parties' authorized representatives. The Parties agree to take action to amend this BA Agreement from time to time as necessary for Covered Entity to comply with the requirements of the Privacy Rule, Security Rule and the Health Insurance Portability and Accountability Act of 1996.
11. **Headings.** The headings used in this BA Agreement have been inserted for convenience of reference only and do not define or limit the provisions hereof.
12. **Counterparts.** This BA Agreement may be executed in any number of counterparts, each of which will be deemed an original, but all of which together will constitute one

and the same instrument. Faxed signatures shall be treated as effective as original signatures.

13. **No Third Party Beneficiaries.** Nothing express or implied in this BA Agreement is intended to confer, nor shall anything herein confer, upon any person other than the Parties and the respective successors or assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever.
14. **Disputes.** If any controversy, dispute or claim arises between the Parties with respect to this BA Agreement, the Parties shall make good faith efforts to resolve such matters informally.
15. **No Partnership, Joint Venture, or Fiduciary Relationship Created Hereby.** This BA Agreement does not constitute a joint venture or partnership arrangement between the Parties and it does not create any relationship of principal and agent, or otherwise between the Parties. Neither Party shall be liable for any obligation incurred by the other, except as might otherwise be expressly provided in this BA Agreement. All employees of each Party shall remain the employee of that Party, and shall not be subject to any direction or control by the other Party. Nothing contained in this BA Agreement shall be interpreted as creating a partnership, joint venture, or employment relationship of the Parties, it being understood that the sole relationship created hereby is one of independent contractor.
16. **Failure to Enforce Not a Waiver.** The failure of either Party to enforce at any time any provision of this BA Agreement shall in no way be construed to be a waiver of such provision or of any other provision hereof.
17. **Successors and Assigns.** This BA Agreement shall be binding upon the respective successors, heirs, administrators and permitted assigns of the Parties.
18. **Entire Agreement.** This BA Agreement constitutes the entire agreement of the Parties with respect to the subject matter hereof and supersedes all prior understandings or agreements, written or oral, with respect to the rights and responsibilities of the Parties set forth in this BA Agreement.
19. **Effect on Covered Agreement.** Except as relates to the use, security and disclosure of PHI and electronic transactions, this BA Agreement is not intended to change the terms and conditions of, or the rights and obligations of the Parties under, the Service Agreement.
20. **Interpretation.** A reference in this BA Agreement to a section in the Privacy Rule or Security Rule means the section as amended from time to time. Any ambiguity in this BA Agreement shall be resolved in favor of a meaning that permits Covered Entity and Business Associate to comply with the HIPAA Privacy Rule and the Security Rule.

**WHEREFORE,** this BA Agreement is duly approved as of the date of the Service Agreement.

## **Exhibit 2 - CJIS Security Addendum**

### **Professional Services Agreement #: RC-000660**

This Security Addendum is an agreement between Ramsey County, a political subdivision of the State of Minnesota, on behalf of the Sheriff's Office and Network Communications International Corp., dba NCIC Correctional Services. This Security Addendum is in support of a contract between the Contracting Government Agency and the Contractor for the provision of services that require compliance with the Federal Bureau of Investigation's (FBI) Criminal Justice Information Systems Security Policy (CJIS Security Policy).

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.

#### **1.0 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.

**1.03 Contract** – the primary agreement between the CGA and the Contractor for the provision of services.

## 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 acknowledgement of such receipt and the contents of the Security Addendum. The signed acknowledgements 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 CJIS Security Policy 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 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 the Contractor.

4.02 Security violations can justify termination of the Contract between the CGA and the Contractor.

4.03 Upon notification, the CSO and FBI reserve 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 CSO will provide the CGA with timely written notice of any action taken. 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 CSO or FBI by the CGA. 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 or the Contract.

## 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; (4) Title 28, Code of Federal Regulations, Part 20; and (5) the Contract. 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 Contract 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 Contract 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 23606

Network Communications International  
Corp dba NCIC Correctional Services

Ramsey County Sheriff's Office

\_\_\_\_\_  
Signature of officer

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Printed Name & Title

\_\_\_\_\_  
Printed Name & Title

\_\_\_\_\_  
Date

\_\_\_\_\_  
Date

**Exhibit 3 - CJIS Security Addendum Certification**  
**Professional Services Agreement #: RC-000660**

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 the 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

# **NCIC CORRECTIONAL SERVICES**

## **Exhibit 4 - Service Level Agreement (SLA)**

### **Professional Services Agreement #: RC-000660**

#### **A. SCALABILITY/RELIABILITY**

##### **1. AVAILABILITY**

- a) The proposed solution shall be available 99.9% of the time per month. This applies to all deployed services including, but not limited to Inmate Telephone Service (ITS), Video Visitation Service (VVS), Secure Messaging, Ticketing, Digital Mail Service and Educational / Entertainment Options.

##### **2. COMMERCIAL POWER OUTAGES**

- a) The network, including the central Network Operations Center (“NOC”) and all other network elements under the control and management of NCIC, shall survive interruptions in commercial power to allow for ongoing, uninterrupted provision of service at the Facility(ies).
- b) In the event of a power outage, any on-premise components must be temporarily restored by NCIC-supplied battery back-up; connections to County / Facility-owned generator circuits will be at the County’s discretion.
- c) In the event of a power outage, NCIC’s solution shall function for a minimum of 90 minutes in the Facility(ies).
- d) NCIC’s solution shall be capable of full recovery from a power outage immediately once commercial power is restored.

##### **3. BUSINESS CONTINUITY AND DISASTER RECOVERY**

- a) Disaster recovery must include restoration time in accordance with Facility(ies) needs. NCIC’s solution shall include alternative routing of traffic for disasters impacting recovery. NCIC’s solution shall include redundant hosting and data backup components with system continuity and functionality measures in the event of a disaster. NCIC’s solution shall secure data and provide continuity of services in accordance with all federal, state and local requirements.

## B. SYSTEM MAINTENANCE

### 1. REPAIR, MAINTENANCE AND MOVE, ADD & CHANGE WORK

- a) Maintenance and support of all system components including but not limited to telephones, kiosks, tablets, tablet charge carts, wireless access points, circuits, network components, software, call processors and all other elements of NCIC's service will be the responsibility of NCIC. During the original contract term and renewals, NCIC will be responsible for repair or replacement of faulty or damaged equipment regardless of the cause including but not limited to inmate damage, natural disaster, and County's actions or operations, however; County personnel will work in good faith with NCIC to ensure that any intentional misuse of or damage to NCIC-provided equipment is discouraged, to the extent that is operationally feasible.

### 2. COUNTY AUTHORIZED REPRESENTATIVES

- a) County will establish an authorized list of County employed individuals who have the authority to open trouble tickets, request maintenance dispatch or support services outside of normal business hours. NCIC's system will be permission/role based for the authorized list of County employed individuals.

### 3. TROUBLE REPORTING

- a) NCIC shall provide an electronic trouble ticket system via the proposed system to initiate trouble tickets for repairs, track the real-time status and provide current and historical reports of those tickets. NCIC's system must generate an auto-tracking number or other unique identifier immediately upon initiation into the system. All updates to open trouble tickets should be sent in real-time electronically to the originator of the ticket and carbon copy the County's shared email addresses: [oitadmin@co.ramsey.mn.us](mailto:oitadmin@co.ramsey.mn.us) and [sdjailadmins@co.ramsey.mn.us](mailto:sdjailadmins@co.ramsey.mn.us). The trouble ticket system shall include, at a minimum:

1. Date and time trouble reported;
2. Name of County staff member reporting trouble;
3. Name of affected County facility;
4. Trouble ticket number;
5. Date and time of Technician arrival and check-in at facility (if applicable);
6. Name of NCIC staff performing the service;
7. Description of trouble;
8. Diagnosis of trouble and work performed;
9. Date and time trouble corrected;
10. Length of time ticket remained open;
11. Status of open tickets.



#### 4. TROUBLE REPORTING DEDICATED TOLL-FREE TELEPHONE NUMBER

- a) NCIC shall provide a dedicated toll-free telephone number for County that will reach a live help desk contact. This contact shall be located within the continental United States, and be available on a 24/7/365 basis.

#### 5. REPAIR PRIORITY LEVELS AND PERFORMANCE REQUIREMENTS

- a) NCIC's solution must include repair priority levels and identified performance response times. By way of example, the table below defines repair priority levels along with associated performance requirements. The items included in the table are not all inclusive and County, at its sole discretion, may deem any repair as a priority 1, 2 or 3 depending on the unique circumstances of each issue (and its overall effect on facility operations).
- b) At the time of the initial report of a repair, NCIC shall immediately begin utilizing NCIC's remote diagnostic capability in order to attempt to rectify the problem. If remote diagnostics are unavailable or if such efforts don't result in a resolution, a technician must be physically at the facility within two (2) hours.

Example: Priority levels and performance requirements:

Priority Level	Characteristics	Performance Requirement
1	Loss of critical functionality as determined by County	4-hour resolution
	Complete system failure	
	Complete loss of recording functions at a County facility	
	Complete loss of call monitoring capabilities at a County facility	
	Complete loss of administrative or investigative access or function at a County facility	
	When 50% or more of inmate telephones, video visiting, or tablets are not working in a specific area / housing unit	
2	Loss of significant functionality as determined by County	8-hour resolution
	Loss of call monitoring capabilities at a County facility (other than a complete loss)	
	Data back-up failure	
	When 50% or less of inmate telephones, video visiting, or tablets are not working in a specific area / housing unit	
3	Loss of non-significant functionality as determined by County	24-hour resolution
	Software fixes not critical to operations	
	Loss of trouble ticket system	

## 6. SYSTEM AUTO-MONITORING

- a) NCIC's system should have auto-monitoring capabilities, alerting of potential system malfunctions or disruptions of service. In addition, NCIC shall provide fault management capabilities that recognize, isolate, correct, and log faults that occur in the system.

## 7. NOTIFICATION OF SYSTEM FAILURES

- a) NCIC shall provide County with real-time contact notification of all Priority 1 system alerts and alarms (as defined in the previous table) including the final resolution of all incidents. In addition, NCIC shall notify the affected facility designee and County personnel of any failure and provide an estimated time of service restoration. For extended outages, NCIC shall provide a detailed plan of repair, including how NCIC will provision alternative service during an extended disruption of service. NCIC shall provide a detailed description of notification capabilities.

## 8. HARDWARE/SOFTWARE REPLACEMENT

- a) NCIC shall maintain a complete set of replacement parts for all hardware and software components of the service. NCIC shall have a plan of action for delivery of the hardware/software in the event of a failure. Such plan shall include, but not be limited to:
  - 1. Immediate emergency service restoration;
  - 2. Complete system replacement;
  - 3. Personnel resources required.

## 9. ESCALATION PROCEDURE

- a) NCIC shall provide an escalation procedure for 24-hour coverage to be invoked in the event that first level NCIC maintenance personnel are unable to remedy County's service request. NCIC shall provide escalation procedures, for each level up to the Company President/Owner, that include, at minimum, the following:
  - 1. A list of individuals (by name and title) at each level of escalation;
  - 2. The role of each individual in the escalation process;
  - 3. Email address;
  - 4. Wireless and work telephone numbers.
- b) These escalation lists and processes must be kept current, and Subscriber shall be notified two weeks in advance of changes so that all appropriate Subscriber personnel can be notified in advance.

## 10. PREVENTIVE MAINTENANCE

- a) NCIC shall perform Preventive Maintenance, facility inspections, test routines, and diagnostics on the systems as required. The schedule shall be consistent with the operating requirements of Subscriber and be based upon the specific needs of the equipment being maintained. NCIC shall notify County or designee at a minimum of forty-eight (48) hours in advance of any facility visit.
- b) Preventive Maintenance that may disrupt service to the users may be required to be done outside of normal business hours.
- c) NCIC shall maintain a Preventative Maintenance plan including, but not limited to the following:
  - 1. Assuring that any remote access devices and other key components are in good working condition.
  - 2. Checking and testing battery back-up systems.
  - 3. Test system and power failure back-up operations.
- d) NCIC must maintain reports identifying the Preventative Maintenance functions actually performed, the results of testing completed, and any changes and/or updates to either the equipment or software. There shall be no charge to County for Preventive Maintenance performed during the contract term.