

Software Support, Maintenance and Updates Agreement

THIS SOFTWARE SUPPORT AGREEMENT (the "Agreement") dated this 17th day of July 2026 (the "Execution Date")

BETWEEN:

Ryman, Inc. DBA: Complete Technology
Solutions
(the
"Vendor")

OF THE FIRST PART

And
CareerSource North Central Florida
(the "Licensee")

OF THE SECOND PART

IN CONSIDERATION OF the provisions contained in this Agreement and for other good and valuable consideration, the receipt and sufficiency of which is acknowledged, the parties agree as follows:

Software Support, Maintenance and Updates

1. This agreement entitles Licensee to 12 months support (July 1, 2026 - June 30, 2027), updates and maintenance term for software and cloud-hosting billed at \$5,546.73 per month (\$66,560.76 annually). Licensed modules: ATLAS CORE Bundled Module includes ATLAS Assignments, Audit Interface, Case Management, Customer Dashboard, Programs/Forms Builder, E-Courses, Events, E-Signature, Flags, Forms Report, Locations, Staff Forms, Staff Positions, System Alerts, Reports and Workflows. ATLAS Document Storage and ATLAS Kiosk Software.
2. After discontinuation of update, support and maintenance service, Vendor will be released from duties in their entirety as related to the continued update, support and maintenance portions of the agreement.

License

3. "Software" includes the executable computer programs and any related printed, electronic and online documentation and any other files that may accompany the product.
4. Title, copyright, intellectual property rights and distribution rights of the Software remain exclusively with the Vendor. Intellectual property rights include the look and feel of the Software. This Agreement constitutes a license for use only and is not in any way a transfer of ownership rights to the Software.
5. The rights and obligations of this Agreement are personal rights granted to the Licensee only. The Licensee may not transfer or assign any of the rights or obligations granted under this Agreement to any other person or legal entity. The Licensee may not make available the Software for use by one or more third parties unless specifically allowed by vendor.
6. The Software may not be modified, reverse-engineered, or de-compiled in any manner through current or future available technologies at any-time during or after this agreement is in effect.

7. Failure to comply with any of the terms under the License section will be considered a material breach of this Agreement.

Limitation of Liability

8. The Software is provided by the Vendor and accepted by the Licensee "as is". The Vendor will not be liable for any general, special, incidental or consequential damages including, but not limited to, loss of production, loss of profits, loss of revenue, loss of data, or any other business or economic disadvantage suffered by the Licensee arising out of the use or failure to use the Software.
9. The Vendor makes no warranty expressed or implied regarding the fitness of the Software for a particular purpose or that the Software will be suitable or appropriate for the specific requirements of the Licensee.
10. The Vendor does not warrant that use of the Software will be uninterrupted or error-free. The Licensee accepts that software in general is prone to bugs and flaws within an acceptable level as determined in the industry.

Warrants and Representations

11. The Vendor warrants and represents that it is the copyright holder of the Software. The Vendor warrants and represents that granting the license to use this Software is not in violation of any other agreement, copyright or applicable statute.

Acceptance

12. All terms, conditions and obligations of this Agreement will be deemed to be accepted by the Licensee ("Acceptance") upon execution of this Agreement.

Term

13. The term of this Agreement will begin on Acceptance and will continue for a period of one Year. (July 1, 2026-June 30, 2027).
14. This Agreement may be negotiated to be extended for up to two one-year periods.
15. At the end of the term, Licensee will retain all rights to customer, document and associated metadata.

Termination

16. Termination for Cause or Convenience

All non-Federal entity's contracts in excess of \$10,000 must address termination for cause and for convenience by the non-Federal entity including the manner by which it will be affected and the basis for the settlement.

The Licensee or Contractor may terminate this Contract upon thirty (30) days written notice to the other party. In the event of a termination for convenience, the Licensee shall be responsible for any outstanding allowable costs incurred up through the revised ending date of the Contract.

This Contract is subject, but not limited to, suspension, partial or full termination for cause if the Contractor is issued a notice of intent to terminate and does not commence correction of such nonperformance within 5 days of written notice and diligently complete the correction thereafter. Reason for Termination for Cause include but are not limited to breach of the Agreement terms. Notice of intent to terminate will be provided to the Contractor by registered mail.

17. This Agreement will be terminated and the License forfeited where the Licensee has failed to comply with any of the terms of this Agreement or is in breach of this Agreement. On termination of this Agreement within the first year, for any reason, the Licensee will promptly destroy the Software or return the Software to the Vendor. Any and all associated image and metadata will remain the property of the licensee.

Equal Employment Opportunity

- 18 Except as otherwise provided under 41 CFR Part 60, all contracts that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 must include:
- The equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246,
 - Equal Employment Opportunity" (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and
 - implementing regulations at 41 CFR part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

Debarment and Suspension

19. (Executive Orders 12549 and 12689)

- A contract award (see 2 CFR 180.220) must 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.

The Contractor certifies that the Contractor is not currently listed in the government-wide exclusions in SAM, is not debarred, suspended, or otherwise excluded by agencies or declared ineligible under statutory or regulatory authority other than Executive Order 12549. The Contractor further agrees to immediately notify Licensee in the government-wide exclusions in SAM, or is debarred, suspended, or otherwise excluded by agencies or declared ineligible under statutory or regulatory authority other than Executive Order 12549.

Byrd Anti-Lobbying

20. (31 U.S.C. 1352)

Contractors that apply or bid for an award exceeding \$100,000 must file the required certification. 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 must also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier, up to the non-Federal award.

Force Majeure

21. The Vendor will be free of liability to the Licensee where the Vendor is prevented from executing its obligations under this Agreement in whole or in part due to Force Majeure, such as earthquake, typhoon, flood, fire, and war or any other unforeseen and uncontrollable event where the Vendor has taken any and all appropriate action to mitigate such an event.

Governing Law

22. The Parties to this Agreement submit to the jurisdiction of the courts of the State of Florida for the enforcement of this Agreement or any arbitration award or decision arising from this Agreement. This Agreement will be enforced or construed according to the laws of the State of Florida.

Miscellaneous

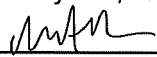
23. This Agreement can only be modified in writing signed by both the Vendor and the Licensee.
24. This Agreement does not create or imply any relationship in agency or partnership between the Vendor and the Licensee.
25. Headings are inserted for the convenience of the parties only and are not to be considered when interpreting this Agreement. Words in the singular mean and include the plural and vice versa. Words in the masculine gender include the feminine gender and vice versa. Words in the neuter gender include the masculine gender and the feminine gender and vice versa.
26. If any term, covenant, condition or provision of this Agreement is held by a court of competent jurisdiction to be invalid, void or unenforceable, it is the parties' intent that such provision be reduced in scope by the court only to the extent deemed necessary by that court to render the provision reasonable and enforceable and the remainder of the provisions of this Agreement will in no way be affected, impaired or invalidated as a result.
27. This Agreement contains the entire agreement between the parties. All understandings have been included in this Agreement. Representations which may have been made by any party to this Agreement may in some way be inconsistent with this final written Agreement. All such statements are declared to be of no value in this Agreement. Only the written terms of this Agreement will bind the parties.
28. This Agreement and the terms and conditions contained in this Agreement apply to and are binding upon the Vendor's successors and assigns.

Notices

All notices to the parties under this Agreement are to be provided at the following addresses, or at such addresses as may be later provided in writing:

- a) Ryman, Inc. DBA: Complete Technology Solutions
12153 Cortez Blvd, Brooksville, FL 34608
- b) CareerSource North Central Florida
1112 North Main Street, Gainesville, FL 32601

Vendor: Ryman, Inc.

Per: 

Maurice Ryman

Name of Vendor's Agent

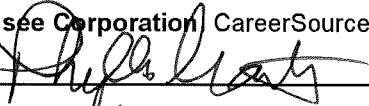
President

Title of Vendor's Agent

7/17/2026

Date

Licensee Corporation: CareerSource North Central Florida

Per: 

Phyllis Marty

Name of Licensee's Agent

CEO

Title of Licensee's Agent

7/21/26

Date

Attachment A Service Level Agreement

Attachment B Security Overview

Attachment C Confidentiality Agreement

Attachment A

Service Level Agreement (SLA)

for *CareerSource North Central Florida*
by

Complete Technology Solutions (CTS)

Effective Date: July 1, 2026

Document Owner:

Complete Technology Solutions

Version

Version	Date	Description	Author
1.0	05-30-2011	Service Level Agreement	Maurice Ryman
1.1	05-30-2013	Service Level Agreement Revised	Maurice Ryman
1.2	05-30-2019	Service Level Agreement Reviewed	Maurice Ryman
1.3	06-15-2021	Service Level Agreement Revised	Maurice Ryman
1.4	06-15-2023	Service Level Agreement Reviewed	Maurice Ryman
1.5	06-30-2025	Service Level Agreement Revised	Maurice Ryman
1.6	07-16-2026	Service Level Agreement Reviewed	Maurice Ryman

1. Agreement Overview

This Agreement represents a Service Level Agreement ("SLA" or "Agreement") between CTS, the Provider, and the Customer for the provisioning of IT services required to support and sustain ATLAS.

This Agreement remains valid until superseded by a revised agreement mutually endorsed by the stakeholders.

This Agreement outlines the parameters of all IT services covered as they are mutually understood by the primary stakeholders. This Agreement does not supersede current processes and procedures unless explicitly stated herein.

2. Goals & Objectives

The **purpose** of this Agreement is to ensure that the proper elements and commitments are in place to provide consistent IT service support and delivery to the Customer by the Provider.

The **goal** of this Agreement is to obtain mutual agreement for IT service provision between the Provider and Customer.

The **objectives** of this Agreement are to:

- Provide clear reference to service ownership, accountability, roles and/or responsibilities.
- Present a clear, concise and measurable description of service provision to the customer.
- Match perceptions of expected service provision with actual service support & delivery.

3. Stakeholders

The following Service Provider(s) and Customer(s) will be used as the basis of the Agreement and represent the **primary stakeholders** associated with this SLA:

IT Service Provider(s): CTS. ("Provider")

IT Customer(s): CareerSource North Central Florida ("Customer")

4. Periodic Review

This Agreement is valid from the **Effective Date** outlined herein and is valid until further notice. This Agreement should be reviewed at a minimum once per fiscal year; however, in lieu of a review during any period specified, the current Agreement will remain in effect.

The **Business Relationship Manager** ("Document Owner") is responsible for facilitating regular reviews of this document. Contents of this document may be amended as required, provided mutual agreement is obtained from the primary stakeholders and communicated to all parties affected. The Document Owner will incorporate all subsequent revisions and obtain mutual agreements/approvals as required.

Business Relationship Manager: CTS

Review Period: Yearly

Previous Review Date: 07-16-2026

Next Review Date: 07-15-2027

5. Service Agreement

The following detailed service parameters are the responsibility of the Service Provider in the ongoing support of this Agreement.

5.1. Service Scope

The following Services are covered by this Agreement;

- Manned telephone support
- Monitored email support
- Remote assistance using Remote Desktop and a Virtual Private Network where available
- Planned or Emergency Onsite assistance
- Monthly system health check
- Updates and maintenance to software
- Continued On-site training and support
- Data Backup

5.2. Customer Requirements

Customer responsibilities and/or requirements in support of this Agreement include:

- Payment for all SAS costs at the agreed interval.
- Reasonable availability of customer representative(s) when resolving a service-related incident or request.
- Hosting of server and data within customer network
- Maintain proper security precautions to prevent unauthorized access to customer network

5.3. Service Provider Requirements

Service Provider responsibilities and/or requirements in support of this Agreement include:

- Meeting response times associated with service-related incidents.
- Appropriate notification to Customer for all scheduled maintenance.
- Appropriate notification to Customer for all bug fixes or training incidents.
- Maintain industry standard security levels for delivery of web-based content

5.4. Service Assumptions

Assumptions related to in-scope services and/or components include:

- Changes to services will be communicated and documented to all stakeholders.

6. Service Management

Effective support of in-scope services is a result of maintaining consistent service levels. The following sections provide relevant details on service availability, monitoring of in-scope services and related components.

6.1. Service Availability

Coverage parameters specific to the service(s) covered in this Agreement are as follows:

- Telephone support: 9:00 A.M. to 5:00 P.M. EST Monday – Friday
- Calls received out of office hours will be forwarded to a mobile phone and best efforts will be made to answer/action the call, however there will be a backup answer phone service
- Email support: Monitored 9:00 A.M. to 5:00 P.M. EST Monday – Friday
 - Emails received outside of office hours will be collected; however no action can be guaranteed until the next working day
- Onsite assistance guaranteed within 72 hours during the business week

6.2. Service Requests

In support of services outlined in this Agreement, the Service Provider will respond to service-related incidents and/or requests submitted by the Customer within the following time frames:

- 0-8 hours (during business hours) for issues classified as **High** priority.
- Within 48 hours for issues classified as **Medium** priority.
- Within 5 working days for issues classified as **Low** priority.

Remote assistance will be provided in-line with the above timescales dependent on the priority of the support request.

Attachment B

ATLAS Security Overview

ATLAS has been designed with security as a foundational principle. The platform incorporates multiple layers of protection to safeguard customer Personally Identifiable Information (PII), maintain data integrity, and ensure only authorized users have access to sensitive information.

User Authentication and Access Control

Administrative access to ATLAS is secured using industry-standard HTTPS/TLS encryption, ensuring all communications between users and the application remain encrypted in transit.

Access to administrative features is granted only after successful authentication. Every authenticated request is evaluated through a Role-Based Access Control (RBAC) system that verifies a user's permissions before access to any module, record, or administrative function is allowed. Administrators can assign granular permissions to ensure users only have access to the information necessary to perform their job responsibilities.

User sessions are securely managed and automatically expire after periods of inactivity to reduce the risk of unauthorized access.

Password Security

ATLAS follows modern password security best practices.

Passwords are never stored in plain text and cannot be decrypted. Instead, passwords are securely hashed using Laravel's built-in password hashing system (Argon2id or bcrypt, depending on deployment configuration), which incorporates unique salts and adaptive work factors designed to protect against brute-force and rainbow table attacks.

During authentication, the submitted password is securely verified against the stored hash without exposing the original password.

Multi-Factor Authentication (MFA)

ATLAS supports mandatory Multi-Factor Authentication (MFA) for all administrative users.

After successful username and password authentication, users must provide a randomly generated six-digit verification code delivered via email or SMS based on their configured preference. Verification codes expire after five minutes and may only be used once.

This additional authentication layer significantly reduces the risk of unauthorized account access, even if user credentials are compromised.

Application Security

ATLAS is built on the Laravel framework, a mature enterprise application framework recognized for its comprehensive security features.

Built-in protections include:

- Cross-Site Request Forgery (CSRF) protection
- Cross-Site Scripting (XSS) mitigation
- SQL Injection prevention through parameterized database queries
- Authentication middleware
- Authorization middleware
- Input validation and request sanitization
- Secure session management
- Signed URLs where appropriate

Every request is processed through Laravel middleware, ensuring authentication, authorization, and security policies are enforced before application logic executes.

Vulnerability Management

The ATLAS environment undergoes automated vulnerability scanning through an independent third-party security service.

These scans evaluate the platform against more than 11,000 known vulnerabilities, with vulnerability definitions updated regularly to ensure newly disclosed threats are quickly identified. Findings are reviewed and remediated according to internal security procedures.

Operating systems, application frameworks, and supporting software receive security updates and patches as they become available.

Database Security

ATLAS utilizes MySQL as its primary database platform.

Security controls include:

- Default-deny network access policies
- Database ports inaccessible from the public Internet
- Firewall rules restricting access to authorized systems only
- Encrypted connections where supported
- Principle of least privilege for database accounts

The MySQL service is accessible only from approved application servers and authorized administrative systems. External access to database ports is prohibited unless explicitly authorized.

Application data access utilizes Laravel's ORM and parameterized queries to prevent SQL injection attacks.

Application logs, security events, and error notifications are monitored to facilitate rapid investigation of suspicious activity.

Infrastructure Security

ATLAS deployments are hosted on hardened web servers with security best practices applied during provisioning.

Security measures include:

- Regular operating system updates
- Timely application of security patches
- Firewall hardening
- Minimal exposed network services
- Continuous monitoring of exposed ports
- Secure TLS configuration

Firewall rules are reviewed periodically to ensure only required services remain accessible.

Organizations are encouraged to include ATLAS account deactivation within their employee offboarding procedures to ensure former employees no longer retain administrative access.

Secure Deployment Process

Software deployments are performed using encrypted SSH connections and secure Git repositories.

Each deployment follows an automated release process that includes:

- Enabling maintenance mode
- Creating a complete database backup
- Deploying the new application release
- Running required database migrations
- Verifying deployment success
- Maintaining previous releases for immediate rollback if necessary

This deployment strategy minimizes downtime while allowing rapid recovery should an issue occur during deployment.

Source Code Security

Source code is maintained within secure version control repositories accessible only to authorized developers.

Development and deployment processes utilize:

- SSH key authentication
- Encrypted communication channels
- Automated deployment pipelines
- Version-controlled releases
- Peer-reviewed code changes
- Dependency management through Composer
- Continuous updates of supported framework and runtime versions

The application is maintained using current supported versions of Laravel, PHP, MySQL, and other required dependencies to ensure ongoing security and performance.

Monitoring and Incident Response

Application logs, authentication events, and system errors are continuously monitored.

Suspicious activity, failed authentication attempts, and critical system events generate alerts for administrative review. Security incidents are investigated promptly, and corrective actions are implemented as appropriate.

Data Backup and Disaster Recovery

When the optional off-site backup service is enabled, ATLAS automatically creates encrypted backup sets and securely stores them within Amazon Web Services (AWS) Simple Storage Service (Amazon S3).

Backups are protected using Amazon S3 Server-Side Encryption (SSE-S3 with AES-256 encryption), ensuring data remains encrypted both in transit and at rest.

Only authorized systems possessing the appropriate credentials and encryption permissions can retrieve backup data.

Regular backup validation and recovery testing are performed to help ensure backup integrity and disaster recovery readiness.

Confidentiality

All CTS employees and contractors involved in the development, maintenance, or support of ATLAS are bound by confidentiality agreements governing the protection of customer information.

CTS maintains strict internal security policies and follows established procedures to protect customer data throughout the software development lifecycle and ongoing system support.

Security and protection of customer information remain core organizational priorities throughout the design, deployment, operation, and maintenance of the ATLAS platform.

Attachment C

Confidentiality Agreement

THIS AGREEMENT FOR IT SERVICES (this "Agreement") dated this 17 day of July 2026,

BETWEEN

CareerSource North Central Florida (the "Customer")

OF THE FIRST PART

- AND -

Ryman, Inc. DBA: Complete Technology Solutions (CTS) of 12153 Cortez Blvd Brooksville, FL 34608 (the "Services Provider")

OF THE SECOND PART

BACKGROUND:

This agreement sets the conditions related to the access of potentially sensitive information within systems or data retention devices.

IN CONSIDERATION OF the matters described above and of the mutual benefits and obligations set forth in this Agreement, the receipt and sufficiency of which consideration is hereby acknowledged, the parties to this Agreement agree as follows:

Confidentiality.

(a) Service Provider acknowledges that as a result of the retention of Service Provider by the Customer, Service Provider has and will become informed of, and have access to, valuable and confidential information of Customer, including, but not limited to, personal information, contracts, reports, studies, drawings, contracts, business plans, inventions, trade secrets, technical information, know-how, plans and specifications (collectively, the "Confidential Information"), and that this Confidential Information, even though it may be contributed, developed or acquired by Service Provider, is the exclusive property of Customer to be held by Service Provider in trust and solely for the benefit of Customer. Service Provider shall not at any time during or subsequent to the Term use, reveal, report, publish, transfer or otherwise disclose any of the Confidential Information without the prior written consent of Customer, except to personnel with a need to know the Confidential Information for purposes of performing the Work and who agree to be bound by the terms of this Section 10. Service Provider shall inform all personnel receiving the Confidential Information of the confidential nature of this information and take all actions necessary to bind such personnel by the terms of this Section 10. Confidential Information is not information that is presently a matter of public knowledge, or which is published in or otherwise obtainable from any source available to the public without a breach of this provision by Service Provider or its personnel.

(b) In the event that the Service Provider is required, by oral questions, interrogatories, requests for information or documents, subpoena, civil investigative demand or similar process, to disclose any Confidential Information, the Service Provider will provide the Customer with prompt notice thereof so the Customer may seek an appropriate protective order and/or waive compliance by the Service Provider with the provision hereof; provided, however, that if in the absence of a protective order or the receipt of such waiver, the Service Provider is compelled to disclose Confidential Information not otherwise disclosable hereunder to any legislative, judicial or regulatory body, agency or authority or else be exposed to liability for contempt, fine or penalty or to other censure, such Confidential Information may be so disclosed.

(c) Upon the termination of this Agreement, Service Provider shall promptly deliver to Customer, without retaining copies, all contracts, letters, notes, notebooks, reports, Confidential Information, and all other property in his possession belonging to Customer or relating to the business of Customer in his

possession. Service Provider shall represent in writing to Customer that it has complied with the terms of this Section 10(c).

(d) Customer and Service Provider acknowledge that Customer would not have an adequate remedy at law for money damages if the covenants contained in this Section 10 were not complied with in accordance with their terms. Because the breach or threatened breach or any of the covenants in this Section 10 will result in immediate and irreparable injury to Customer, Service Provider agrees that Customer shall be entitled to an injunction restraining Service Provider from violating this Section 10 to the fullest extent allowed by law. Nothing in this Section 10 shall prohibit Customer from pursuing or receiving all other legal or equitable remedies that may be available to Customer for a breach or threatened breach, including the recovery of damages.

(e) The terms of this Section 10 shall survive the expiration or termination of this Agreement.

Background Screening

1. Any Contractor or subcontractor who meets the definition of "Qualified Entity" as defined in s. 943.0542, F.S.:

"Qualified Entity" means a business or organization, whether public, private, operated for profit, operated not for profit, or voluntary, which provides care or care placement services, including a business or organization that licenses or certifies others to provide care or care placement services:

a. Shall register with the Florida Department of Law Enforcement (FDLE) and have all of its employees assigned to work on this Agreement screened in a manner consistent with Section 943.0542, F.S.

b. Shall ensure that any sub-recipient or sub-contractor it retains who also meets the definition of "Qualified Entity" to also register and have all of its employees assigned to work on this Agreement (or Contract) screened in a manner consistent with Section 943.0542, F.S.

c. Shall maintain on file at the Contractor for appropriate monitoring and audit purposes verification for all personnel of Contractor and of any sub-recipient or sub-contractor, if applicable, assigned to work on this Contract of:

1. Passing the level 2 background screening standards as set forth in s. 435.04 F.S.,

2. The highest level of education claimed, if required for the position,

3. All applicable professional licenses claimed, if required by the position, and

4. Applicable employment history, if required by the position.

d. Shall obtain no later than ten days after beginning employment and subsequently maintain on file at the Contractor for appropriate monitoring and audit purposes the above verification for new personnel assigned to this Contract.

e. A level 2 background screening no earlier than five years before the effective date of this Contract shall be accepted as in compliance with this provision.

f. Shall update the background screening before the anniversary date of the initial background screening check, and every five years thereafter, if the individual continues to perform under this Contract.

g. Shall redo the background screening if there is a ninety-day lapse in employment from working on this Contract in which case the person shall be rescreened before being assigned to this Contract.

h. Shall arrange for and pay all the costs for background screenings.

2. Any Contractor or Sub-contractor who does not meet the definition of "Qualified Entity" shall nevertheless comply with all the above standards except a level 1 background screening is substituted for a level 2 screening. The level 1 screening shall include submission of fingerprints as opposed to only a name check.

3. Contractor shall:

a. Require each employee it assigns to this Contract to notify the Contractor within ten days of being arrested for any criminal offense.

b. Review the alleged offense, determine if the offense is one that would exclude the employee under a level 2 screening, and if so, remove the employee from work on this Contract.

c. The employee may not return to work on this Contract until cleared of all charges.

4. Sub-recipient or Subcontractor

a. Require each employee it assigns to a contract or subcontract with the Contractor to notify the Contractor within ten days of being arrested for any criminal offense.

- b. Review the alleged offense, determine if the offense is one that would exclude the employee under a level 2 screening, and if so, remove the employee from work on the contract or subcontract.
- c. The employee may not return to work on the contract or subcontract until cleared of all charges.

Vendor: Ryman, Inc.

per: 

Maurice Ryman

Name of Vendor's Agent

President

Title of Vendor's Agent



Complete Technology Solutions

352-666-0333