

Software Support, Maintenance and Updates Agreement

THIS SOFTWARE SUPPORT AGREEMENT (the "Agreement") dated this **9th day of November 2022** (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 (**November 9, 2022 – October 30, 2023**), updates and maintenance term for ATLAS Employer Portal software billed at \$400.00 per month (\$4,800.00 annually). Licensed module is only for *Employer Portal*.
2. After discontinuation of the Agreement, 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 12 months, with renewal for an additional 1 year. (November 1, 2023 – October 30, 2024)
14. This Agreement may be negotiated to be extended for up to one year (November 1, 2024 – October 30, 2025).
15. At the end of the term, Licensee will retain all rights to customer, document, and associated metadata.
16. Either Party may terminate this Agreement by providing the other Party with not less than sixty (60) days' prior written notice of their desire to terminate the Agreement.

Termination

17. Termination for Cause or Convenience

1. 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.
2. CareerSource North Central Florida or Contractor may terminate this Contract upon thirty (30) days prior written notice to the other party that they desire to terminate this agreement. In the event of a termination by CareerSource North Central Florida or Contractor, CareerSource North Central Florida or Contractor shall be responsible for any outstanding allowable costs incurred up through the desired termination date.
3. 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.
18. 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 images and metadata will remain the property of the licensee.

Equal Employment Opportunity

19. 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

20. (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 the [CareerSource North Central Florida](#) if the Contractor is later listed 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

21. (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

22. 23.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

23. 24.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

24. This Agreement can only be modified in writing signed by both the Vendor and the Licensee.
25. This Agreement does not create or imply any relationship in agency or partnership between the Vendor and the Licensee.
26. 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.

27. 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.
28. This Agreement contains the entire agreement between the parties. All understandings
1. 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.
29. 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) Complete Technology Solutions (Ryman, Inc.)
12155 Cortez Blvd Brooksville Fl, 34608
- b) CareerSource North Central Florida
1112 N. Main Street
Gainesville, FL 32601
C/O Phyllis Marty, Executive Director

Vendor: Complete Technology Solutions
(Ryman, Inc.)



Signature of Vendors Agent

Maurice Ryman

Name of Vendor's Agent

VP of Workforce Development Initiatives

Title of Vendor's Agent

Licensee Corporation: [CareerSource North Central Florida](#)

Signature of Licensee's Agent

[Phyllis Marty](#)
Name of Licensee's Agent

Executive Director
Title of Licensee's Agent

- ***Attachment A: Service Level Agreement***
- ***Attachment B: Security Overview***
- ***Attachment C: Confidentiality Agreement***

Attachment A

Service Level Agreement (SLA)

CareerSource North Central Florida

by

Complete Technology Solutions (CTS)

Effective Date: November 9, 2022

Document Owner:	Complete Technology Solutions
-----------------	-------------------------------

Version

Version	Date	Description	Author
1.2	11-9-2022	Service Level Agreement Reviewed	Maurice Ryman

1. Agreement Overview

This Agreement represents a Service Level Agreement (“SLA” or “Agreement”) between CTS and CareerSource North Central Florida 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(s) by the Service Provider(s).

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

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:

Service Provider(s): CTS (“Provider”)

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 affected parties. 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: 11-09-2022

Next Review Date: 10-01-2023

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
- Monthly system health check
- Updates and maintenance to software
- Continued training and support

- Data Backup
- Reviewing requests for customization to existing portals
- Bi-annual formal touchpoint meetings with customer
- Monthly CTS Newsletter distribution to customer
- Opportunity to showcase partnership at various WD Conferences highlighting best practices
- Working directly with CTS to pilot new portals

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.
- Identification of ATLAS Champion for CTS to train-the-trainer on selected ATLAS portals and services.
- 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.

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 Version 4.x Security Overview:

Administration & Security Protocols and protection of customer PII.

ATLAS has been built from the ground up to ensure complete PII adherence.

User Login and Access: SSL encryption is forced upon entering any administrative area ensuring that any/all information which is entered or retrieved is encrypted between the server and end-user device. Access to documents is only available when the administrative user has successfully validated, and the user is actively logged into the system. All administrative user interaction is validated against an ACL, or access control list, to ensure that the logged-in user has access to only the information and modules within ATLAS that an ATLAS administrator has explicitly allowed.

Additionally, the login system for admins requires a unique username and a password. Login system is secured by taking the password that the admin user provides during registration and adding a salt string to it and then encrypting it using SHA-2 (secure hash algorithm). The password once encrypted cannot be decrypted. When an administrator tries to login after registration the password, they provide in the login field has the same salt string added to it, it is encrypted using SHA-2(256) and then it is compared to the encrypted password string in the database. If the two passwords match the user is granted access, if not the user is presented with an invalid password error.

Multi Factor Authentication: Furthermore, ATLAS is also equipped with a mandatory Multi Factor Authentication system. This security measure requires all users to authenticate not only with the username/password, but also using a randomly generated 6 digit code that is either sent to the users email or via text message based on the users preference. This code is only useable for 5 minutes after the initial request.

Development Framework: Laravel is built using a core PHP framework. PHP is used as the core platform for many popular, large-scale sites. Laravel comes with many security features including Middleware. Middleware executes on every request the system handles, checking to make sure the user that is making a request not only is authenticated, but also has the correct permissions preventing any unwanted action before any code is executed.

Nightly 3rd Party Vulnerability Checks: Our system is checked nightly from a 3rd party vendor checking for 11,000+ known vulnerabilities. This database of this system is updated by the hour to ensure that our application is on top of any potential system vulnerabilities.

Geolocation Traffic Filtering: ATLAS is backed by a Geolocation filter. This system prevents all traffic from outside you desired region from even seeing the system.

Multiple Firewall Layers: ATLAS is behind 3 separate layers of firewalls ensuring the traffic that hits our systems is only desired traffic. We have firewalls in place at the DNS Level, the cloud provider level, and the system level.

3 Layers of Backups: If off-site backup option is elected, ATLAS automatically create a 3 layer backup of the ATLAS installation. The 3 layers are as follows:

1. File level backup.
 - All files from the system are encrypted* and sent to out via our S3 connection to our offsite Backup Provider every hour.
2. Database level backup.
 - All database files are exported and encrypted* as a single file backup and sent to our S3 connection to our offsite Backup Provider every hour.
3. Snapshot backup.
 - A snapshot backup is an exact image of the system that can be redeployed at any time bringing the system to the exact state that the snapshot was taken. This backup process is completed daily.

Our backups are also replicated across multiple cloud servers providing multiple points of recovery.

Database Security: ATLAS is built on a MySQL database core. The default access policy with each deployment is to deny access, and only allow connections from localhost (on-server Apache service) and the ATLAS support team. Access to port 3306 is explicitly denied from all public requests. The ATLAS support team works directly with firewall administrators on each deployment to ensure these ports are closed, and periodic testing ensures that access to MySQL from outside entities remains closed. Laravel inherently provides data sanitization to deter SQL injection and other vulnerabilities. Error and debug logs are sent to the ATLAS support team in real-time so that immediate action can be taken in the event of potential malicious activity.

System Security: All ATLAS deployments are built on an Apache web server core. All patches and updates, which solve known exploits, are performed once knowledge of exploits becomes available. The ATLAS support team works directly with regional firewall administrators to ensure that only the necessary ports are available to the public for ATLAS to function. Periodic testing ensures that only the necessary ports are open to the public. The ATLAS support team works with each region/project to ensure that their employee exit procedure include disabling the employee's administrative ATLAS account, along with verifying any other usernames/passwords that the former employee may have known so that they can be modified to eliminate future system access.

Deployment: Deployment of the ATLAS software is handled over an SSH (secure shell) connection to the remote sever that is to be updated. All data sent over this connection is secure and encrypted. All new code is deployed from our secure remote GIT repository. As updates are made and new features are added to our software, we create new versions (i.e., 3.4). Once a new version is tested and ready for deployment we push the version to our secure remote code storage repository, then we deploy that code to all the region's servers that are to receive the update. This is a completely automated program that puts the region's server into maintenance mode so no one can access the server while it is being updated, it then backs up the regions database. Once the database backup is complete, the deployment program deploys the newest code version from our repository. Each time our software is deployed to a server a new folder is created in the releases folder on the server to contain the code from that deploy, that way in the event of a bad deployment we can immediately roll back to the version from the previous deployment.

Ongoing Security: CTS maintains a strict confidentiality clause with all employees associated with the development and support of the ATLAS system. They are held to the same standard as many other State contractor employees to assure sensitive information is protected. Security of the system is a paramount priority, both within the usage of the system and from the development aspect. CTS maintains a confidentiality agreement with all our clients.

*Only the originating server, with the proper encryption key can retrieve the data.

Documentation Links:

docs.aws.amazon.com

Specifying Amazon S3 encryption - Amazon Simple Storage Service

How to add server-side encryption to an Amazon S3 object.

Attachment C

Confidentiality Agreement:

THIS AGREEMENT FOR IT SERVICES (this "Agreement") dated this 9th day of November 2022,

BETWEEN

CareerSource North Central Florida (1112 N. Main Street Gainesville, FL 32601) (the "Customer")

OF THE FIRST PART

- AND -

Ryman, Inc. DBA: Complete Technology Solutions (CTS) of 12155 Cortez Blvd Brooksville, FL 34608 (the "Services Provider")

OF THE SECOND PART

BACKGROUND:

This agreement sets the conditions as 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. 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. 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.

(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 were not complied with in accordance with their terms. Because the breach or threatened breach or any of the covenants in this section 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 to the fullest extent allowed by law. Nothing in this section 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 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 of 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

VP of Workforce Development Initiatives
Title of Vendor's Agent



Complete Technology Solutions

352-666-0333