

TO: Fiscal Review Committee

FROM: Department of Mental Health and Substance Abuse Services

DATE: August 25, 2017

SUBJECT: Amendment to Kronos Time Keeping and Scheduling System Contract

The subject Contract is between the Department of Mental Health and Substance Abuse Services and Kronos, Inc. (52497). The purpose of the Contract is for the provision of a timekeeping and scheduling system. The Department's proposed amendment would extend the contract by three years and increase the maximum liability of this contract by \$922,492.60.

The Tennessee Department of Mental Health and Substance Abuse Services operates four Joint Commission Accredited Regional Mental Health Institutes (RMHIs) across the State of Tennessee. Prior to the implementation of the system, timekeeping and scheduling is a manual process within each RMHI. These processes are very time consuming and susceptible to human error. These processes also make it difficult for changes to individual work schedules to be monitored and communicated effectively throughout the facilities.

The initial contract between the Department of Mental Health and Substance Abuse Services and Kronos, Inc. was an agency contract for one year for the Department to assess the feasibility of the solution and implement the solution at a pilot site. After the successful rollout of the system at our Middle Tennessee Mental Health Institute, we would like to amend the contract to allow us sufficient time to implement the system at our remaining three facilities and to extend the maintenance period of the contract to three years.

The system has proven to improve clinical efficiency by ensuring required staffing levels are maintained for all RMHI shifts through the use of a scheduling solution. In addition, the timekeeping solution provided by the system improves timeliness, accuracy, and accountability in staff time reporting. This solution reduces the cost of the current paper-based scheduling and timekeeping processes and makes more efficient use of existing RMHI staff.

Supplemental Documentation Required for
Fiscal Review Committee

*Contact Name:	Gene Wood	*Contact Phone:	615-532-6676		
*Presenter's name:	Gene Wood, Richard Zhu, Quinn Simpson				
Edison Contract Number: <i>(if applicable)</i>	52497	RFS Number: <i>(if applicable)</i>	n/a		
*Original or Proposed Contract Begin Date:	11/14/16	*Current or Proposed End Date:	Current: 11/13/17 Proposed: 11/13/20		
Current Request Amendment Number: <i>(if applicable)</i>		One			
Proposed Amendment Effective Date: <i>(if applicable)</i>		11/14/17			
*Department Submitting:		Mental Health & Substance Abuse Services			
*Division:		Hospital Services			
*Date Submitted:		8/31/17			
*Submitted Within Sixty (60) days:		Yes			
<i>If not, explain:</i>		n/a			
*Contract Vendor Name:		Kronos Inc.			
*Current or Proposed Maximum Liability:		Proposed: \$1,587,618.20			
*Estimated Total Spend for Commodities:		n/a			
*Current or Proposed Contract Allocation by Fiscal Year: <i>(as Shown on Most Current Fully Executed Contract Summary Sheet)</i>					
FY: 2017	FY: 2018	FY: 2019	FY: 2020	FY: 2021	FY
\$143,500.00	\$626,623.00	\$407,497.60	\$307,497.60	\$102,500.00	\$
*Current Total Expenditures by Fiscal Year of Contract: <i>(attach backup documentation from Edison)</i>					
FY: 2017	FY: 2018	FY:	FY:	FY	FY
\$143,489.34	\$12,398.80	\$	\$	\$	\$
IF Contract Allocation has been greater than Contract Expenditures, please give the reasons and explain where surplus funds were spent:			Surplus funds have not yet been spent. Time extension provides additional time to implement the timekeeping system and spend thus unspent funds after the originally anticipated end date.		
IF surplus funds have been carried forward, please give the reasons and provide the authority for the carry forward provision:					
IF Contract Expenditures exceeded Contract Allocation, please give the reasons and explain how funding was acquired to pay the overage:					
*Contract Funding Source/Amount:					
State:	\$665,125.60	Federal:			
<i>Interdepartmental:</i>		<i>Other:</i>			

Supplemental Documentation Required for
Fiscal Review Committee

If “ <i>other</i> ” please define:																				
If “ <i>interdepartmental</i> ” please define:																				
Dates of All Previous Amendments or Revisions: <i>(if applicable)</i>	Brief Description of Actions in Previous Amendments or Revisions: <i>(if applicable)</i>																			
Method of Original Award: <i>(if applicable)</i>	Sole source procurement.																			
*What were the projected costs of the service for the entire term of the contract prior to contract award? How was this cost determined?	Quote provided by vendor. Because only one vendor could provide a complete suite of products scalable and able to meet the needs of a variety of business verticals, competitive pricing information with other vendors couldn't be obtained. However, Department obtained pricing information from an existing US Communities contract and Federal GSA contract (General Services Administration) for the same type of product/service and determined the price received from vendor was fair and reasonable.																			
*List number of other potential vendors who could provide this good or service; efforts to identify other competitive procurement alternatives; and the reason a sole-source contract is in the best interest of the State.	<p>TDMHSAS needed a vendor that could provide a <u>complete</u> suite of products with functions both scalable and able to meet the needs for a variety of business verticals. The Department began researching potential solutions for a timekeeping system in fall 2015. In December 2015, TDMHSAS received results of a Vanderbilt study on potential benefits of more automation in time & attendance as well as recommendations for software solutions. They recommended Kronos as the only viable option. After extensive review, the Department was able to identify only one vendor that could provide the tools needed for TDMHSAS – Kronos. The below table provides a comparison of some of the vendors the Department reviewed:</p> <table border="1" data-bbox="922 1171 1455 1564"> <thead> <tr> <th data-bbox="922 1171 1182 1203"></th> <th colspan="2" data-bbox="1182 1171 1455 1203" style="text-align: right;">Require</th> </tr> <tr> <th data-bbox="922 1203 1182 1318">Vendor/Product</th> <th data-bbox="1182 1203 1349 1318">Time & Attendance</th> <th data-bbox="1349 1203 1455 1318">Absence Manager</th> </tr> </thead> <tbody> <tr> <td data-bbox="922 1318 1182 1381">Kronos/Workforce Management</td> <td data-bbox="1182 1318 1349 1381" style="text-align: center;">Yes</td> <td data-bbox="1349 1318 1455 1381" style="text-align: center;">Yes</td> </tr> <tr> <td data-bbox="922 1381 1182 1413">*Ceridian/Dayforce</td> <td data-bbox="1182 1381 1349 1413" style="text-align: center;">Yes</td> <td data-bbox="1349 1381 1455 1413" style="text-align: center;">Yes</td> </tr> <tr> <td data-bbox="922 1413 1182 1476">*Success Factors (SAP Partnership)</td> <td data-bbox="1182 1413 1349 1476" style="text-align: center;">No</td> <td data-bbox="1349 1413 1455 1476" style="text-align: center;">No</td> </tr> <tr> <td data-bbox="922 1476 1182 1564">Workday (used to be PeopleSoft, now separate entity)</td> <td data-bbox="1182 1476 1349 1564" style="text-align: center;">No</td> <td data-bbox="1349 1476 1455 1564" style="text-align: center;">Yes</td> </tr> </tbody> </table> <p data-bbox="922 1564 1455 1621">*SaaS (Software as a Service) cannot be installed within the State's data center</p>			Require		Vendor/Product	Time & Attendance	Absence Manager	Kronos/Workforce Management	Yes	Yes	*Ceridian/Dayforce	Yes	Yes	*Success Factors (SAP Partnership)	No	No	Workday (used to be PeopleSoft, now separate entity)	No	Yes
	Require																			
Vendor/Product	Time & Attendance	Absence Manager																		
Kronos/Workforce Management	Yes	Yes																		
*Ceridian/Dayforce	Yes	Yes																		
*Success Factors (SAP Partnership)	No	No																		
Workday (used to be PeopleSoft, now separate entity)	No	Yes																		

Rule Exception Request

Use this document to request changes to Central Procurement Office templates, policies, or other procurement documents or to modify the "necessary contract clauses" identified in Tenn. Comp. R. & Reg. 0690-03-01-.17 ("CPO Rule 17"). Complete this document in conformity with CPO Rule 17, which is available [here](#). Send the completed document in PDF format to: AgSprs.Agsprs@tn.gov All Rule Exception Requests are subject to review and approval by the Chief Procurement Officer. Rule Exception Requests that propose to modify any of CPO Rule 17's necessary contract clauses shall be subject to review and approval by the Comptroller of the Treasury.

APPROVED
Kevin C. Bartels for
Michael F. Perry
 CHIEF PROCUREMENT OFFICER

Digitally signed by Kevin C. Bartels for Michael F. Perry
 DN: cn=Kevin C. Bartels for Michael F. Perry,
 o=CPO, ou, email=Kevin.C.Bartels@tn.gov, c=US
 Date: 2016.10.19 08:59:36 -05'00'

APPROVED

 COMPTROLLER OF THE TREASURY

Agency request tracking #	
1. Procuring Agency	Mental Health & Substance Abuse Services
2. Edison contract ID #	
3. Contractor or Grantee	Kronos Incorporated
4. Contract's Effective Date	October 2016 (est)
5. Contract or grant contract's Term (with ALL options to extend exercised)	Not to exceed 12 months
6. Contract's Maximum Liability (with ALL options to extend exercised)	\$ 665,125.60
7. Citation and explanation of the rule(s) for which the exception is requested	<p>Per FA Template: Procurement professionals shall adhere to this template with revisions only as instructions permit. Changes to this template require a Rule Exception as set forth in Tenn. Comp. R. & Regs. 0690-03-01-.17 and the <i>Procurement Procedures Manual of the Central Procurement Office</i>.</p> <p>0690-03-01-.17 NECESSARY OR PROHIBITED CONTRACT CLAUSES AND RULE EXCEPTIONS.</p> <p>(1) The purpose of this Rule is to prescribe the necessary and prohibited contract clauses for contracts subject to these Rules. The form and content of all contract clauses shall be established by Central Procurement Office Policy. This Rule shall also prescribe a procedure for approving exceptions or modifications to contract.</p>

<p>8. Description of requested changes if adding new provisions or modifying existing provisions, insert the new or modified provisions in their entirety.</p>	<p>Following consultation with CPO and STS, Department requests the following modifications to provisions listed below and attachments hereto:</p> <p><u>STS provisions</u></p> <p><u>A.x. Security Plan.</u> Contractor shall maintain the AICPA SSAE 16 SOC 1 Type II and the AT 101 SOC 2 Type II security standard in the Contractor Private Cloud environment for the security, availability and confidentiality criteria. Said criteria provide a framework for proactively guarding against security threats, unauthorized access, use and disclosure, unauthorized or accidental destruction or change and accidental loss and shall</p> <ol style="list-style-type: none"> (1) Protect all information and design information security controls in order to ensure: <ol style="list-style-type: none"> i. Integrity, which means guarding against improper information modification or destruction, and includes ensuring information authenticity; ii. Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and iii. Availability, which means ensuring timely and reliable access to and use of information. (2) Secure the System and the information contained therein that connects to the State network, regardless of location. (3) Adopt and implement, at a minimum, the policies, procedures, controls, and standards consistent with the AICPA Trust Principles Criteria for security, confidentiality and availability and the State's Enterprise Information Security Policies (included as Attachment 12) to ensure the integrity, confidentiality, and availability of information and information systems for which Contractor is responsible under this contract or to which it may otherwise have access under this contract. (4) Contractor shall ensure that each user role is based on the business functions they are required to perform. Annually upon request, the State shall receive the report of an independent third party auditor attesting to controls in place in the environment, including vulnerability scanning and remediation. (5) Staff with data access shall sign a nondisclosure agreement. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of State data, Contractor shall afford the State access to Contractor's facilities. Such inspections shall be limited to a guided tour of the data center facility, completion of an industry standard questionnaire, examination of the results of the annual AICPA SOC 1 and SOC 2 Type II audit conducted by an independent third party, and reasonable access to knowledgeable personnel to discuss the controls in place. For the avoidance of doubt, in no event shall the State or its designees be permitted to access Processor's systems, network servers, scan summaries or activities logs. (6) Through the publication of its annual SOC reporting, Contractor shall disclose its non-proprietary security processes and technical limitations to the State. The State and the Contractor shall understand each other's roles and responsibilities. (7) Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of data. Such security measures shall be in accordance with recognized industry practice and not less
--	---

stringent than the measures Contractor applies to its own personal data.

A.x. Data Recovery Plan. The State's environment and all State data in the Contractor Cloud will be replicated to a secondary Contractor Cloud data center. Basic Disaster Recovery Services provides a Recovery Point Objective (RPO) of 24 hours and Contractor strives to restore Application Availability in a commercially reasonable timeframe ✓

A.x. Compliance with State Enterprise Information Policies and applicable laws. The Contractor is required conform with the State Enterprise Information Policies as amended and attached as Attachment 12 and to all applicable State and Federal laws regarding information security. As additional State and Federal regulatory requirements are imposed upon Contractor, the Contractor shall ensure that the environment, content and applications are kept up to date with the emerging and applicable requirements. In the event that additional State and Federal requirements are imposed upon Contractor, and these requirements result in additional cost to Contractor, Contractor may request that its prices be equitably adjusted to reflect the additional cost. The State may propose an amendment to the Contract to grant Contractor's requested price increase. In the event the State does not approve an amendment to the Contract granting the requested price increase, Contractor may terminate the Contract and such termination refusal shall not be considered a breach of contract. The Contractor shall be entitled to compensation for all conforming goods delivered in accordance with the Contract and authorized services completed as of the termination date. In no event shall the State be liable to the Contractor for compensation for any goods neither requested or for any services neither requested by the State nor performed by the Contractor. In no event shall the Contractor's exercise of its right to terminate this Contract under this Section relieve either party of any liability for any other damages or claims arising under this Contract. ✓

A.x. Encryption. All data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for enforcing the encryption of the data. The Contractor shall ensure drive encryption consistent with AES 256 bit standard or higher. ✓

A.x. Separation of Duties. To reduce the risk of accidental change or unauthorized access to operational software and business data, the State should be a separation of duties based on test, and production environment. The State Content will be included in the State databases, in either the production or testing environment. The Contractor will have the same security obligations for both environments. ✓

The Contractor shall limit staff knowledge of State data to that which is need to know to perform job duties

A.x. Removable Media. To the extent applicable, removable media should be sanitized prior to removing it from the facilities for maintenance or repair. Removable media should be disposed of securely when no longer required, using approved State procedures. Removable media containing confidential information, confidential data, or sensitive data must be protected against unauthorized access, misuse or corruption during transport. ✓

A.x. Malicious Code. The Contractor shall represent and warrant that it has tested the Application using commercially reasonable methods designed to ensure that upon providing access to State, the Application is free from all computer viruses, worms, time-outs, other harmful or malicious code intended to or can disrupt, erase or otherwise harm the Application, Equipment, or State's software, hardware, networks, data or information. ✓

A.x. Protection of Information. The Contractor shall be responsible for properly protecting the State's Confidential Information processed and stored as a result of work under this contract. All Confidential Information shall be protected by both parties to the same extent they would their own proprietary data, Personally Identifiable Data and/or company trade secrets. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct ✓

as applicable to Privacy Act Information. The State will retain unrestricted rights to State data. The State also maintains the right to request full copies of the data at any time.

The data that is processed and stored by the various applications within the network cloud environment may contain financial data as well as Personally Identifiable Information (PII). This data shall be protected against unauthorized access, disclosure or modification, theft, or destruction as set forth in Section A.21. The Contractor shall ensure that the facilities that house the network infrastructure are physically secure. The data must be available to the State upon written request within one business day or within the timeframe specified otherwise, and shall not be used for any other purpose other than that specified herein. During the Term and no more than fifteen (15) days after termination, the Contractor shall provide requested data at no additional cost to the State. After such period, Contractor shall have no further obligations to store, or make available the State Content and will securely delete any and all State Contract without liability.

a. Acceptable Use:

- (1) The State shall take all reasonable steps to ensure that no unauthorized persons have access to the Services, and to ensure that no persons authorized to have such access shall take any action that would be in violation of this contract.
- (2) The State represents and warrants to Contractor that the State has the right to publish and disclose the State Content in connection with the Services. The State represents and warrants to Contractor that the State Content: (a) does not infringe or violate any third-party right, including but not limited to intellectual property, privacy, or publicity rights, (b) is not abusive, profane, defamatory or offensive to a reasonable person, or, (c) is not hateful or threatening.
- (3) The State will not (a) use, or allow the use of, the Services in contravention of any federal, state, local, foreign or other applicable law, or rules or regulations of regulatory or administrative organizations; (b) introduce into the Services any virus or other code or routine intended to disrupt or damage the Services, or alter, damage, delete, retrieve or record information about the Services or its users; (c) excessively overload the Contractor systems used to provide the Services; (d) perform any security integrity review, penetration test, load test, denial of service simulation or vulnerability scan; (e) use any tool designed to automatically emulate the actions of a human user (e.g., robots); or, (f) otherwise act in a fraudulent, malicious or negligent manner when using the Services.
- (4) The State shall be responsible with respect claims alleging that: (a) employment-related claims arising out of State's configuration of the Services; (b) State's modification or combination of the Services with other services, software or equipment not furnished by Contractor, provided that such State modification or combination is the cause of claim and was not authorized by Contractor; or, (c) that the State Content infringes in any manner any intellectual property right of any third party, or any of the State Content contains any material or information that is obscene, defamatory, libelous, or slanderous violates any person's right of publicity, privacy or personality, or has otherwise caused or resulted in any tort, injury, damage or harm to any other person.

- b. Connectivity and Access. The State acknowledges that the State shall (a) be responsible for securing, paying for, and maintaining connectivity to the Services (including any and all related hardware, software, third party services and related equipment and components); and (b) provide Contractor and Contractor's representatives with such physical or remote access to the State's computer and network environment as

	<p>Contractor deems reasonably necessary in order for Contractor to perform its obligations under the contract. The State will make all necessary arrangements as may be required to provide access to the State's computer and network environment if necessary for Contractor to perform its obligations under the contract.</p> <p>A.x. <u>Data Location.</u> The Contractor shall provide its services to the State and its end users solely from data centers in the United States of America. Storage of State data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store State data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access State data remotely only as required to provide technical support and other services ✓</p> <p>A.x. <u>Data Ownership.</u> The State will own all right, title and interest in its data that is provided in relation to the services provided by this contract. The Contractor shall not access State user accounts or State data except: ✓</p> <ol style="list-style-type: none"> 1. In the course of data center operations, 2. In response to service or technical issues, 3. As required by the express terms of this contract, or 4. At the State's written request. <p>All data obtained by the Contractor from the State in the performance of this contract shall remain the property of the State.</p> <p>Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of State information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of State information and comply with the following conditions:</p> <ol style="list-style-type: none"> 1. At no time shall any data or processes that either belong to or are intended for the use of the State or its officers, agents or employees, be copied, disclosed or retained by the Contractor for subsequent use in any transaction that does not include the State. 2. The Contractor shall not use any information of the State delivered by the State in connection with the service for any purpose other than fulfilling the service. <p>A.x. <u>Import and Export of Data.</u> The State shall have the ability to Import or export State Content or State data piecemeal or in entirety at its discretion without interference from the Contractor. This includes the ability for the State to import or export the State's data to or from other service providers. ✓</p> <p>A.x. <u>Transfer of Data.</u> Upon request from the State made within 15 days from the termination of this Contract all data hosted and processed by the State on Contractor's equipment shall be removed and returned to the State in a usable format in use at the time of the request, unless the parties enter into a similar, successive Contract. Upon such return in the event of termination of the contract, Contractor shall have no further obligation to store or make available the State content and will sanitize any and all State Content in accordance with this Contract ✓</p> <p>A.x. <u>Access to Security Logs and Reports.</u> Contractor shall provide reports to the State in a format as agreed to by both the Contractor and the State. Reports shall include latency statistics, user access, user access IP address, Application-level user access history and Applicable-level security logs for all State files related to this contract. For avoidance of doubt, in no event shall the State or its designees be permitted to access Contractor's systems, network ✓</p>
--	--

	<p>servers, scan summaries or activities logs.</p> <p>A.x. <u>Physical Security.</u> All enterprise data processing facilities that process or store data shall have multiple layers of physical security. Each layer should be independent and separate of the preceding and/or following layer(s).</p> <p>All facilities should have, at a minimum, a single security perimeter protecting it from unauthorized access, damage and/or interference. Secure areas should be protected by appropriate entry controls to restrict access only to authorized personnel. Procedures for working in secure areas should be created and implemented. Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled, and if possible, isolated from information processing facilities. Equipment should be located in secured areas or protected to reduce the risks from environment threats and hazards, and to reduce the opportunities for unauthorized access. Secured cabinets or facilities should support further segregation based on role and responsibility.</p> <p>Users should ensure that unattended data processing equipment has appropriate protection. All systems and devices owned and operated by or on behalf of the State should be configured to clear and lock the screen or log the user off the system after a defined period of inactivity.</p> <p>The Contractor shall inspect the results of an independent audit of its data centers at least annually, and provide a redacted version of the audit report upon request. The Contractor may remove its proprietary information from the redacted version. Contractor shall also continuously monitor the data center's performance, including frequent visits to the site.</p> <p>A.23. <u>Assessment of the System.</u> The Contractor is responsible for mitigating all security risks found during any assessment and continuous monitoring activities.</p> <p>A.x. <u>System Patching and Penetration Scanning.</u></p> <ol style="list-style-type: none"> 1. The Contractor will conduct periodic and special vulnerability scans, and install software / hardware patches and upgrades to protect all automated information assets. These audits shall be performed by Kronos using a third party tool, of the internal and external user interface, annually. 2. The Contractor must submit, for review the proposed scope of testing as well as the name and qualifications of the party performing the tests. The Contractor is responsible for the costs of this testing. 3. The Contractor must address and resolve any high or critical vulnerabilities in the Application or Service as identified by the scanning tool. The Contractor must arrange for repeat testing to ensure that all identified vulnerabilities have been addressed. 4. Kronos shall conduct as part of its security program, on at least an annual basis, contract with an independent third party to conduct a network and application penetration test on the then most recent version of the application released to market in the shared computing environment of the Kronos network containing Customer Data (i.e. Kronos Cloud). The penetration test will include, but is not limited to, the potential for unauthorized internet access, compromise of roles, and escalation of privileges for the application. Kronos will provide an executive summary of such penetration test including the scope and methodology of the test and confirmation that high and critical Risk Findings as identified by the scanning tool have been remediated or a plan (including time frame) is in place to remediate. Customer may choose to elect to purchase additional application penetration testing of any custom code delivered to the customer on behalf of Kronos. Penetration testing includes the web application vulnerabilities defined by the Open Web Application Security Project (OWASP) Top 10 and those listed in the SANS 25 (as applicable) or its successor current at the time of the test. <p>A.x. <u>Data Security</u> As part of the Services for the Extension Applications, Kronos shall provide</p>
--	---

those administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of State data as described in Attachment 11 herein [requesting approval of this via RER – attachment 11 is attached].

E.3. Security and Standards-Compliance Requirements.

- (a) Data Security. As part of the Services, Contractor shall provide those administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of State data as described in Attachment 6.

State acknowledges that such safeguards endeavor to mitigate security incidents, but such incidents may not be mitigated entirely or rendered harmless. State should consider any particular Contractor supplied security-related safeguard as just one tool to be used as part of State's overall security strategy and not a guarantee of security. Both parties agree to comply with all applicable privacy or data protection statutes, rules, or regulations governing the respective activities of the parties under the Agreement.

As between State and Contractor, all Personally Identifiable Data is State's Confidential Information and will remain the property of State as set forth in section E.2 above. State represents that to the best of State's knowledge such Personally Identifiable Data supplied to Contractor is accurate. State hereby consents to the use, processing or disclosure of Personally Identifiable Data by Contractor and Contractor's Suppliers wherever located only for the purposes described herein and only to the extent such use or processing is necessary for Contractor to carry out Contractor's duties and responsibilities under the Agreement or as required by law.

Prior to initiation of the Services under the Agreement and on an ongoing basis thereafter, State agrees to provide notice to Contractor of any extraordinary privacy or data protection statutes, rules, or regulations which are or become applicable to State's industry and which could be imposed on Contractor as a result of provision of the Services. State will ensure that: (a) the transfer to Contractor and storage of any Personally Identifiable Data by Contractor or Contractor's Supplier's data center is permitted under applicable data protection laws and regulations; and, (b) State will obtain consents from individuals for such transfer and storage to the extent required under applicable laws and regulations.

- (b) Security Certification, Accreditation, Audit. Annually at the State's request, the contractor shall provide proof of any security certifications, accreditation, or audit on a yearly basis to the State to validate the hosting solution security. (Examples: SOC 2 Type II/ SOC 3, ISO 27001). The State shall receive the report of an independent third party auditor attesting to controls in place in the environment, including vulnerability scanning and remediation. In addition, the State may request annually to proceed with an inspection. Such inspections shall be limited to a guided tour of the data center facility, completion of an industry standard questionnaire, examination of the results of the annual AICPA SOC 1 and SOC 2 Type II audit conducted by an independent third party, and reasonable access to knowledgeable personnel to discuss the controls in place. For the avoidance of doubt, in no event shall the State or its designees be permitted to access Processor's systems, network servers, scan summaries or activities logs.

- (c) Security Incident and Data Breach. Contractor shall inform the State of any security incident or data breach impacting the State Content. The Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise, defined by laws (including such applicable privacy laws) or contained in the contract. Discussing security incidents with the State should be handled on an urgent as-needed basis, as part of Contractor communication and mitigation processes, defined by law or contained in the contract.

Contractor shall report any security incident to the appropriate State identified

contact immediately. If Contractor has actual knowledge of a confirmed data breach that affects the security of any State content that is subject to applicable data breach notification law, Contractor shall:

1. Promptly notify the appropriate State identified contact within 24 hours or sooner, unless shorter time is required by applicable law,
2. Take commercially reasonable measures to investigate perceived security incidents to address the data breach in a timely manner
3. Cooperate with the State as reasonably requested by the State to investigate and resolve the data breach,
4. Promptly implement necessary remedial measures, if necessary, and
5. Document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

Unless otherwise stipulated, if a data breach is a direct result of the Contractor breach of its contract obligation to encrypt personal data or otherwise prevent its release, prevent malicious code as provided in Section A.11 of this Contract, or to protect the credentials of Contractor's employees or subcontractors, the Contractor shall bear the costs of remedial measures as required by laws consistent with the contract which may include: (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state law; (3) a credit monitoring service required by state (or federal) law; (4) a website or a toll-free number and call center for affected individuals required by state law - all not to exceed the average per record per person cost calculated for data breaches in the United States (currently \$201 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause; all [(1) through (5)] subject to this contract's limitation of liability.

E.x. Intellectual Property. The Contractor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all claims or suits which may be brought against the State concerning or arising out of any claim of an alleged patent, copyright, trade secret or other intellectual property infringement. In any such claim or action brought against the State, the Contractor shall satisfy and indemnify the State for the amount of any settlement or final judgment, and the Contractor shall be responsible for all legal or other fees or expenses incurred by the State arising from any such claim. The State shall give the Contractor notice of any such claim or suit, however, the failure of the State to give such notice shall only relieve Contractor of its obligations under this Section to the extent Contractor can demonstrate actual prejudice arising from the State's failure to give notice. This Section shall not grant the Contractor, through its attorneys, the right to represent the State of Tennessee in any legal matter, as provided in Tenn. Code Ann. § 8-6-106.

The State may participate in the defense of such action with counsel of its own selection and at its sole cost. Contractor shall have no liability to indemnify or defend State to the extent the alleged infringement is based on: (a) a modification of the Services by anyone other than Contractor; (b) use of the Services other than in accordance with the Documentation for such Service or as authorized by the Contract; (c) use of the Services in conjunction with any data, equipment, service or software not provided or approved by Contractor, where the Services would not otherwise itself be infringing or the subject of the claim; or (d) use of the Services by State other than in accordance with the terms of the contract.

FA Template sections:

A.1. The Contractor shall provide the goods or services and deliverables as described, and detailed Section A.3 below and both parties shall meet all service and delivery timelines as specified by this Contract.

A.x. Change Orders. The State may, at its sole discretion and within written notice to the Contractor, request changes in the Scope that are necessary but were inadvertently unspecified in this contract. ✓

a. Change Order Creation. After receipt of a written request for additional services from the State, the Contractor shall respond to the State, within a maximum of ten (10) business days, with a written proposal for completing the service. Contractor's proposal must specify:

- (1) The effect, if any, of implementing the requested change(s) on all other services required under this Contract;
- (2) The specific effort involved in completing the change(s);
- (3) The specific schedule for completing the change(s);
- (4) The maximum number of person hours required for the change(s); and
- (5) The maximum cost for the change(s) – this maximum cost shall in no instance exceed the product of the person hours required multiplied by the appropriate payment rate proposed for such work.

The Contractor shall not perform any additional service until the State has approved the proposal. If approved, the State will sign the proposal, and it shall constitute a Change Order between the Contract Parties pertaining to the specified change(s) and shall be incorporated, hereby, as a part of this Contract.

b. Change Order Performance. Subsequent to creation of a Change Order, the Contractor shall complete the required services. The State will be the sole judge of the acceptable completion of work and, upon such determination, shall provide the Contractor written approval.

A.x. Warranty Contractor represents and warrants that the term of the warranty ("Warranty Period") shall be the Term of this Contract. If Contractor fails to provide the goods or services as warranted, then Contractor will re-provide the goods or services at no additional charge. Any nonconformance of the goods or services to the terms and conditions of this Contract, including any SLAs and support obligations of Contractor, shall constitute a "Defect" and shall be considered "Defective." If Contractor receives notice of a Defect during the Warranty Period, then Contractor shall correct the Defect, at no additional charge. If Contractor is unable or unwilling to re-provide the goods or services as warranted 15 days after receiving notice, then the State shall be entitled to recover the fees paid to Contractor for the Defective goods or services during the period in which the Defective goods and services were unavailable. Any exercise of the State's rights under this Section shall not prejudice the State's rights to seek any other remedies available under this Contract and applicable law. ✓

Except as provided for in this section A.26, Contractor hereby disclaims all warranties, conditions, guaranties and representations relating to the Services, express or implied, oral or in writing, including without limitation the implied warranties of merchantability, fitness for a particular purpose, title and non-infringement, and whether or not arising through a course of dealing. The Services are not guaranteed to be error-free or uninterrupted. Except as specifically provided in this Contract, Contractor makes no warranties or representations concerning the compatibility of the Services, the SaaS Applications or the Equipment nor any results to be achieved therefrom.

a. Application Warranty. The Services provided under this Contract, when used, under normal operation as specified in the Documentation and when used as authorized herein, shall perform in accordance with the Documentation throughout the Warranty Period.

Contractor represents and warrants that all Services provided under this Contract shall be provided in a timely and professional manner, by qualified and skilled individuals, and in conformity with the terms of the Contract.

- b. **Equipment Warranty.** Contractor warrants to the State that each item of Equipment shall be free from Defects during the Warranty Period. This warranty is extended to State only and shall not apply to any Equipment (or parts thereof) to the extent occurring as a result of the following:
 - i. damage, defects or malfunctions resulting from misuse, accident, neglect, tampering, (including without limitation modification or replacement of any Contractor components on any boards supplied with the Equipment), unusual physical or electrical stress or causes other than normal and intended use;
 - ii. failure of State to provide and maintain a suitable installation environment, as specified in the published specifications for such Equipment; or
 - iii. malfunctions resulting from the use of badges or supplies not approved by Contractor.

C.1. **Maximum Liability.** In no event shall the maximum liability of the State under this Contract exceed six hundred sixty five thousand one hundred twenty five dollars and sixty cents (\$665,125.60) ("Maximum Liability"). This Contract does not grant the Contractor any exclusive rights. The State does not guarantee that it will buy any minimum quantity of goods or services under this Contract except as set forth in Section C.3 below. Subject to the terms and conditions of this Contract, the Contractor will only be paid for goods or services provided under this Contract after an invoice is issued by Contractor to the State as specified by this Contract.

C.2. **Compensation Firm.** The payment methodology in Section C.3. of this Contract shall constitute the entire compensation, except as provided in this Section C, due the Contractor for the goods or services provided under this Contract regardless of the difficulty, materials or equipment required. The payment methodology includes all applicable taxes, fees, overhead, and all other direct and indirect costs incurred or to be incurred by the Contractor.

C.3. **Payment Methodology.** The Contractor shall be compensated based on the payment methodology for goods or services authorized by the State in a total amount as set forth in Section C.1.

- a. The Contractor's compensation shall be in accordance with the terms of the contract.
- b. The Contractor shall be compensated based upon the following payment methodology:

Quantities listed in the following tables are the MINIMUM quantities to be purchased under this agreement; additional quantities are possible with the same unit prices.

APPLICATIONS

Item/License	Qty	PEPM	Monthly Price
Workforce Timekeeper	1500	\$4.27	\$6,405.00
Workforce Employee	1500	\$0.00	Included
Workforce Manager	150	\$0.00	Included
Workforce Integration Manager	1500	\$0.00	Included
Workforce Mobile Employee	1500	\$0.00	Included
Workforce Mobile Manager	150	\$0.00	Included
Workforce Scheduler	1500	\$1.30	\$1,950.00
Workforce Forecast Manager for Healthcare Section A.34	1500	\$1.83	\$2,745.00
Workforce Extensions for Healthcare	1	\$0.00	\$0.00

Encryption Gateway for Kronos Cloud Section A.34			
Workforce Absence Manager	1500	\$1.30	\$1,950.00
KSS Tool Attestation Tool Kit	1500	\$0.26	\$390.00
Workforce Analytics	1500	\$2.12	\$3,180.00

RENTAL EQUIPMENT

Item	Qty	Total Price
Implementation WFC SaaS Attachment 7		\$157,628.00
KnowledgePass SaaS WFC		Included
Training Points WFC SaaS	45,250	Included

CORE PROFESSIONAL / EDUCATIONAL SERVICES* SUMMARY

Item	Qty	Unit Price	Monthly Price
Kronos InTouch 9000 H3, Standard, HID Prox	67	\$102.40	\$6,860.80
Touch ID Option for H1/H2/H3 InTouch	67	\$32.00	\$2,144.00
North America Power Kit for Mount Over Outlet - InTouch STD	67	\$0.00	\$0.00

CLOUD SERVICES SUMMARY

Item	Duration	Total Price
Cloud Hosting Encryption at Rest of Customer at Storage Level		\$0.00

Ninety (90) days following the Effective Date of the Contract, contractor will invoice the Application and rental equipment fees listed in C.3.b. monthly at the commencement of each month. Any credits, if applicable under the Attachment 5, Service Level Agreement, will be applied to the following month's invoice.

*Professional/Educational Service fees will be made using the following methodology/milestones:

- (1) Delivery and Acceptance of Project Initiation Documents (20%) including
 - i. Kickoff Meeting and Presentation as referenced in Section A.3.g
 - ii. Master Project Management Plan as referenced in Section A.3.h.(1)
 - iii. Implementation Plan as referenced in Section A.3.i
 - iv. Operations Guide as referenced in Section A.3.j
 - v. Security Plan as referenced in Section A.3.k
 - vi. Data Recovery Plan as referenced in Section A.3.l
 - vii. Training Plan as referenced in Section A.3.m
- (2) Delivery and Acceptance of Implementation and Training at the Pilot Regional Mental Health Institute (RMHI) (25%) including: Post Implementation Assessment for the Pilot site as referenced in Section A.3.n
- (3) Delivery and Acceptance of Implementation and Training at the State's remaining three RMHIs (25%) including: Post Implementation Assessment for the three sites as referenced in Section A.3.n
- (4) Final Acceptance / Sign-off of Project (30%) including: Final Project Report as referenced in Section A.3.o

- c. The Contractor shall be compensated for changes requested and performed pursuant to Contract Section A.6, without a formal amendment of this Contract based upon the payment rates detailed in the schedule below and as agreed pursuant to Section A.3 and Attachment 2, PROVIDED THAT compensation to

the Contractor for such "change order" work shall not exceed \$200,000. If, at any point during the Term, the State determines that the cost of necessary "change order" work based on Attachment 2 would exceed the maximum amount, the State may amend this Contract to address the need.

Service Description	Amount (per compensable increment)
Consulting/Implementation Services	(500 hours x \$200/hour) \$100,000
Optional components (from Attachment 2)	\$100,000

C.6. Payment of Invoice. The State payment terms are Net 45 days from the State receipt and the State shall not prejudice the State's right to object to or question any payment, invoice, or other related matter. Unless otherwise set forth in this contract, a payment by the State shall not be construed as acceptance of goods delivered, any part of the services provided, or as approval of any amount invoiced. Payment shall be in accordance with the Prompt Payment Act.

D.4. Subject to Funds Availability. The Contract is subject to the appropriation and availability of State or federal funds. In the event that the funds are not appropriated or are otherwise unavailable, the State reserves the right to terminate this Contract upon a thirty (30) days prior written notice to the Contractor. The State's exercise of its right to terminate this Contract shall not constitute a breach of Contract by the State. Upon receipt of the written notice, the Contractor shall cease all work associated with the Contract. If the State terminates this Contract due to lack of funds availability, the Contractor shall be entitled to compensation for all conforming goods requested and delivered in accordance with the contract as of the termination date. Should the State exercise its right to terminate this Contract due to unavailability of funds, the Contractor shall have no right to recover from the State any actual, general, special, incidental, consequential, or any other damages of any description or amount.

D.5. Termination for Convenience. The State may terminate this Contract for convenience without cause and for any reason. The State shall give the Contractor at least thirty (30) days written notice before the termination date. The Contractor shall be entitled to compensation for all conforming goods delivered in accordance with the contract, authorized services completed as of the termination date. In no event shall the State be liable to the Contractor for compensation for any goods neither requested or for any services neither requested by the State nor performed by the Contractor. In no event shall the State's exercise of its right to terminate this Contract for convenience relieve the Contractor of any liability to the State for any damages or claims arising under this Contract.

D.6. Termination for Cause. If the Contractor fails to properly perform its obligations under this Contract in a material manner, or if the Contractor materially violates any terms of this Contract ("Breach Condition"), the State shall have the right to terminate the Contract if such breach is not cured within fifteen (15) days after the receipt of the contract written notice. The State may withhold payments in excess of compensation for completed services or provided Equipment subject to such breach. Notwithstanding the above, the Contractor shall not be relieved of liability to the State for damages sustained by virtue of any Breach Condition and the State may seek other remedies allowed at law or in equity consistent with the terms of the contract for breach of this Contract. For purposes of this Contract, "material breach" means, with respect to a given breach, that a reasonable person in the position of the nonbreaching party would wish to terminate this agreement because of that breach.

Contractor may terminate the Services and the contract upon a material breach

of the contract by the other party if such breach is not cured within thirty (30) days after receipt of written notice.

- D.10. Prohibition of Illegal Immigrants. The requirements of Tenn. Code Ann. § 12-3-309 addressing the use of illegal immigrants in the performance of any contract to supply goods or services to the state of Tennessee, shall be a material provision of this Contract, a breach of which shall be grounds for monetary and other penalties, up to and including termination of this Contract. ✓
- a. The Contractor agrees that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Contract. Upon request from the State, the Contractor shall reaffirm this attestation, in writing, by submitting to the State a completed and signed copy of the document at Attachment 3, semi-annually during the Term. If the Contractor is a party to more than one contract with the State, the Contractor may submit one attestation that applies to all contracts with the State. All Contractor attestations shall be maintained by the Contractor and made available to State officials upon request.
 - b. Prior to the use of any subcontractor in the performance of this Contract, and semi-annually thereafter, during the Term, the Contractor shall obtain and retain a current, written attestation that the subcontractor shall not knowingly utilize the services of an illegal immigrant to perform work under this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant to perform work under this Contract. Attestations obtained from subcontractors shall be maintained by the Contractor and made available to State officials upon request.
 - c. The Contractor shall maintain records for all personnel used in the performance of this Contract. Contractor's records shall be subject to review and random inspection at any reasonable time upon reasonable notice by the State.
 - d. The Contractor understands and agrees that failure to comply with this section will be subject to the sanctions of Tenn. Code Ann. § 12-3-309 for acts or omissions occurring after its effective date.
 - e. For purposes of this Contract, "illegal immigrant" shall be defined as any person who is not: (i) a United States citizen; (ii) a Lawful Permanent Resident; (iii) a person whose physical presence in the United States is authorized; (iv) allowed by the federal Department of Homeland Security and who, under federal immigration laws or regulations, is authorized to be employed in the U.S.; or (v) is otherwise authorized to provide services under the Contract.
- D.11. Records. The Contractor shall maintain documentation for all charges under this Contract. The books, records, and documents of the Contractor, for work performed or money received under this Contract, shall be maintained for a period of five (5) full years from the date of the final payment and shall be subject to audit at any reasonable time (not more than once per year) and upon a thirty (30) days prior reasonable notice by the State, the Comptroller of the Treasury, or their duly appointed representatives. The financial statements shall be prepared in accordance with generally accepted accounting principles and may be made available subject to a confidentiality agreement. ✓
- D.12. Monitoring. The Contractor's activities conducted and records maintained pursuant to this Contract shall be subject to monitoring and evaluation by the State, the Comptroller of the Treasury, or their duly appointed representatives in accordance with Section A. ✓
- D.13. Progress Reports. The Contractor shall submit brief, periodic, progress reports to the State as requested in accordance with Section A. ✓

D.16 Patient Protection and Affordable Care Act. To the extent applicable and such information is required for the purposes of this Contract, the Contractor agrees that it will be responsible for compliance with the Patient Protection and Affordable Care Act ("PPACA") with respect to itself and its employees, including any obligation to report health insurance coverage, provide health insurance coverage, or pay any financial assessment, tax, or penalty for not providing health insurance. The Contractor shall indemnify the State and hold it harmless for any costs to the State arising from Contractor's failure to fulfill its PPACA responsibilities for itself or its employees. ✓

D.19. Hold Harmless. The Contractor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all claims, liabilities, losses, and causes of action which may arise, accrue, or result to any person, firm, corporation, or other entity which may be injured or damaged as a result of wrongful acts, omissions, or negligence on the part of the Contractor, its employees, or any person acting for or on its or their behalf relating to this Contract. The Contractor further agrees it shall be liable for the reasonable cost of attorneys for the State to enforce the terms of this Contract. ✓

In the event of any suit or claim, the Parties shall give each other immediate notice and provide all necessary assistance to respond. The failure of the State to give notice shall only relieve the Contractor of its obligations under this Section to the extent that the Contractor can demonstrate actual prejudice arising from the failure to give notice. This Section shall not grant the Contractor, through its attorneys, the right to represent the State in any legal matter, as the right to represent the State is governed by Tenn. Code Ann. § 8-6-106.

D.20. HIPAA Compliance. To the extent applicable under the scope of this Contract, the State and Contractor shall comply with obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Health Information Technology for Economic and Clinical Health ("HITECH") Act and any other relevant laws and regulations regarding privacy (collectively the "Privacy Rules"). The obligations set forth in this Section shall survive the termination of this Contract. ✓

- a. Contractor warrants to the State that it is familiar with the requirements of the Privacy Rules, and will comply with all applicable requirements in the course of this Contract.
- b. Contractor warrants that it will cooperate with the State, including cooperation and coordination with State privacy officials and other compliance officers required by the Privacy Rules, in the course of performance of the Contract so that both parties will be in compliance with the Privacy Rules.
- c. The State and the Contractor will sign documents, including but not limited to business associate agreements, as required by the Privacy Rules and that are reasonably necessary to keep the State and Contractor in compliance with the Privacy Rules. This provision shall not apply if information received or delivered by the parties under this Contract is NOT "protected health information" as defined by the Privacy Rules, or if the Privacy Rules permit the parties to receive or deliver the information without entering into a business associate agreement or signing another document.
- d. The Contractor will indemnify the State and hold it harmless for any violation by the Contractor or its subcontractors of the Privacy Rules in accordance with this Section D.20. This includes the costs of responding to a breach of protected health information, the costs of responding to a government enforcement action related to the breach, and any fines, penalties, or damages paid by the State because of the

violation. The Indemnified Party(ies) shall provide written notice to the indemnifying party promptly after receiving notice of such Claim. If the defense of such Claim is materially prejudiced by a delay in providing such notice, the purported indemnifying party shall be relieved from providing such indemnity to the extent of the delay's impact on the defense. The indemnifying party shall have sole control of the defense of any indemnified Claim and all negotiations for its settlement or compromise, provided that such indemnifying party shall not enter into any settlement which imposes any obligations or restrictions on the applicable Indemnified Parties without the prior written consent of the other party. The Indemnified Parties shall cooperate fully, at the indemnifying party's request and expense, with the indemnifying party in the defense, settlement or compromise of any such action. The indemnified party may retain its own counsel at its own expense, subject to the indemnifying party's rights above. The obligations of the Contractor to indemnify the State under this Section shall not exceed the limitation of liability set forth in Section D.18 of this Contract.

D.30. Incorporation of Additional Documents. Each of the following documents is included as a part of this Contract by reference. In the event of a discrepancy or ambiguity regarding the Contractor's duties, responsibilities, and performance under this Contract, these items shall govern in order of precedence below:

- a. any amendment to this Contract, with the latter in time controlling over any earlier amendments;
- b. this Contract with any attachments or exhibits (excluding the items listed at subsections c. through f., below), which includes Attachment 1 – System Requirements; Attachment 2 – Pricing List; Attachment 3 – Attestation Re: Personnel Used in Contract Performance; Attachment 4 – Letter of Diversity Commitment;-; Attachment 5 – Service Level Agreement; Attachment 6 – the Cloud Services Guidelines; Attachment 7 – Description of the Implementation Services; Attachment 8– The Support Policies;, Attachment 9 – JBoss End User License terms, Attachment 9.A BAA Attachment 9.B – The Extensions Cloud Services and Attachment 12 - State Enterprise Security Policy.

D.31. Insurance. Contractor shall provide the State a certificate of insurance ("COI") evidencing the coverages and amounts specified below. The COI shall be provided ten (10) business days prior to the Effective Date and again ten (10) business days following the renewal or replacement of coverages required by this Contract. If insurance expires during the Term, the State must receive a new COI at least thirty (30) calendar days prior to the insurance's expiration date. If the Contractor loses insurance coverage, does not renew coverage, or for any reason becomes uninsured during the Term, the Contractor shall notify the State immediately.

The COI shall be on a form of an ACORD certificate and signed by an authorized representative of the insurer. The COI shall list each insurer's national association of insurance commissioners (also known as NAIC) number or federal employer identification number and list the State of Tennessee, Risk Manager, 312 Rosa L. Parks Ave., 3rd floor Central Procurement Office, Nashville, TN 37243 in the certificate holder section. At any time, the State may require the Contractor to provide a valid COI detailing coverage description; insurance company; policy number; exceptions; exclusions; policy effective date; policy expiration date; limits of liability; and the name and address of insured. The Contractor's failure to maintain or submit evidence of insurance coverage is considered a material breach of this Contract.

If the Contractor desires to self-insure, then a COI will not be required to prove coverage. In place of the COI, the Contractor must provide a certificate of self-insurance or a letter on the Contractor's letterhead detailing its coverage, liability policy amounts, and proof of funds to reasonably cover such expenses. Compliance with Tenn. Code Ann. § 50-6-405 and the rules of the TDCI is

required for the Contractor to self-insure workers' compensation.

All insurance companies must be: (a) acceptable to the State; (b) authorized by the TDCI to transact business in the State of Tennessee; and (c) rated A- VII or better by A. M. Best. The Contractor shall provide the State evidence that all subcontractors maintain the required insurance or that the subcontractors are included under the Contractor's policy.

The Contractor agrees to name the State as an additional insured on any insurance policies with the exception of workers' compensation (employer liability) and professional liability (errors and omissions) ("Professional Liability") insurance. Also, all policies shall contain an endorsement for a waiver of subrogation in favor of the State.

The Contractor agrees that the insurance requirements specified in this Section do not reduce any liability the Contractor has assumed under this Contract including any indemnification or hold harmless requirements.

The State agrees that it shall give written notice to the Contractor as soon as practicable after the State becomes aware of any claim asserted or made against the State, but in no event later than thirty (30) calendar days after the State becomes aware of such claim. The failure of the State to give notice shall only relieve the Contractor of its obligations under this Section to the extent that the Contractor can demonstrate actual prejudice arising from the failure to give notice. This Section shall not grant the Contractor or its insurer, through its attorneys, the right to represent the State in any legal matter, as the right to represent the State is governed by Tenn. Code Ann. § 8-6-106.

The State, acting reasonably, reserves the right to request amendment or require additional endorsements, types of coverage, and higher or lower limits of coverage depending on the nature of the work. Purchases or contracts involving any hazardous activity or equipment, tenant, concessionaire and lease agreements, alcohol sales, cyber-liability risks, environmental risks, special motorized equipment, or property may require customized insurance requirements (e.g. umbrella liability insurance) in addition to the general requirements listed below.

Any change to the insurance requirement shall be mutually agreed to.

The Contractor shall obtain and maintain, at a minimum, the following insurance coverages and policy limits.

a. Commercial General Liability Insurance

- 1) The Contractor shall maintain commercial general liability insurance, which shall be written on an Insurance Services Office, Inc. (also known as ISO) occurrence form (or a substitute form providing equivalent coverage) and shall cover liability arising from property damage, premises/operations, independent contractors, contractual liability, completed operations/products, personal and advertising injury, and liability assumed under an insured contract (including the tort liability of another assumed in a business contract).
- 2) The Contractor shall maintain bodily injury/property damage with a combined single limit not less than one million dollars (\$1,000,000) per occurrence and two million dollars (\$2,000,000) aggregate for bodily injury and property damage, including products and completed operations coverage with an aggregate limit of at least two million dollars (\$2,000,000).

E.2. Confidentiality of Records and Confidential Information. Strict standards of confidentiality of records and information shall be maintained in accordance with applicable state and federal law. All material and information, regardless of form, medium or method of communication and including without limitation State Content and Personally Identifiable Data and PHI, provided to the Contractor by the State or acquired by the Contractor on behalf of the State that is regarded as confidential under state or federal law shall be regarded as State's "Confidential Information." Nothing in this Section shall permit

Contractor to disclose any State's Confidential Information. The Application and the Document includes Contractor's trade secret and proprietary information and shall be treated as Contractor's Confidential Information. Confidential Information any non-public information of a party or its Suppliers relating to such entity's business activities, financial affairs, technology, marketing or sales plans that is disclosed pursuant to this contract and reasonably should have been understood by the receiving party, because of (i) legends or other markings, (ii) the circumstances of disclosure or (iii) the nature of the information itself, to be proprietary and confidential to the disclosing party.

Confidential Information will only be disclosed to authorized personnel on a Need-To-Know basis. Both parties shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. Any Confidential Information made available to the receiving party by the disclosing party other party shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. Confidential Information shall not be disclosed by either party except as required or permitted under state or federal law, or authorized by the disclosing party. Contractor shall take all necessary steps to safeguard the confidentiality of such material or information in conformance with the contract and with applicable state and federal law. Upon termination of the Contract, all State's Confidential Information in the Contractor's possession shall be returned to the State or destroyed by the Contractor set forth in the Contract.

The obligations set forth in this Section shall survive the termination of this Contract.

Notwithstanding the foregoing, a party may disclose Confidential Information to the extent required: (a) to any consultants, contractors, and counsel who have a need to know in connection with the Agreement and have executed a non-disclosure agreement with obligations at least as stringent as this Section, or (c) by law (including without limitation the *Tennessee Public Record Act*), or by a court or governmental agency, or if necessary in any proceeding to establish rights or obligations under the Contract; provided, the receiving party shall, unless legally prohibited, provide the disclosing party with reasonable prior written notice sufficient to permit the disclosing party an opportunity to contest such disclosure. If a party commits, or threatens to commit, a breach of this Section, the other party shall have the right to seek injunctive relief from a court of competent jurisdiction.

This Contract imposes no obligation upon either Party with respect to the other Party's Confidential Information which the receiving Party can establish: (a) is or becomes generally known through no breach of the Contract by the receiving party, or (b) is already known or is independently developed by the receiving party without use of or reference to the Confidential Information.

E.x. Software License. Contractor grants a license to the State to use all software provided under this Contract as set forth in Section A. Subject to the terms and conditions of the Contract, Contractor hereby grants State a limited, revocable, non-exclusive, non-transferable, non-assignable right to use during the Term and for internal business purposes only: a) the Applications and related services, including the Documentation; b) training materials and KnowledgePass Content; and, c) any embedded third party software, libraries, or other components, which form a part of the Services. Unauthorized use and/or copying of such technology are prohibited by law, including United States and foreign copyright law. State shall not reverse compile, disassemble or otherwise convert the Applications or other software comprising the Services into uncompiled or unassembled code. State shall not use any of the third party software programs (or the data models therein) included in the Services except solely as part of and in connection with the Services.

State acknowledges and agrees that the right to use the Applications is limited

based upon the amount of the Monthly Service Fees paid by State. State agrees to use only the modules and/or features for the number of employees and users as described on the Section C.3. State agrees not to use any other modules or features nor increase the number of employees and users unless State pays for such additional modules, features, employees or users, as the case may be. State may not license, relicense or sublicense the Services, or otherwise permit use of the Services (including timesharing or networking use) by any third party. State may not provide service bureau or other data processing services that make use of the Services without the express prior written consent of Contractor. No license, right, or interest in any Contractor trademark, trade name, or service mark, or those of Contractor's licensors or Suppliers, is granted hereunder.

State may authorize its third party contractors and consultants to access the Services through State's administrative access privileges on an as needed basis, provided State: a) abides by its obligations to protect Confidential Information as set forth in this Contract; and b) remains responsible for all such third party usage and compliance with the Contract.

State acknowledges and agrees that, as between State and Contractor, Contractor retains ownership of all right, title and interest to the Services, all of which are protected by copyright and other intellectual property rights, and that, other than the express rights granted herein and under any other agreement in writing with State, State shall not obtain or claim any rights in or ownership interest to the Services or Applications or any associated intellectual property rights in any of the foregoing. State agrees to comply with all copyright and other intellectual property rights notices contained on or in any information obtained or accessed by State through the Services.

E.x. Drug-Free Workplace. The Contractor agrees that it shall provide a drug-free workplace pursuant to the Drug-Free Workplace Act of 1988, Title 41 of the United States Code (41 USC) §§ 701 et seq., and the regulations in Title 45 of the Code of Federal Regulations (45 CFR) Part 82. ✓

E.x. Rule 2 Compliance. Solely to the extent applicable to the Scope of this Contract, the State and the Contractor shall comply with obligations under Rule 2 of the Confidentiality of Alcohol and Drug Abuse Patient Records, and its accompanying regulations as codified at 42 CFR § 2.1 et seq. ✓

a. The Contractor warrants to the State that it is familiar with the requirements of Rule 2 of the Confidentiality of Alcohol and Drug Abuse Patient Records, and its accompanying regulations, and will comply with all applicable requirements in the course of this Contract.

b. The Contractor warrants that it will cooperate with the State, including cooperation and coordination with State privacy officials and other compliance officers required by Rule 2 of the Confidentiality of Alcohol and Drug Abuse Patient Records, and its regulations, in the course of performance of the Contract so that both parties will be in compliance with Rule 2 of the Confidentiality of Alcohol and Drug Abuse Patient Records.

c. The State and the Contractor will sign documents, including but not limited to business associate agreements, as required by Rule 2 of the Confidentiality of Alcohol and Drug Abuse Patient Records, and that are reasonably necessary to keep the State and the Contractor in compliance with Rule 2 of the Confidentiality of Alcohol and Drug Abuse Patient Records. This provision shall not apply if information received by the State under this Contract is NOT "protected health information" as defined by Rule 2 of the Confidentiality of Alcohol and Drug Abuse Patient Records, or if Rule 2 of the Confidentiality of Alcohol and Drug Abuse Patient Records permits the State to receive such information without entering into a business associate agreement or signing another such document.

E.x. Professional Practice. The Contractor shall assure that there is a code of conduct in place and applicable to all employees that covers, at minimum, business practices, and service recipient/staff interaction/fraternization. Further, Contractor's personnel shall conduct their practice in conformity with all applicable statutes, rules and regulations, and recognized ethical standards of their profession. Procedures for reporting violations of the ethical standards shall be developed and communicated to staff upon hire and annually thereafter, which shall include a non-reprisal approach for persons reporting suspected violations, as well as a description of possible sanctions for violating the standards. Failure to implement a code of conduct in accordance with this section and to adequately address suspected violations of the code of conduct may be cause for termination of this Contractor Contract.

E.x. Additional Subcontracting Requirements. If subcontracts are approved by the State, they shall contain, in addition to those sections identified in D.5., sections on "Confidentiality of Records", "HIPAA Compliance," and "Rule 2 Compliance" (as identified by the section headings). Notwithstanding any use of approved subcontractors, the Contractor shall be the prime contractor and shall be responsible for all work performed.

E.x. Contractor Commitment to Diversity. Contractor shall assist the State in monitoring the Contractor's reasonable business efforts of commitment to diversity by providing, as requested, a quarterly report of participation in the performance of this Contract by small business enterprises and businesses owned by minorities, women, and Tennessee service-disabled veterans. Such reports shall be provided to the State of Tennessee Governor's Office of Diversity Business Enterprise in the required form and substance.

E.x. Additional lines, items, or options. At its sole discretion, the State may make written requests to the Contractor to add lines, items, or options that are needed and within the Scope but were not included in the original Contract. Such lines, items, or options will, once mutually agreed by the parties be added to the Contract through a Memorandum of Understanding ("MOU"), not an amendment.

a. After the Contractor receives a written request to add lines, items, or options, the Contractor shall have ten (10) business days to respond with a written proposal. The Contractor's written proposal shall include:

- (1) The effect, if any, of adding the lines, items, or options on the other goods or services required under the Contract;
- (2) Any pricing related to the new lines, items, or options;
- (3) The expected effective date for the availability of the new lines, items, or options; and
- (4) Any additional information requested by the State.

b. The State may negotiate the terms of the Contractor's proposal by requesting revisions to the proposal.

c. To indicate acceptance of a proposal, the State will sign it. The signed proposal shall constitute a MOU between the Parties, and the lines, items, or options shall be incorporated into the Contract as if set forth verbatim.

d. Only after a MOU has been executed shall the Contractor perform or deliver the new lines, items, or options.

9. Justification	Mental Health has conducted negotiations with Central Procurement Office and STS for this sole source contract. These changes have been reviewed by Mental Health and Central Procurement Office's attorneys and determined to be legally sound and acceptable. If this language cannot be accepted in the contract, Mental Health will be unable to receive the services because this is a sole source procurement.
Signature of Agency head or designee and date	
E. Douglas Varney, Commissioner	Date Sept. 30, 2016



STIS Pre-Approval Endorsement Request E-Mail Transmittal

TO : STIS Contracts
Department of Finance & Administration
E-mail : it.abc@tn.gov

FROM : Norman Maxwell
E-mail : norman.a.maxwell@tn.gov

DATE : 6/30/2016

RE : Request for STIS Pre-Approval Endorsement

Applicable RFS #
STIS Endorsement Signature & Date:
<hr/> <p>Chief Information Officer</p> <p><i>NOTE: Proposed contract/grant support is applicable to the subject IT service technical merit.</i></p>

Strategic Technology Solutions (STIS) pre-approval endorsement is required pursuant to procurement regulations pertaining to contracts with information technology as a component of the scope of service. This request seeks to ensure that STIS is aware of and has an opportunity to review the procurement detailed below and in the attached document(s). This requirement applies to any procurement method regardless of dollar amount.

Please indicate STIS endorsement of the described procurement (with the appropriate signature above), and return this document via e-mail at your earliest convenience.

Contracting Agency	Mental Health and Substance Abuse Services
Agency Contact (name, phone, e-mail)	Richard Zhu, Richard.zhu@tn.gov
<p>Attachments Supporting Request (mark all applicable)</p> <p>Note: The complete draft procurement document and the applicable documents listed below must accompany this request when submitted to STIS. Special Contract Requests and Amendment Requests without Agency Head signature are acceptable. STIS is aware that these documents will not have CPO signature when submitted with this request.</p> <p> <input checked="" type="checkbox"/> Solicitation Document <input type="checkbox"/> Special Contract Request <input type="checkbox"/> Amendment Request <input checked="" type="checkbox"/> Proposed Contract/Grant or Amendment <input type="checkbox"/> Original Contract/Grant and Previous Amendments (if any) </p>	
Information Systems Plan (ISP) Project Applicability	

Applicable RFS #

To avoid delay of STS pre-approval, the applicability of an ISP project to the procurement must be confirmed with agency IT staff prior to submitting this request to STS. If necessary, agency IT staff should contact STS Planning with questions concerning the need for an ISP project.

IT Director/Staff Name Confirming (required): Norman Maxwell

Applicable – Approved ISP Project# Work ID 1001865 – Workforce Scheduling System (33901)

Not Applicable

Subject Information Technology Service Description

Provide a brief summary of the information technology services involved. Clearly identify included technologies such as system development/maintenance, security, networking, etc. As applicable, identify the contract or solicitation sections related to the IT services.

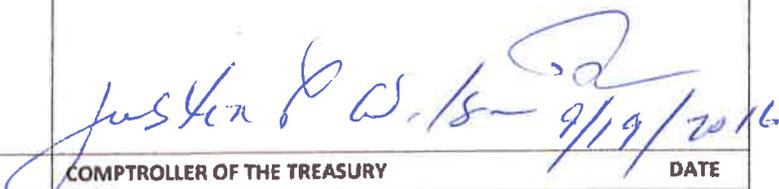
SaaS with KRONOS

Special Contract Request

This form should be utilized to facilitate contract and procurement requests that require the Chief Procurement Officer's prior approval and that of the Comptroller of the Treasury, as applicable.

NOT required for a contract with a federal, Tennessee, or Tennessee local government entity or a grant.

Route a completed request, as one file in PDF format, via e-mail attachment sent to: agsprs.agsprs@tn.gov.

<p>APPROVED</p> <p style="font-size: 24pt; font-weight: bold; margin-top: 20px;">Michael F. Perry -AK</p> <p style="font-size: 8pt; margin-top: 5px;">Digitally signed by Michael F. Perry -AK DN: cn=Michael F. Perry -AK, o=CPO, ou=CPO, email=andy.kidd@tn.gov, c=US Date: 2016.08.12 12:41:33 -05'00'</p>	<p>APPROVED</p> <div style="text-align: center; margin-top: 20px;">  </div> <p style="text-align: center; margin-top: 5px;">9/19/2016</p>
CHIEF PROCUREMENT OFFICER	COMPTROLLER OF THE TREASURY
DATE	DATE

Request Tracking #	
1. Contracting Agency	
2. Type of Contract or Procurement Method	<input type="checkbox"/> No Cost <input type="checkbox"/> Revenue <input checked="" type="checkbox"/> Sole Source <input type="checkbox"/> Proprietary <input type="checkbox"/> Competitive Negotiation <input type="checkbox"/> Other _____
3. Requestor Contact Information	Quinn Wilson Simpson quinn.simpson@tn.gov 615-253-7854
4. Brief Goods or Services Caption	Workforce management & timekeeping services.
5. Description of the Goods or Services to be Acquired	Department seeks to procure a system to track and manage scheduling and workforce resource allocation for four Regional Mental Health Institutes across the state (RMHIs).
6. Proposed Contractor	Kronos Acquisition Corporation
7. Name & Address of the Contractor's principal owner(s) <i>- NOT required for a TN state education institution</i>	Kronos Acquisition Corporation 297 Billerica Road Chelmsford, MA 01824
8. Proposed Contract Period - with ALL options to extend exercised <i>The proposed contract start date shall follow the approval date of this request.</i>	12 months
9. Office for Information Resources Pre-Approval Endorsement Request <i>- information technology (N/A to THDA)</i>	<input type="checkbox"/> Not Applicable <input checked="" type="checkbox"/> Attached

Request Tracking #	
10. eHealth Pre-Approval Endorsement Request – health-related professional, pharmaceutical, laboratory, or imaging	<input checked="" type="checkbox"/> Not Applicable <input type="checkbox"/> Attached
11. Human Resources Pre-Approval Endorsement Request – state employee training	<input type="checkbox"/> Not Applicable <input type="checkbox"/> Attached
12. Are these goods or services currently available on a statewide contract? If YES, please explain why the current statewide contract is not being used for this procurement.	<input checked="" type="checkbox"/> NO <input type="checkbox"/> YES,
13. Maximum Contract Cost – with ALL options to extend exercised	\$ 461,368.00
14. Was there an initial government estimate? If so, what amount?	<input checked="" type="checkbox"/> NO <input type="checkbox"/> YES, \$
15. Cost Determination Used- How did agency arrive at the estimate of expected costs?	Quote provided by vendor.
16. Explanation of Fair and Reasonable Price- Explain how agency determined that price is fair and reasonable	Because the Department believes there is only one vendor that can provide a complete suite of products with functions that are both scalable and able to meet the needs for a variety of business verticals, competitive pricing information with other vendors cannot be obtained. However, the Department obtained pricing information from US Communities contract and Federal GSA contract (General Services Administration) for the same type of product/service and determined the price we received from the vendor is fair and reasonable.
17. Documentation of Discussions with Contractor- How did agency document discussions with Contractor? Attach documentation to this request as applicable.	Phone calls, emails, on site meetings.
18. Explanation of Need for or requirement placed on the State to acquire the goods or services	TDMHSAS hopes to achieve an automated approach to timekeeping and scheduling for staff who do not directly key time into Edison. Implementing an automated, biometric timeclock-based system will reduce time reporting errors, improve staffing efficiencies, provide a real-time staff schedule, track absences and overtime, and produce accurate and timely reports. By acquiring scheduling software that can be specifically tailored to healthcare, we hope to achieve a reduction in the cost of overtime and contract labor by gaining the ability to predict workforce needs for fluctuating patient populations while reducing staff needed to manage schedules. Automating the time keeping process for the RMHIs will ultimately improve the business and administrative processes for the Department, thus enabling us to achieve our goal of becoming more customer focused.
19. Proposed contract impact on current State operations	<ul style="list-style-type: none"> • Increased efficiency. • Reduced expenses and dependency on contract resources. • Reduced overtime. • Increased employee morale.

Request Tracking #	
20. Justification – Specifically explain why the goods or services should be acquired through the procurement method or contract type selected.	TDMHSAS needs a vendor that can provide a <u>complete</u> suite of products with functions that are both scalable and able to meet the needs for a variety of business verticals. In December, TDMHSAS received the results of a study done by Vanderbilt on the potential benefits of more automation in time & attendance as well as recommendations for software solutions. They recommended Kronos as the only viable option. After extensive review, the Department determined that other vendors could not meet the requirements of the Department and was able to identify only one vendor that could provide the tools needed for TDMHSAS – Kronos.
For No Cost and Revenue Contracts Only	
21. What costs will the State incur as a result of this contract? If any, please explain.	
22. What is the total estimated revenue that the State would receive as a result of this contract?	
23. Could the State also contract with other parties interested in entering substantially the same agreement? Please explain.	<input type="checkbox"/> NO <input type="checkbox"/> YES
24. Summary of State responsibilities under proposed contract	
For Sole Source and Proprietary Procurements Only	
25. Explanation of Need for or requirement placed on the State to acquire the goods or services	Please see #18.
26. Evidence of Contractor's experience & length of experience providing the goods or services to be procured.	Contractor has thirty-nine years of experience in this industry. Thirty-two states across the country currently use Kronos for workforce management and timekeeping; contractor has thousands of contracts worldwide.
27. Has the contracting agency procured the subject goods or services before? If yes, provide the method used to purchase the goods or services and the name and address of the contractor.	<input checked="" type="checkbox"/> NO <input type="checkbox"/> YES, Method: Name/Address:

Request Tracking #																														
<p>28. Contractor selection process and efforts to identify reasonable, competitive, procurement alternatives</p>	<p>The Department has been actively researching potential solutions for this timekeeping system since fall 2015. In December, TDMHSAS received the results of a study done by Vanderbilt on the potential benefits of more automation in time & attendance as well as recommendations for software solutions. They recommended Kronos as the only viable option. After extensive review, the Department was able to identify only one vendor that could provide the tools needed for TDMHSAS – Kronos. The below table provides a comparison of some of the vendors the Department reviewed:</p> <table border="1" data-bbox="711 506 1471 890"> <thead> <tr> <th rowspan="2">Vendor/Product</th> <th colspan="4">Required Functionality</th> </tr> <tr> <th>Time & Attendance</th> <th>Absence Management</th> <th>Predictive Analytics</th> <th>Acuity-Based Scheduling</th> </tr> </thead> <tbody> <tr> <td>Kronos/Workforce Management</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> </tr> <tr> <td>*Ceridian/Dayforce</td> <td>Yes</td> <td>Yes</td> <td>No</td> <td>No</td> </tr> <tr> <td>*Success Factors (SAP Partnership)</td> <td>No</td> <td>No</td> <td>Yes</td> <td>No</td> </tr> <tr> <td>Workday (used to be PeopleSoft, now separate entity)</td> <td>No</td> <td>Yes</td> <td>No</td> <td>No</td> </tr> </tbody> </table> <p>*SaaS (Software as a Service) cannot be installed within the State's data center</p>	Vendor/Product	Required Functionality				Time & Attendance	Absence Management	Predictive Analytics	Acuity-Based Scheduling	Kronos/Workforce Management	Yes	Yes	Yes	Yes	*Ceridian/Dayforce	Yes	Yes	No	No	*Success Factors (SAP Partnership)	No	No	Yes	No	Workday (used to be PeopleSoft, now separate entity)	No	Yes	No	No
Vendor/Product	Required Functionality																													
	Time & Attendance	Absence Management	Predictive Analytics	Acuity-Based Scheduling																										
Kronos/Workforce Management	Yes	Yes	Yes	Yes																										
*Ceridian/Dayforce	Yes	Yes	No	No																										
*Success Factors (SAP Partnership)	No	No	Yes	No																										
Workday (used to be PeopleSoft, now separate entity)	No	Yes	No	No																										

Signature Required for all Special Contract Requests

Signature of Agency head or authorized designee, title of signatory, and date (the authorized designee may sign his or her own name if indicated on the Signature Certification and Authorization document)

Signature:  Date: 4/13/16

E. Douglas Varney, Commissioner



STS Pre-Approval Endorsement Request E-Mail Transmittal

TO : STS Contracts
Department of Finance & Administration
E-mail : it.abc@tn.gov

FROM : Norman Maxwell
E-mail : norman.a.maxwell@tn.gov

DATE : 6/30/2016

RE : Request for STS Pre-Approval Endorsement

Applicable RFS

STS Endorsement Signature & Date:

**Mark F. Bengel (by
Robert Fayne)**

Digitally signed by Mark F. Bengel (by Robert Fayne)
DN: cn=Mark F. Bengel (by Robert Fayne), o=Finance & Admin
Strategic Technology Solutions, ou=IT Planning & Governance,
email=robert.fayne@tn.gov, c=US
Date: 2016.07.25 14:51:06 -05'00'

Chief Information Officer

NOTE: Proposed contract/grant support is applicable to the subject IT service technical merit.

Strategic Technology Solutions (STS) pre-approval endorsement is required pursuant to procurement regulations pertaining to contracts with information technology as a component of the scope of service. This request seeks to ensure that STS is aware of and has an opportunity to review the procurement detailed below and in the attached document(s). This requirement applies to any procurement method regardless of dollar amount.

Please indicate STS endorsement of the described procurement (with the appropriate signature above), and return this document via e-mail at your earliest convenience.

Contracting Agency	Mental Health and Substance Abuse Services
Agency Contact (name, phone, e-mail)	Richard Zhu, Richard.zhu@tn.gov
Attachments Supporting Request (mark all applicable) Note: The complete draft procurement document and the applicable documents listed below must accompany this request when submitted to STS. Special Contract Requests and Amendment Requests without Agency Head signature are acceptable. STS is aware that these documents will not have CPO signature when submitted with this request.	
<input checked="" type="checkbox"/> Solicitation Document <input type="checkbox"/> Special Contract Request <input type="checkbox"/> Amendment Request <input checked="" type="checkbox"/> Proposed Contract/Grant or Amendment <input type="checkbox"/> Original Contract/Grant and Previous Amendments (if any)	
Information Systems Plan (ISP) Project Applicability	

Applicable RFS #

To avoid delay of STS pre-approval, the applicability of an ISP project to the procurement must be confirmed with agency IT staff prior to submitting this request to STS. If necessary, agency IT staff should contact STS Planning with questions concerning the need for an ISP project.

IT Director/Staff Name Confirming (required): Norman Maxwell

Applicable – Approved ISP Project# Work ID 1001865 – Workforce Scheduling System (33901)

Not Applicable

Subject Information Technology Service Description

Provide a brief summary of the information technology services involved. Clearly identify included technologies such as system development/maintenance, security, networking, *etc.* As applicable, identify the contract or solicitation sections related to the IT services.

SaaS with KRONOS

TO: Andy Kidd - Director of Sourcing
Kevin C. Bartels - Sourcing Staff Attorney

FROM: Chris Romaine – Sourcing Analyst CR 

DATE: 7/29/2016

SUBJECT: Recommendation of Sole Source

Special Contract Request (cy16-7152)⁶⁶⁷⁸ is a 12 month, \$461,368.00 sole source contract with Kronos Acquisition Corporation to procure an automated system to track and manage scheduling and workforce resource allocation for four Regional Mental Health Institutes across the state (RMHIs).

The system is expected to automate the timekeeping and scheduling for those who do not directly key time into Edison. Implementing an automated, biometric timeclock- based system will reduce time reporting errors, improve staffing efficiencies, provide a real-time staff schedule, track absences and overtime, and produce accurate and timely reports

Kronos is the only supplier that can provide the complete suite of products able to meet the needs of TDMHSAS.

Sourcing Analyst recommends the approval of this Sole Source contract request.

**Andy T.
Kidd**

Digitally signed by Andy T. Kidd
DN: cn=Andy T. Kidd, o=CPO,
ou=CPO - Sourcing,
email=andy.kidd@tn.gov, c=US
Date: 2016.08.12 12:41:13 -05'00'

Director of Sourcing

Date

Kevin C. Bartels

Digitally signed by Kevin C. Bartels
DN: cn=Kevin C. Bartels, o, ou=CPO Legal,
email=Kevin.C.Bartels@tn.gov, c=US
Date: 2016.08.08 15:56:49 -05'00'

Staff Attorney – Sourcing

Date

Veronica Peters

From: Elizabeth Stafford <Elizabeth.Stafford@tn.gov>
Sent: Monday, September 19, 2016 10:24 AM
To: Veronica Peters; Sherry Whitby
Cc: Andy Kidd
Subject: RE: UPDATE needed on REVISED Special Contract cy16-6678

Hi Veronica,

From Chris Romaine: "We are doing it for one year because the statewide team is supposed to have a contract in place with Kronos within a year and then we will join the SWC."

Please let me know if you have any additional questions.

Thanks!



Elizabeth Stafford | Sourcing Analyst
Tennessee Tower, 3rd Floor
312 Rosa L. Parks Ave., Nashville, TN 37243
p. 615-532-0764
elizabeth.stafford@tn.gov
tn.gov/generalservices/

From: Veronica Peters [mailto:Veronica.Peters@cot.tn.gov]
Sent: Monday, September 19, 2016 10:20 AM
To: Sherry Whitby; Elizabeth Stafford; Andy Kidd
Subject: UPDATE needed on REVISED Special Contract cy16-6678
Importance: High

Good morning, we are looking for an update on Revised cy16-6678. Below is info COT needs to complete.
Thanks

The SCR is for a sole source procurement for 1 year.

Why is the request for only a single year?

Is the intent of the procurement to not use the solution after the first year?

If this solution works, it will need to go to the FRC next year, so why not just go to the FRC this year and enter into a multi-year contract?

Thanks

Donald J. Ivancic

Legislative Procurement Compliance Manager
State of Tennessee – Comptroller of the Treasury
Office of Management Services
505 Deaderick St Suite 1400
Nashville TN 37243
Office: 615 401-7753



CONTRACT

(fee-for-goods or services contract with an individual, business, non-profit, or governmental entity of another state)

Begin Date 11/14/2016	End Date 11/13/2017 10/30/2017	Agency Tracking #	Edison Record ID
---------------------------------	--	--------------------------	-------------------------

Contractor Legal Entity Name Kronos Incorporated.	Edison Vendor ID 196888
---	-----------------------------------

Goods or Services Caption (one line only)
Time Keeping System

Contractor <input checked="" type="checkbox"/> Contractor	CFDA #
---	---------------

Funding —					
FY	State	Federal	Interdepartmental	Other	TOTAL Contract Amount
2017	\$665,125.60				\$665,125.60
TOTAL:	\$665,125.60				\$665,125.60

Contractor Ownership Characteristics:

Minority Business Enterprise (MBE): African American, Asian American, Hispanic American, Native American

Woman Business Enterprise (WBE)

Tennessee Service Disabled Veteran Enterprise (SDVBE)

Tennessee Small Business Enterprise (SBE): \$10,000,000.00 averaged over a three (3) year period or employs no more than ninety-nine (99) employees.

Other:

Selection Method & Process Summary (mark the correct response to confirm the associated summary)

<input type="checkbox"/> Competitive Selection	Describe the competitive selection process used
<input checked="" type="checkbox"/> Other	Sole Source Procurement

Budget Officer Confirmation: There is a balance in the appropriation from which obligations hereunder are required to be paid that is not already encumbered to pay other obligations.

Ben Wood

Speed Chart (optional)	Account Code (optional)
-------------------------------	--------------------------------

Amendment Request

This request form is not required for amendments to grant contracts. Route a completed request, as one file in PDF format, via e-mail attachment sent to: Agsprs.Agsprs@tn.gov

APPROVED	
CHIEF PROCUREMENT OFFICER	DATE

Agency request tracking #	
1. Procuring Agency	Mental Health and Substance Abuse Services
2. Contractor	Kronos Inc.
3. Edison contract ID #	52497
4. Proposed amendment #	1
5. Contract's Original Effective Date	11/14/16
6. Current end date	11/13/17
7. Proposed end date	11/13/20
8. Current Maximum Liability or Estimated Liability	\$ 665,125.60
9. Proposed Maximum Liability or Estimated Liability	\$ 1,587,618.20
10. Strategic Technology Solutions Pre-Approval Endorsement Request – information technology service (N/A to THDA)	<input type="checkbox"/> Not Applicable <input checked="" type="checkbox"/> Attached
11. eHealth Pre-Approval Endorsement Request – health-related professional, pharmaceutical, laboratory, or imaging	<input checked="" type="checkbox"/> Not Applicable <input type="checkbox"/> Attached
12. Human Resources Pre-Approval Endorsement Request – state employee training service	<input checked="" type="checkbox"/> Not Applicable <input type="checkbox"/> Attached
13. Explain why the proposed amendment is needed	
Initial contract between Department and Kronos Inc. was for one year for Department to assess the feasibility of the solution and implement the solution at a pilot site. After the successful rollout of the system at our Middle Tennessee Mental Health Institute, Department would like to amend the contract to allow sufficient time to implement the system at our remaining three facilities and to extend the maintenance period of the contract to three years.	
14. If the amendment involves a change in Scope, describe efforts to identify reasonable, competitive, procurement alternatives to amending the contract.	
n/a	

Agency request tracking #	
Signature of Agency head or authorized designee, title of signatory, and date (the authorized designee may sign his or her own name if indicated on the Signature Certification and Authorization document)	

Marie Williams, Commissioner

Date



CONTRACT AMENDMENT COVER SHEET

Agency Tracking # -	Edison ID 52497	Contract #	Amendment # 1		
Contractor Legal Entity Name Kronos Incorporated			Edison Vendor ID 196888		
Amendment Purpose & Effect(s) Extend time for implementation and add dollars for annual monitoring.					
Amendment Changes Contract End Date: <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO		End Date: November 13, 2020			
TOTAL Contract Amount INCREASE or DECREASE per this Amendment (zero if N/A):			\$ 922,492.60		
Funding —					
FY	State	Federal	Interdepartmental	Other	TOTAL Contract Amount
2017	\$143,500.00				\$143,500.00
2018	\$626,623.00				\$626,623.00
2019	\$407,497.60				\$407,497.60
2020	\$307,497.60				\$307,497.60
2021	\$102,500.00				\$102,500.00
TOTAL:	\$1,587,618.20				\$1,587,618.20
American Recovery and Reinvestment Act (ARRA) Funding: <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO					
Budget Officer Confirmation: There is a balance in the appropriation from which obligations hereunder are required to be paid that is not already encumbered to pay other obligations.			<i>CPO USE</i>		
Speed Chart (optional)		Account Code (optional)			



CONTRACT AMENDMENT COVER SHEET

Agency Tracking # -	Edison ID 52497	Contract #	Amendment # 1		
Contractor Legal Entity Name Kronos Incorporated			Edison Vendor ID 196888		
Amendment Purpose & Effect(s) Extend time for implementation and add dollars for annual monitoring.					
Amendment Changes Contract End Date: <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO		End Date: November 13, 2020			
TOTAL Contract Amount INCREASE or DECREASE per this Amendment (zero if N/A):			\$ 922,492.60		
Funding —					
FY	State	Federal	Interdepartmental	Other	TOTAL Contract Amount
2017	\$143,500.00				\$143,500.00
2018	\$626,623.00				\$626,623.00
2019	\$407,497.60				\$407,497.60
2020	\$307,497.60				\$307,497.60
2021	\$102,500.00				\$102,500.00
TOTAL:	\$1,587,618.20				\$1,587,618.20
American Recovery and Reinvestment Act (ARRA) Funding: <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO					
Budget Officer Confirmation: There is a balance in the appropriation from which obligations hereunder are required to be paid that is not already encumbered to pay other obligations.			<i>CPO USE</i>		
Speed Chart (optional)		Account Code (optional)			

**AMENDMENT ONE
OF CONTRACT 52497**

This Amendment is made and entered by and between the State of Tennessee, Department of Mental Health and Substance Abuse Services, hereinafter referred to as the "State" and Kronos Inc., hereinafter referred to as the "Contractor." For good and valuable consideration, the sufficiency of which is hereby acknowledged, it is mutually understood and agreed by and between said, undersigned contracting parties that the subject contract is hereby amended as follows:

1. Contract section C.1. is deleted in its entirety and replaced with the following:
 - C.1. Maximum Liability. In no event shall the maximum liability of the State under this Contract exceed one million five hundred eighty seven thousand six hundred eighteen dollars and twenty cents (\$1,587,618.20) ("Maximum Liability"). This Contract does not grant the Contractor any exclusive rights. The State does not guarantee that it will buy any minimum quantity of goods or services under this Contract except as set forth in Section C.3 below. Subject to the terms and conditions of this Contract, the Contractor will only be paid for goods or services provided under this Contract after an invoice is issued by Contractor to the State as specified by this Contract

2. Contract section B. is deleted in its entirety and replaced with the following:
 - B.1. This Contract shall be effective on November 14, 2017 ("Effective Date") and extend for a period ending November 13, 2020 ("Term"). The State shall have no obligation for goods or services provided by the Contractor prior to the Effective Date.

3. The following is added as Contract section B.2..
 - B.2. Renewal Options. This Contract may be renewed upon satisfactory completion of the Term. The State reserves the right to execute up to four (4) renewal options under the same terms and conditions for a period not to exceed twelve (12) months each by the State, at the State's sole option. In no event, however, shall the maximum Term, including all renewals or extensions, exceed a total of sixty (60) months

Required Approvals. The State is not bound by this Amendment until it is signed by the contract parties and approved by appropriate officials in accordance with applicable Tennessee laws and regulations (depending upon the specifics of this contract, said officials may include, but are not limited to, the Commissioner of Finance and Administration, the Commissioner of Human Resources, and the Comptroller of the Treasury).

Amendment Effective Date. The revisions set forth herein shall be effective November 14, 2017. All other terms and conditions of this Contract not expressly amended herein shall remain in full force and effect.

IN WITNESS WHEREOF,

KRONOS INC.:

SIGNATURE

DATE

PRINTED NAME AND TITLE OF SIGNATORY (above)

DEPARTMENT OF MENTAL HEALTH AND SUBSTANCE ABUSE SERVICES:

MARIE WILLIAMS, COMMISSIONER

DATE



CONTRACT

(fee-for-goods or services contract with an individual, business, non-profit, or governmental entity of another state)

Begin Date 11/14/2016	End Date 11/13/2017 10/30/2017	Agency Tracking #	Edison Record ID
---------------------------------	---	--------------------------	-------------------------

Contractor Legal Entity Name Kronos Incorporated.	Edison Vendor ID 196888
---	-----------------------------------

Goods or Services Caption (one line only)
Time Keeping System

Contractor <input checked="" type="checkbox"/> Contractor	CFDA #
---	---------------

Funding —					
FY	State	Federal	Interdepartmental	Other	TOTAL Contract Amount
2017	\$665,125.60				\$665,125.60
TOTAL:	\$665,125.60				\$665,125.60

Contractor Ownership Characteristics:

Minority Business Enterprise (MBE): African American, Asian American, Hispanic American, Native American

Woman Business Enterprise (WBE)

Tennessee Service Disabled Veteran Enterprise (SDVBE)

Tennessee Small Business Enterprise (SBE): \$10,000,000.00 averaged over a three (3) year period or employs no more than ninety-nine (99) employees.

Other:

Selection Method & Process Summary (mark the correct response to confirm the associated summary)

Competitive Selection Describe the competitive selection process used

Other Sole Source Procurement

Budget Officer Confirmation: There is a balance in the appropriation from which obligations hereunder are required to be paid that is not already encumbered to pay other obligations.

Ben Wood

Speed Chart (optional)	Account Code (optional)
-------------------------------	--------------------------------



**CONTRACT BETWEEN
STATE OF TENNESSEE, DEPARTMENT OF MENTAL HEALTH & SUBSTANCE ABUSE SERVICES
AND
KRONOS INCORPORATED**

This Contract, by and between the State of Tennessee, Department of Mental Health and Substance Abuse Services ("State" or "Customer") and Kronos Incorporated ("Contractor" or "Kronos"), is for the provision of a Time Keeping System, as further defined in the "SCOPE." State and Contractor may be referred to individually as a "Party" or collectively as the "Parties" to this Contract.

The Contractor is a For-Profit Corporation

Contractor Place of Incorporation or Organization: 297 Billerica Rd Chelmsford, MA

Contractor Edison Registration ID # 196888

A. SCOPE:

A.1. The Contractor shall provide the goods or services and deliverables as described, and detailed Section A.3 below and both parties shall meet all service and delivery timelines as specified by this Contract.

A.2. Definitions. Following are key definitions related to specific services requested in this Contract.

- a. "Application(s)" or " SaaS A pplication(s)" m eans t hose vendor s oftware a pplication programs set forth on Section A.3 (a)which are made accessible for the State to use under the terms of this Contract.
- b. "Business A ssociate Agreement" or " BAA" m eans t he Business A ssociate Agreement applicable for the Extension Application attached hereto as Attachment 10.
- c. "Cloud Services" means those services related to the State's cloud environment such as infrastructure, equ ipment, band width, s erver monitoring, bac kup s ervices, s torage ar ea network (SAN) s ervices, s ecurity s ervices, s ystem a dministration, c onnectivity s ervices, performance tuning, up date installation and m aintenance s ervices related thereto. Cloud Services are described in Attachment 6.
- d. "Days", shall mean calendar days unless otherwise stated in the Contract section.
- e. "Defect", s hall m ean a c ondition i n t he product which does not s ubstantially p erform i n accordance with the requirements set forth in the Documentation.
- f. "Deliverables", shall mean a services to be delivered to the State by the Contractor to fulfill the terms of this Contract.
- g. "Documentation" m eans technical pu blications pub lished b y t he Contractor relating t o the use of the Services or Applications.
- h. "Encrypt" or "Encryption" means to cryptographically protect data using methods such as symmetric enc ryption al gorithm, as ymmetric enc ryption al gorithm or a one -way has hing algorithm.
- i. "Encryption Gateway Tool" means the Kronos Cloud Encryption Gateway.
- j. "Equipment" means Contractor equipment specified in Section A.3(b).
- k. "Extension Applications" means the Forecast Manager for Healthcare for Kronos Cloud as described in Section A.3.
- l. "Extension Cloud Services" means those services described in Attachment 11, the "Cloud Services for Extension Applications".
- m. "HIPAA" means the Health Insurance Portability & Accountability Act of 1996 , P.L. 104-191, as am ended f rom t ime t o t ime, t ogether w ith i ts i mplementing r egulations promulgated under HIPAA and u nder t he H ealth I nformation T echnology f or E conomic and Clinical Health Act (the "HITECH Act"), Title XIII of Division A and Title IV of Division B of t he A merican R ecovery and R einvestment A ct of 2009 ("ARRA"), b y t he U .S.



Department of Health and Human Services, including, but not limited to, the Privacy Rule, the Security Rule and the Breach Notification Rule, as amended from time to time.

- n. "Hours", shall mean sequential hours unless otherwise stated in the Contract section.
- o. "Implementation Services" means those professional and educational services provided by Contractor to set up the cloud environment and configure the Applications. The initial Implementation Services are provided on a fixed fee basis and fixed scope basis. The Implementation Services are described in the SOW set forth at Attachment 7.
- p. "Personally Identifiable Data" means information concerning individually identifiable employees of the State protected against disclosure under applicable law or regulation.
- q. "PHI" means Protected Health Information as defined by HIPAA. PHI shall be deemed to be Personally Identifiable Data under the Contract.
- r. "Services" means (i) the Cloud Services, (ii) accessibility to the commercially available version of the Applications by means of access to the password protected State area of Contractor's website, and all such services, items and offerings accessed by the State therein, and (ii) the Equipment rented hereunder, if any.
- s. "Solution" means for the purposes of section A.30 the combination and use of the Extension Applications working with the Encryption Gateway Tool.
- t. "State Content" means all content the State, or others acting on behalf of or through the State, posts or otherwise inputs into the Services.
- u. "Statement of Work", "SOW", are interchangeable terms referring to a written description of the Implementation Services mutually agreed upon by Contractor and State.
- v. "Supplier" means any contractor, subcontractor or licensor of Contractor providing software, equipment and/or services to Contractor which are incorporated into or otherwise related to the Services. The use of Suppliers not specifically for the State contract but in general, by Kronos shall not be considered subcontracting for the purposes of this Contract.
- w. "Third Party Software", shall mean software not owned by the State or the Contractor.
- x. "Training Points" has the meaning ascribed to it in Section A.3 paragraph n below.
- y. "Vendor-Owned Software," shall mean commercially available software the rights to which are owned by Contractor, including but not limited to commercial "off-the-shelf" software which is not developed using State's money or resources.

A.3. Service Description. Contractor shall deliver that Application, Implementation Services and Services described below based on the number of licenses identified in Section C.3. The initial Services requirements are set forth in Attachment 1:

a. **APPLICATIONS**

Item #	Item Name	Item Description
1	Workforce Timekeeper	Pay Rules engine that automates the error-prone, manual processes of tracking employees time and applying complex pay policies
2	Workforce Employee	Provides Employee Self Service via standard browsers
3	Workforce Manager	Allows managers to view their employees and make edits to timecards. All edits have an audit trail so you can not only see who made the edit and what the edit was, but also where they were when they made the edit.
4	Workforce Integration Manager	Integration tool that allows Kronos to pass data between 3rd party applications
5	Workforce Mobile Employee	Provides Employees the ability to perform common functions on a smart phone (iPhone or Android phone).



6	Workforce Mobile Manager	Provides Managers the ability to perform common functions on a smart phone (iPhone or Android phone).
7	Workforce Scheduler	Automated labor scheduling solution that lets managers accurately create schedules that align labor with anticipated demand while adhering to all company and regulatory scheduling policies consistently.
8	Workforce Forecast Manager for Healthcare	Workforce Scheduler addition that provides the ability to staff based on projected volume
9	Workforce Extensions for Healthcare Encryption Gateway for Kronos Cloud See section A.30	This is the encryption gateway for Workforce Scheduler for Healthcare
10	Workforce Absence Manager	Allow organizations to calculate and project accrual balances such as Vacation, Sick, Personal Time, Compensatory Time, etc. Proactively Capture Attendance Events, Consistently Apply Attendance Rules, Gain Control Employee Attendance with visibility to trends and issues. Automates the administration and tracking of FMLA and other paid and unpaid leave policies and helps organizations achieve compliance with required federal, state, and local mandates.
11	KSS Tool Attestation Tool Kit	Tool that allows employees to correct exceptions to their time cards electronically, with the exceptions routed to the manager for approval. Also provides for "attestation language" that can be presented to the employee before approving their time card.
12	Workforce Analytics	Greater Workforce Return by providing instant insight to trends and performance: See Workforce Performance as it occurs; Improve work day results and Return & Ensure Expected/Required Outcomes

b. RENTAL EQUIPMENT

Item #	Item Name	Item Description
13	Kronos InTouch 9000 H3, Standard, HID Prox	Web-based time clock / terminal that combines reliable, employee-friendly data collection functionality
14	Touch ID Plus Option for H1/H2/H3 InTouch	Biometric verification technology for the time clock- ideal for eliminating "buddy punching"

c. WORKFORCE (WF) TIMEKEEPER See Attachment 7

Item #	Item Name	Item Description
15	WF Timekeeper Additional Testing & Deployment Group	Additional groups/sites to be deployed in addition to the initial deployment group
16	WF Timekeeper - Onsite Assessment	Kronos on-site visit(s) for the assessment sessions
17	Single Sign on Authentication. Requires a SAML 2.0 compatible customer solution	Configuration of Single Sign On.

d. WF ACCRUALS See Attachment 7

Item #	Item Name	Item Description
18	Workforce Absence Manager - Calculated Accruals Standard Configuration	Set up of the calculation of accruals (PTO, leave, sick, etc.) policies

e. WF SCHEDULER See Attachment 7

Item #	Item Name	Item Description
19	Additional Scheduling Unit/Group Bundle	Additional Scheduling Unit/Group Bundle - The base implementation includes Scheduling Units, this bundle includes up to



		5 additional Scheduling Units configured/deployed
20	Employee Self Scheduling	Employee Self Scheduling – The employee self-scheduling process provides an electronic means for employees to indicate the shifts they would like to work for the upcoming schedule period. There is an 'opening' date and 'closing' date during which the employees may submit their requests.
21	Workload Generator Configuration (Required for Healthcare Customers)	A matrix that contains the number of workers needed for a specific job, time span and location. this matrix is utilized to populate the workload planner and ultimately produce a staffing plan
22	Volume Import	Volume Import - Volume Import interface for Workload Generator that imports census data
23	Onsite Assessment	Centrally Conducted On-Site Requirements Assessment
24	Auto-Scheduler // Schedule Generator / Priority Scheduling Engine	The Schedule Generator is used to create the necessary number of open shifts to cover a workload within a zone when only one shift template that can be applied. The Priority Schedule Engine is a feature of Workforce Scheduler. It enables a user to assign open shifts to Employees, by selecting a procedure set that sorts employees, matches employees to a selected open shift, and assigns employees with the best match to the open shift. Priority Scheduling also helps to fill the open shifts according to rules that can be based on production schedules, labor standards, or employee requests. It also creates new schedules or quickly and accurately modifies a schedule, as business conditions change or staff responds to a posted schedule

f. **CORE PROFESSIONAL / EDUCATIONAL SERVICES Summary See attachment 7**

Item #	Item Name	Item Description
25	Implementation WFC SaaS see Attachment 7	Implementation costs for implementing the core solution and additional core solution that required to meet the needs of the agency and more described in paragraphs c to e above.
26	KnowledgePass SaaS WFC	Annual Education Subscription that provides for unlimited access to on-demand training tools such as tutorials and job aids
27	Training Points WFC SaaS	Training "points" or "dollars" that are included in the scope of the proposed solution

g. Kickoff Meeting and Presentation. Contractor shall participate in a State-led Kickoff Meeting. The purpose of the Kickoff Meetings shall be to introduce Contractor to State project stakeholders, and ensure agreement regarding project objectives, roles and responsibilities, strategy, and known risks. Contractor shall prepare and deliver a presentation for the kickoff meeting that synthesizes their approach to the overall project, provides high-level milestones, and introduces the Contractor team.

h. Project Management and Reporting. For the Implementation Services, Contractor shall designate a single Project Manager to serve as Contractor's primary point of contact for all activities and issues. Contractor shall ensure all project activities are performed efficiently, accurately and on schedule. The Contractor Project Managers shall coordinate all project activities with the State Project Manager to ensure Contractor activities are managed consistently with overall Contract requirements.

The Contractor Project Managers shall ensure timely and accurate submission of project management deliverables for the Implementation Services to the State Project Manager as



listed below:

- (1) Master Project Management Plan. Contractor shall designate a single Project Manager to collaborate with the State Project Manager to develop a Master Project Management Plan that describes the approach, activities, stages, duration and risks for all Project work. State shall provide written acceptance of the Master Project Management Plan. State shall be responsible for the Master Project Management Plan. Contractor shall collaborate with the State Project Manager to prepare and provide the following for inclusion in the Master Project Management Plan:

- (i) Work Breakdown Structure and Project Schedule: lists the work packages to be performed for the project and a schedule baseline that will be used as a reference point for managing project progress as it pertains to schedule and timeline.
- (ii) Change Management Plan: a proposed plan for managing project changes including, but not limited to: processes, scope, resources and implementation.
- (iii) Risk Management Plan: potential project risks, mitigation strategies and risk management processes.
- (iv) Issue Management Plan: a plan for documenting, tracking and reporting of issues, including the process for escalating issues for joint management decisions by the Contractor and State.

- (2) Weekly Status Report. Contractor shall prepare and submit to the State Project Manager a Weekly Status Report. The report shall contain a synopsis of the status of activities, outstanding issues and expected resolution dates, and key risks and issues. Items to be tracked in this report will include at a minimum, open technical questions, requests for information, schedule of resources for the coming weeks, and requests for documentation.

Contractor shall also report progress against the Project Schedule in the Weekly Status Report, including, at minimum, an assessment of progress against plan, and details of slipping tasks. For any planned tasks that are not worked or completed during the reporting period, Contractor shall include an explanation of the failure to meet the schedule and detailed plans to overcome the failure and prevent its recurrence.

State shall indicate acceptance or modification of the weekly status report during the weekly status meeting with the State Project Manager and other appropriate members. State may request an updated Weekly Status Report if modifications are deemed to be needed.

- (3) Monthly Progress Report. Contractor shall prepare and submit to State a Monthly Progress Report throughout the project's duration. Monthly Progress Reports shall contain, at a minimum:
 - (i) Progress toward project milestones
 - (ii) Explanations of schedule and cost variances relative to the previous month's progress report and the baseline schedule and cost projections
 - (iii) Updates on implementation
 - (iv) Status of deliverables
 - (v) Action items and status
 - (vi) Status of Modification Requests

- i. Implementation Plan. Contractor shall, in collaboration with the project team, create an Implementation Plan. The Implementation Plan shall describe the following:

- (1) Implementation schedule detailing milestones for each RMHI
- (2) Installation of equipment plan including clock dimensions



- (3) Initial configurations for each care unit at the RMHI
- (4) Authentication and access configurations for the system

The State shall provide written acceptance of the Implementation Plan and reserves the right to request periodic updates to the document.

- j. Operations Guide for Equipment. Contractor shall provide an Equipment Operations Guide which gives system users and technical staff the knowledge to operate and update clock configurations independent of Contractor assistance. The Guide shall address a view of the Equipment explaining levels of configuration and relationships between settings. It should also address security levels contained in the Equipment and describe access granted by each level.
- k. Security Plan. Contractor shall maintain the AICPA SSAE 16 SOC 1 Type II and the AT 101 SOC 2 Type II security standard in the Contractor Private Cloud environment for the security, availability and confidentiality criteria. Said criteria provide a framework for proactively guarding against security threats, unauthorized access, use and disclosure, unauthorized or accidental destruction or change and accidental loss and shall
 - (1) Protect all information and design information security controls in order to ensure:
 - i. Integrity, which means guarding against improper information modification or destruction, and includes ensuring information authenticity;
 - ii. Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
 - iii. Availability, which means ensuring timely and reliable access to and use of information.
 - (2) Secure the System and the information contained therein that connects to the State network, regardless of location.
 - (3) Adopt and implement, at a minimum, the policies, procedures, controls, and standards consistent with the AICPA Trust Principles Criteria for security, confidentiality and availability and the State's Enterprise Information Security Policies (included as Attachment 12) to ensure the integrity, confidentiality, and availability of information and information systems for which Contractor is responsible under this contract or to which it may otherwise have access under this contract.
 - (4) Contractor shall ensure that each user role is based on the business functions they are required to perform. Annually upon request, the State shall receive the report of an independent third party auditor attesting to controls in place in the environment, including vulnerability scanning and remediation.
 - (5) Staff with data access shall sign a nondisclosure agreement. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of State data, Contractor shall afford the State access to Contractor's facilities. Such inspections shall be limited to a guided tour of the data center facility, completion of an industry standard questionnaire, examination of the results of the annual AICPA SOC 1 and SOC 2 Type II audit conducted by an independent third party, and reasonable access to knowledgeable personnel to discuss the controls in place. For the avoidance of doubt, in no event shall the State or its designees be permitted to access Processor's systems, network servers, scan summaries or activities logs.
 - (6) Through the publication of its annual SOC reporting, Contractor shall disclose its non-proprietary security processes and technical limitations to the State. The State and the Contractor shall understand each other's roles and responsibilities.
 - (7) Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of data. Such security measures shall be in accordance with



recognized industry practice and not less stringent than the measures Contractor applies to its own personal data.

- i. Data Recovery Plan. The State's environment and all State data in the Contractor Cloud will be replicated to a secondary Contractor Cloud data center. Basic Disaster Recovery Services provides a Recovery Point Objective (RPO) of 24 hours and Contractor strives to restore Application Availability in a commercially reasonable timeframe
- m. Training Plan. Contractor shall provide a Training Plan that addresses the following areas: Contractor shall develop a Training Plan detailing training for each role type that will interact with the solution. Contractor and State shall collaborate and develop the specific role types, permissions and training for each category of users.
- n. The training services which will be detailed in the training plan include the KnowledgePass Education Subscription and Training Points:
 - (1) KnowledgePass Education Subscription. The KnowledgePass Education Subscription is purchased as set forth in Attachment 7 and Section C, Contractor will provide State with the KnowledgePass Education Subscription. The KnowledgePass Education Subscription provides access to certain educational offerings provided by Contractor (the "KnowledgePass Content"). State recognizes and agrees that the KnowledgePass Content is copyrighted by Contractor. State is permitted to make copies of the KnowledgePass Content provided in *pdf form solely for State's internal use. State may not disclose such KnowledgePass Content to any third party other than State's employees. State may not edit, modify, revise, amend, change, alter, customize or vary the KnowledgePass Content without the written consent of Contractor, provided that State may download and modify contents of training kits solely for State's internal use.
 - (2) Training Points. "Training Points" which are purchased by State may be redeemed for an equivalent value of instructor-led training sessions offered by Contractor. Training Points may be redeemed only during the Term, after which time such Training Points shall expire and be of no value. Training Points may not be exchanged for other Contractor products or services. The Training Points and training sessions are set forth in SOW. Participation in such training courses is limited to the number of seats indicated for the courses corresponding to the modules forming a part of the Services purchased by State.
- o. Implementation Services. Contractor agreed to complete the Implementation Services, as described in the contract for the fixed fee set forth in Section C, unless additional hours are required to complete such services due to a material change in the scope of the project, the State's delay in fulfilling its obligations, or as a result of a change in the complexity of the original scope of services based on the information unknown at the time the parties entered into this contract. Any such additional hours shall be agreed upon by the parties pursuant to the change order process described in the contract upon completion of the Implementation Services, Kronos will invoice the State for any remaining fees up to the fixed fee amount and such fees will be payable in accordance with section C.
- p. Contractor's configuration of the Applications will be based on information and work flows that Contractor obtains from the State during the discovery portion of the implementation. The State shall provide Contractor with necessary configuration-related information in a timely manner to ensure that mutually agreed implementation schedules are met.
- q. Post Implementation Assessment. After each site installation, Contractor shall prepare and deliver to the State a Post-Implementation Assessment report describing issues encountered during implementation, actions taken to remediate the issues, and lessons learned from the implementation.
- r. Final Project Report. Contractor shall create a Final Project Report using the State's Project Closure Report, summarizing project activities, lessons learned and recommended next steps. The Project Closure Report shall be submitted to the State Project Manager no later than fifteen (15) business days prior to the final signoff of the final project implementation. State will provide written acceptance of the Project Closure Report.



Support and Maintenance: Contractor shall provide support and maintenance for the Application and rented Equipment.

- a. **Support Services.** As part of such support, Contractor will make updates to the Services available to State at no charge as such updates are released generally to Contractor's customers. State agrees that Contractor may install critical security patches and infrastructure updates automatically as part of the Services. Contractor's then-current Support Services Policies shall apply to all Support Services provided by Contractor and are attached as Attachment 8 to this Contract ("Support Policies"). In the event of a conflict between the Support Policies and this contract, the terms of this contract shall prevail.

(1) Contractor shall be responsible for making available a Support Center.

- (i) the State may log questions online via the Contractor Customer Portal.
- (ii) Contractor shall provide 24/7 support for the cloud infrastructure, the availability to the cloud environment, and telephone support for the logging of functional problems and user problems.
- (iii) Contractor shall provide a toll-free phone number to facilitate communication and provide access to technical support.
- (iv) Contractor may establish additional points or modes of contact (e.g., chat or messaging through secure website) to expand or enhance access to service or support.
- (v) Contractor shall respond to any calls or messages within the response time set forth in paragraph 2(ii) below.

(2) Support. The Contractor shall, at a minimum:

- (i) Make appropriate Contractor support resources available to the State on a 24/7 basis, to provide the services described and detailed in this section.
- (ii) Priority levels are defined as follow:
Kronos provides support on a "priority" basis. As such, customers with the most critical request(s) will be serviced first. Kronos Support has set up the following guidelines to assess the priority of each service request:

High Priority: A critical customer issue with no available workaround where the system or a module may be down, experiencing major system degradation, data corruption or other related factors resulting in the customer not being able to process their payroll such as:

- a. Unable to sign-off Time Cards
- b. Totals are not accurate
- c. Unable to collect punches from terminals
- d. Unable to access a critical application function such as scheduling
- e. Unplanned Application Outage
- f. No workaround is available.

Medium Priority: A serious customer issue which impacts ability to utilize the product effectively such as:

- a. Intermittent or inconsistent functionality results or data accuracy — accrual balances not matching pay codes but balances are accurate
- b. Data display inaccuracies or inconsistencies across multiple tasks
- c. System performance is inconsistent or fluctuates
- d. A workaround is available.

Low Priority: Non-critical problem generally Use and Usability issues and or "how to" questions such as:

- a. How do I set up a holiday pay rule?
- b. How do I run a report?
- c. How often should database maintenance be executed?



d. A workaround is available on the customer portal.

(iii) Support Services response time shall mean from the time the case priority is set by Contractor's Support Center until a Contractor support representative contacts the State to begin service. Contractor utilizes a priority based support focus. Customers with the most critical request will be serviced in accordance with the following guidelines:

Priority	Platinum
High	1 hour
Medium	4 hours
Low	8 hours

(iv) The above are only guidelines and may be modified, for a particular incident, based on joint agreement between the State and the Contractor.

b. Support Services for Equipment. Depot Exchange support services for rented Equipment are included in the rental fees for such Equipment and are described as follows:

(1) *Depot Exchange.* The State has selected Depot Exchange Support Services, the following provisions shall apply: Upon the failure of installed Equipment, State shall notify Contractor of such failure and Contractor will provide remote fault isolation at the FRU (Field Replacement Unit) or subassembly level and attempt to resolve the problem. Those failures determined by Contractor to be Equipment related shall be dispatched to a Contractor Depot Repair Center, and State will be provided with a Return Material Authorization Number (RMA) for the failed Equipment if State is to return the failed Equipment to Contractor, as reasonably determined by Contractor. State must return the failed Equipment with the supplied RMA number. Hours of operation, locations and other information related to Contractor's Depot Repair Centers are available upon request and are subject to change. Return and repair procedures for failed Equipment shall be provided based on the Depot option - Depot Exchange and as specified herein and in Contractor's then-current Support Services Policies. Service packs for the Equipment (as described in subsection (ii) below) are included in both Depot Exchange and Depot Repair Support Services.

Contractor will provide a replacement for the failed Equipment at the FRU or subassembly level on an "advanced exchange" basis, utilizing a carrier of Contractor's choice. Replacement Equipment will be shipped the same day, for delivery to State's location as further described in the Support Policies. REPLACEMENT EQUIPMENT MAY BE NEW OR RECONDITIONED. State shall specify the address to which the Equipment is to be shipped. All shipments will include the Contractor provided RMA designating the applicable Contractor Depot Repair Center, as the recipient. State, upon receipt of the replacement Equipment from Contractor, shall package the defective Equipment in the materials provided by Contractor, with the RMA supplied and promptly return failed Equipment directly to Contractor.

(2) *Responsibilities of State.* It is State's responsibility to purchase and retain, at State's location and at State's sole risk and expense, a sufficient number of spare products ("Spare Products") to allow State to replace failed Equipment at State's locations in order for State to continue its operations while repairs are being performed and replacement Equipment is being shipped to State. For the Depot Exchange Equipment Support Services option, State agrees that it shall return failed Equipment promptly as the failures occur and that it shall not hold failed Equipment and send failed Equipment to Contractor in "batches" which shall result in a longer turnaround time to State. In addition, State agrees to:



- (i) Maintain the Equipment in an environment conforming to the Contractor published specifications for such Equipment;
- (ii) Not perform self-repairs on the Equipment (i.e., replacing components) without prior written authorization from Contractor;
- (iii) De-install all failed Equipment and install all replacement Equipment in accordance with Contractor's written installation guidelines;
- (iv) Ensure that the Equipment is returned to Contractor properly packaged; and
- (v) Obtain an RMA before returning any Equipment to Contractor and place the RMA clearly and conspicuously on the outside of the shipping package. State may only return the specific Equipment authorized by Contractor when issuing the RMA.

(3) Delivery. All domestic shipments within the United States are FOB Destination to/from State and Contractor with the shipping party bearing all costs and risks of loss, and with title passing upon delivery to the identified destination.

(4) Business Continuity and Disaster Recovery. Contractor shall maintain, throughout the term of the Agreement, a Business Continuity Plan. Upon State's written request, Contractor will issue to the State a summary statement on the design of the business continuity management framework. The Business Continuity Plan is confidential and Contractor will not provide actual plans nor will it allow customers to participate in business continuity activities

A.5. Optional Services / Service Catalog The State may, at its sole discretion, purchase additional, optional services as listed in Attachment 2 from the Contractor during the term of this contract through the use of separate mutually agreed Change Order or, as applicable, written statement(s) of work.

A.6. Change Orders. The State may, at its sole discretion and within written notice to the Contractor, request changes in the Scope that are necessary but were inadvertently unspecified in this contract.

a. Change Order Creation. After receipt of a written request for additional services from the State, the Contractor shall respond to the State, within a maximum of ten (10) business days, with a written proposal for completing the service. Contractor's proposal must specify:

- (1) The effect, if any, of implementing the requested change(s) on all other services required under this Contract;
- (2) The specific effort involved in completing the change(s);
- (3) The specific schedule for completing the change(s);
- (4) The maximum number of person hours required for the change(s); and
- (5) The maximum cost for the change(s) – this maximum cost shall in no instance exceed the product of the person hours required multiplied by the appropriate payment rate proposed for such work.

The Contractor shall not perform any additional service until the State has approved the proposal. If approved, the State will sign the proposal, and it shall constitute a Change Order between the Contract Parties pertaining to the specified change(s) and shall be incorporated, hereby, as a part of this Contract.

b. Change Order Performance. Subsequent to creation of a Change Order, the Contractor shall complete the required services. The State will be the sole judge of the acceptable completion of work and, upon such determination, shall provide the Contractor written approval.

A.7. Compliance with State Enterprise Information Policies and applicable laws. The Contractor is required conform with the State Enterprise Information Policies as amended and attached as Attachment 12 and to all applicable State and Federal laws regarding information security. As additional State and Federal regulatory requirements are imposed upon Contractor, the Contractor shall ensure that the environment, content and applications are kept up to date with



the emerging and applicable requirements. In the event that additional State and Federal requirements are imposed upon Contractor, and these requirements result in an additional cost to Contractor, Contractor may request that its prices be equitably adjusted to reflect the additional cost. The State may propose an amendment to the Contract to grant Contractor's requested price increase. In the event the State does not approve an amendment to the Contract granting the requested price increase, Contractor may terminate the Contract and such termination refusal shall not be considered a breach of contract. The Contractor shall be entitled to compensation for all conforming goods delivered in accordance with the Contract and authorized services completed as of the termination date. In no event shall the State be liable to the Contractor for compensation for any goods neither requested or for any services neither requested by the State nor performed by the Contractor. In no event shall the Contractor's exercise of its right to terminate this Contract under this Section relieve either party of any liability for any other damages or claims arising under this Contract.

A.8. Encryption. All data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for enforcing the encryption of the data. The Contractor shall ensure drive encryption consistent with AES 256 bit standard or higher.

A.9. Separation of Duties. To reduce the risk of accidental change or unauthorized access to operational software and business data, the State should be a separation of duties based on test, and production environment. The State Content will be included in the State databases, in either the production or testing environment. The Contractor will have the same security obligations for both environments.

The Contractor shall limit staff knowledge of State data to that which is need to know to perform job duties

A.10. Removable Media. To the extent applicable, removable media should be sanitized prior to removing it from the facilities for maintenance or repair. Removable media should be disposed of securely when no longer required, using approved State procedures. Removable media containing confidential information, confidential data, or sensitive data must be protected against unauthorized access, misuse or corruption during transport.

A.11. Malicious Code. The Contractor shall represent and warrant that it has tested the Application using commercially reasonable methods designed to ensure that upon providing access to State, the Application is free from all computer viruses, worms, time-outs, other harmful or malicious code intended to or can disrupt, erase or otherwise harm the Application, Equipment, or State's software, hardware, networks, data or information.

A.12. Protection of Information. The Contractor shall be responsible for properly protecting the State's Confidential Information processed and stored as a result of work under this contract. All Confidential Information shall be protected by both parties to the same extent they would their own proprietary data, Personally Identifiable Data and/or company trade secrets. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information. The State will retain unrestricted rights to State data. The State also maintains the right to request full copies of the data at any time.

The data that is processed and stored by the various applications within the network cloud environment may contain financial data as well as Personally Identifiable Information (PII). This data shall be protected against unauthorized access, disclosure or modification, theft, or destruction as set forth in Section A.22. The Contractor shall ensure that the facilities that house the network infrastructure are physically secure. The data must be available to the State upon written request within one business day or within the timeframe specified otherwise, and shall not be used for any other purpose other than that specified herein. During the Term and no more than fifteen (15) days after termination, the Contractor shall provide requested data at no additional cost to the State. After such period, Contractor shall have no further obligations to store, or make available the State Content and will securely delete any and all State Contract without liability.

a. Acceptable Use:



- (1) The State shall take all reasonable steps to ensure that no unauthorized persons have access to the Services, and to ensure that no persons authorized to have such access shall take any action that would be in violation of this contract.
- (2) The State represents and warrants to Contractor that the State has the right to publish and disclose the State Content in connection with the Services. The State represents and warrants to Contractor that the State Content: (a) does not infringe or violate any third-party right, including but not limited to intellectual property, privacy, or publicity rights, (b) is not abusive, profane, defamatory or offensive to a reasonable person, or, (c) is not hateful or threatening.
- (3) The State will not (a) use, or allow the use of, the Services in contravention of any federal, state, local, foreign or other applicable law, or rules or regulations of regulatory or administrative organizations; (b) introduce into the Services any virus or other code or routine intended to disrupt or damage the Services, or alter, damage, delete, retrieve or record information about the Services or its users; (c) excessively overload the Contractor systems used to provide the Services; (d) perform any security integrity review, penetration test, load test, denial of service simulation or vulnerability scan; (e) use any tool designed to automatically emulate the actions of a human user (e.g., robots); or, (f) otherwise act in a fraudulent, malicious or negligent manner when using the Services.
- (4) The State shall be responsible with respect claims alleging that: (a) employment-related claims arising out of State's configuration of the Services; (b) State's modification or combination of the Services with other services, software or equipment not furnished by Contractor, provided that such State modification or combination is the cause of claim and was not authorized by Contractor; or, (c) that the State Content infringes in any manner any intellectual property right of any third party, or any of the State Content contains any material or information that is obscene, defamatory, libelous, or slanderous violates any person's right of publicity, privacy or personality, or has otherwise caused or resulted in any tort, injury, damage or harm to any other person.

- b. **Connectivity and Access.** The State acknowledges that the State shall (a) be responsible for securing, paying for, and maintaining connectivity to the Services (including any and all related hardware, software, third party services and related equipment and components); and (b) provide Contractor and Contractor's representatives with such physical or remote access to the State's computer and network environment as Contractor deems reasonably necessary in order for Contractor to perform its obligations under the contract. The State will make all necessary arrangements as may be required to provide access to the State's computer and network environment if necessary for Contractor to perform its obligations under the contract.

A.13. **System Interfaces.** The Contractor is required to exchange information between the State System and entities that are internal or external to the State. The discovery phase of the design process must include evaluation of the existing interfaces and specify modifications, enhancements, or replacements to the interfaces which must be integrated into the system. The Contractor shall develop interfaces that feature standardized data formats and characteristics as well as standardized methods of communication and data interchange where applicable. The Contractor must also provide data schema and mappings and a fully documented set of standard application interfaces to allow for future external data sharing.

The Contractor shall develop specification documentation for each interface incorporated into the State system during the Design Phase of this project. The Interface Specifications shall be non-proprietary and the property of the State. The State shall have full distribution rights to the interface specifications developed for the system. The system shall provide State staff the ability to select the method of interchange. Interfaces may be real time, batch or a combination of both.

The Contractor shall use encryption for all data transfers and must secure all Application Program Interfaces (APIs) and Open Interfaces. Protocols and communication ports associated with



specific interfaces shall be determined by the Contractor and approved by the State during design.

A.14. Retention of Data. The Contractor shall maintain all data belonging to the State, in accordance with the requirements for data storage and retention found in this Contract, that this is in its possession through the term of the Contract.

A.15. Data Location. The Contractor shall provide its services to the State and its end users solely from data centers in the United States of America. Storage of State data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store State data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access State data remotely only as required to provide technical support and other services.

A.16. Additional SaaS Provisions

(a) State's Obligation

The State shall solely provide the information which is required for the Contractor to perform the Services.

When using and applying the information generated by the Services, State is responsible for ensuring that State complies with applicable laws and regulations if the Services include the Workforce Absence Management Application. The State does not rely upon Contractor or these Applications for any advice or guidance regarding compliance with federal and state laws.

(b) Suspension by Contractor

Contractor may suspend the affected Cloud Services immediately upon notice in the event of any State breach of the State's obligations with respect to the rights to use, acceptable use, or security, if such suspension is necessary to prevent ongoing damage to Contractor's Applications or Cloud Services or Contractor's other customers. Such suspensions shall extend only until the condition prompting the suspension persists. In any event, such suspension rights may limit access to and use of the Cloud Services but may not limit in any way Contractor's obligation to return State Content to the State and to allow the State to retrieve the State Content at any time.

A.17. Data Ownership. The State will own all right, title and interest in its data that is provided in relation to the services provided by this contract. The Contractor shall not access State user accounts or State data except:

1. In the course of data center operations,
2. In response to service or technical issues,
3. As required by the express terms of this contract, or
4. At the State's written request.

All data obtained by the Contractor from the State in the performance of this contract shall remain the property of the State.

Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of State information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of State information and comply with the following conditions:

1. At no time shall any data or processes that either belong to or are intended for the use of the State or its officers, agents or employees, be copied, disclosed or retained by the Contractor for subsequent use in any transaction that does not include the State.
2. The Contractor shall not use any information of the State delivered by the State in connection with the service for any purpose other than fulfilling the service.

A.18. Import and Export of Data. The State shall have the ability to Import or export State Content or State data piecemeal or in entirety at its discretion without interference from the Contractor. This



includes the ability for the State to import or export the State's data to or from other service providers.

- A.19. Transfer of Data. Upon request from the State made within 15 days from the termination of this Contract all data hosted and processed by the State on Contractor's equipment shall be removed and returned to the State in a usable format in use at the time of the request, unless the parties enter into a similar, successive Contract. Upon such return in the event of termination of the contract, Contractor shall have no further obligation to store or make available the State content and will sanitize any and all State Content in accordance with this Contract
- A.20. Access to Security Logs and Reports. Contractor shall provide reports to the State in a format as agreed to by both the Contractor and the State. Reports shall include latency statistics, user access, user access IP address, Application-level user access history and Applicable-level security logs for all State files related to this contract. For avoidance of doubt, in no event shall the State or its designees be permitted to access Contractor's systems, network servers, scan summaries or activities logs.
- A.21. The J Boss® Enterprise Middleware components of the Service are subject to the end user license agreement found at Attachment 9.
- A.22. Physical Security. All enterprise data processing facilities that process or store data shall have multiple layers of physical security. Each layer should be independent and separate of the preceding and/or following layer(s).

All facilities should have, at a minimum, a single security perimeter protecting it from unauthorized access, damage and/or interference. Secure areas should be protected by appropriate entry controls to restrict access only to authorized personnel. Procedures for working in secure areas should be created and implemented. Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled, and if possible, isolated from information processing facilities. Equipment should be located in secured areas or protected to reduce the risks from environment threats and hazards, and to reduce the opportunities for unauthorized access. Secured cabinets or facilities should support further segregation based on role and responsibility.

Users should ensure that unattended data processing equipment has appropriate protection. All systems and devices owned and operated by or on behalf of the State should be configured to clear and lock the screen or log the user off the system after a defined period of inactivity.

The Contractor shall inspect the results of an independent audit of its data centers at least annually, and provide a redacted version of the audit report upon request. The Contractor may remove its proprietary information from the redacted version. Contractor shall also continuously monitor the data center's performance, including frequent visits to the site.

- A.23. Assessment of the System. The Contractor is responsible for mitigating all security risks found during any assessment and continuous monitoring activities.
- A.24. Click Through Licenses. No "click through" licenses or provisions will be allowed during this contract.
- A.25. Change Control and Advance Notice. The Contractor shall give advance notice to the State of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.
- A.26. System Patching and Penetration Scanning.
 - 1. The Contractor will conduct periodic and special vulnerability scans, and install software / hardware patches and upgrades to protect all automated information assets. These audits shall be performed by Kronos using a third party tool, of the internal and external user interface, annually.



2. The Contractor must submit, for review the proposed scope of testing as well as the name and qualifications of the party performing the tests. The Contractor is responsible for the costs of this testing.
3. The Contractor must address and resolve any high or critical vulnerabilities in the Application or Service as identified by the scanning tool. The Contractor must arrange for repeat testing to ensure that all identified vulnerabilities have been addressed.
4. Kronos shall conduct as part of its security program, on at least an annual basis, contract with an independent third party to conduct a network and application penetration test on the then most recent version of the application released to market in the shared computing environment of the Kronos network containing Customer Data (i.e. Kronos Cloud). The penetration test will include, but is not limited to, the potential for unauthorized internet access, compromise of roles, and escalation of privileges for the application. Kronos will provide an executive summary of such penetration test including the scope and methodology of the test and confirmation that high and critical Risk Findings as identified by the scanning tool have been remediated or a plan (including time frame) is in place to remediate. Customer may choose to elect to purchase additional application penetration testing of any custom code delivered to the customer on behalf of Kronos. Penetration testing includes the web application vulnerabilities defined by the Open Web Application Security Project (OWASP) Top 10 and those listed in the SANS 25 (as applicable) or its successor current at the time of the test.

A.27. Warranty

Contractor represents and warrants that the term of the warranty (“Warranty Period”) shall be the Term of this Contract. If Contractor fails to provide the goods or services as warranted, then Contractor will re-provide the goods or services at no additional charge. Any nonconformance of the goods or services to the terms and conditions of this Contract, including any SLAs and support obligations of Contractor, shall constitute a “Defect” and shall be considered “Defective.” If Contractor receives notice of a Defect during the Warranty Period, then Contractor shall correct the Defect, at no additional charge. If Contractor is unable or unwilling to re-provide the goods or services as warranted 15 days after receiving notice, then the State shall be entitled to recover the fees paid to Contractor for the Defective goods or services during the period in which the Defective goods and services were unavailable. Any exercise of the State’s rights under this Section shall not prejudice the State’s rights to seek any other remedies available under this Contract and applicable law.

Except as provided for in this section A.26, Contractor hereby disclaims all warranties, conditions, guaranties and representations relating to the Services, express or implied, or oral or in writing, including without limitation the implied warranties of merchantability, fitness for a particular purpose, title and non-infringement, and whether or not arising through a course of dealing. The Services are not guaranteed to be error-free or uninterrupted. Except as specifically provided in this Contract, Contractor makes no warranties or representations concerning the compatibility of the Services, the SaaS Applications or the Equipment nor any results to be achieved therefrom.

- a. Application Warranty. The Services provided under this Contract, when used, under normal operation as specified in the Documentation and when used as authorized herein, shall perform in accordance with the Documentation throughout the Warranty Period.

Contractor represents and warrants that all Services provided under this Contract shall be provided in a timely and professional manner, by qualified and skilled individuals, and in conformity with the terms of the Contract.

- b. Equipment Warranty. Contractor warrants to the State that each item of Equipment shall be free from Defects during the Warranty Period. This warranty is extended to State only and shall not apply to any Equipment (or parts thereof) to the extent occurring as a result of the following:
 - i. damage, defects or malfunctions resulting from misuse, accident, neglect, tampering, (including without limitation modification or replacement of any Contractor components on any boards supplied with the Equipment), unusual physical or electrical stress or causes other than normal and intended use;



- ii. failure of State to provide and maintain a suitable installation environment, as specified in the published specifications for such Equipment; or
- iii. malfunctions resulting from the use of bad goods or supplies not approved by Contractor.

A.28. Inspection and Acceptance. The State shall have the right to inspect all goods or services provided by Contractor under this Contract. If, upon inspection, the State determines that the goods or services are Defective, the State shall notify Contractor, and Contractor shall re-deliver the goods or provide the services at no additional cost to the State. If after a period of thirty (30) days following delivery of goods or performance of services the State does not provide a notice of any Defects, the goods or services shall be deemed to have been accepted by the State.

A.29 Service Level Agreement Contractor shall provide the service levels as set forth in Attachment 5 and which is hereby incorporated herein by reference. The state's remedy in the event of any service errors, delays, outage or interruption of the services or failure by contractor to meet the terms of the applicable service level agreement, shall be the remedies provided in Attachment 5.

A.30 Health Care Extension Contractor will provide the Healthcare Extension under the terms set forth below and Attachment 11:

These additional WFC Extensions for Healthcare supplemental terms and conditions shall supplement the Contract. The State is deriving from Kronos the Extensions for Healthcare Application(s) referred to as the *Extension Applications* to be used and managed in Kronos' cloud environment (the "*Kronos Private Cloud*" or "*KPC*") and in accordance with this Section A.30 and Attachment 10. For greater certainty the parties acknowledge that client partnership services are not being ordered under this contract.

Contractor agrees to host and manage the Extension Applications in the Contractor Private Cloud for the benefit of State and in accordance with this Section A.30 and the Contract. State and Contractor agree that the terms and conditions set forth in this section A.30 shall only apply to the Extension Applications in Contractor's Private Cloud, and the services related thereto. The Extension Applications described section A.3 shall be delivered by means of State's permitted access to the Contractor Private Cloud. Notwithstanding any provision in the contract or any prior Statement of Work signed by the parties for the Extension Cloud Services to the contrary, the terms and conditions of this WFC HC Addendum shall apply to the Extension Applications hosted by Kronos in the Kronos Private Cloud. In the event of a conflict or inconsistency between the contract and this Section A.30, and only as it pertains to the Extension Applications, the provisions of this this section A.30 shall prevail.

(a) Contractor Cloud Encryption Gateway

- i. As part of acquiring the Extension Applications pursuant to this section A.30, Kronos licenses to State the right to use the Encryption Gateway Tool. The Encryption Gateway Tool will Encrypt PHI before it is transmitted to the Contractor Private Cloud and it will un-Encrypt the PHI when it is extracted from the Contractor Private Cloud in accordance with the encryption product documentation.
- ii. Contractor will deliver the Encryption Gateway Tool by giving State access to the secure Customer portal and such tool shall be available for download and to be installed by State, on State's server and behind its firewall at its location. The Encryption Gateway Tool will at all times be under State's control and State shall install updates to the Encryption Gateway Tool, when such updates are made available by Contractor. The Encryption Gateway Tool is licensed to State concurrently with the Extension Application(s) and upon termination or expiration of the Extension Application(s), State's right to use the Encryption Gateway Tool shall also terminate. State agrees to uninstall the Encryption Gateway Tool upon termination of State's right to use of the Extension Applications.
- iii. As part of the Services for the Extension Applications, State is entitled to receive the Support Services detailed in the underlying SaaS Agreement.
- iv. The Application Availability SLA of the SaaS Agreement shall not apply to the Encryption



Gateway Tool which is installed on State's server at State's control.

(b) State responsibilities

State agrees to:

- i. install, maintain and use the Encryption Gateway Tool as part of the cloud hosting services for the Extension Applications in accordance with the product documentation. State acknowledges that its failure to immediately apply updates to the Encryption Gateway Tool when such updates become available may: (i) compromise the security of State Content, including, Personally Identifiable Data and PHI; and (ii) result in incompatibility between the Healthcare Extensions and the Encryption Gateway Tool, which could cause failures in Encrypting and un-Encrypting data, and affect the scope of the Services provided by Contractor and its ability to adhere with its compliance programs, including those verified by the independent auditor report (i.e., SOC reports). State acknowledges Contractor shall not provide any credits for SLA issues under the contract that resulted from State's failure to update the Encryption Gateway Tool.
- ii. install and maintain the encryption gateway private key per the encryption product documentation, and not share the encryption gateway private key with any third party who does not have a need to know, including not sharing the encryption gateway private key with Contractor. Should State lose the key, any encrypted data will remain encrypted.
- iii. enter and maintain PHI only in the fields defined in the Extension Applications product documentation; and to only send PHI data (e.g., screen shots containing PHI) to Kronos by means of secure support channels for such data.
- iv. use unique user ID and passwords for all users of Extension Applications
- v. configure Extension Application user's account to meet State's HIPAA policy requirements for complexity, length duration and lockout.
- vi. determine user access/authorization to the application level of the Solution and assure that the level of access and the user assigned roles and permission are appropriate, which includes periodic application level logical access review.
- vii. review application logs to meet State's HIPAA compliance program.
- viii. immediately notify Contractor in the event State discovers a security issue with the Solution.
- ix. provide Contractor resources with application level accounts as reasonably needed to support the Extension Applications, and not unreasonably withhold such access.

(c) Business Associate Agreement

The parties agree that the provisions of the Business Associate Agreement attached hereto and incorporated herein by reference as Attachment 10 shall apply

(d) Data Security

As part of the Services for the Extension Applications, Kronos shall provide those administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of State data as described in Attachment 11 herein.

B. TERM OF CONTRACT:

November 14, 2016

This Contract shall be effective on November 2, 2016 ("Effective Date") and extend for a period of twelve (12) months after the Effective Date ("Term"). The State shall have no obligation for goods or services provided by the Contractor prior to the Effective Date.

C. PAYMENT TERMS AND CONDITIONS:

- C.1. Maximum Liability. In no event shall the maximum liability of the State under this Contract exceed six hundred sixty five thousand one hundred twenty five dollars and sixty cents (\$665,125.60) ("Maximum Liability"). This Contract does not grant the Contractor any exclusive rights. The State does not guarantee that it will buy any minimum quantity of goods or services under this Contract except as set forth in Section C.3 below. Subject to the terms and conditions of this Contract, the Contractor will only be paid for goods or services provided under this Contract after an invoice is issued by Contractor to the State as specified by this Contract.

Handwritten signature and date: 11/14/16



Compensation Firm. The payment methodology in Section C.3. of this Contract shall constitute the entire compensation, except as provided in this Section C, due the Contractor for the goods or services provided under this Contract regardless of the difficulty, materials or equipment required. The payment methodology includes all applicable taxes, fees, overhead, and all other direct and indirect costs incurred or to be incurred by the Contractor.

C.3. **Payment Methodology.** The Contractor shall be compensated based on the payment methodology for goods or services authorized by the State in a total amount as set forth in Section C.1.

- a. The Contractor's compensation shall be in accordance with the terms of the contract.
- b. The Contractor shall be compensated based upon the following payment methodology:

Quantities listed in the following tables are the MINIMUM quantities to be purchased under this agreement; additional quantities are possible with the same unit prices.

APPLICATIONS

Item/License	Qty	PEPM	Monthly Price
Workforce Timekeeper	1500	\$4.27	\$6,405.00
Workforce Employee	1500	\$0.00	Included
Workforce Manager	150	\$0.00	Included
Workforce Integration Manager	1500	\$0.00	Included
Workforce Mobile Employee	1500	\$0.00	Included
Workforce Mobile Manager	150	\$0.00	Included
Workforce Scheduler	1500	\$1.30	\$1,950.00
Workforce Forecast Manager for Healthcare Section A.30	1500	\$1.83	\$2,745.00
Workforce Extensions for Healthcare Encryption Gateway for Kronos Cloud Section A.30	1	\$0.00	\$0.00
Workforce Absence Manager	1500	\$1.30	\$1,950.00
KSS Tool Attestation Tool Kit	1500	\$0.26	\$390.00
Workforce Analytics	1500	\$2.12	\$3,180.00

RENTAL EQUIPMENT

Item	Qty	Unit Price	Monthly Price
Kronos InTouch 9000 H3, Standard, HID Prox	67	\$102.40	\$6,860.80
Touch ID Option for H1/H2/H3 InTouch	67	\$32.00	\$2,144.00
North America Power Kit for Mount Over Outlet - InTouch STD	67	\$0.00	\$0.00

CORE PROFESSIONAL / EDUCATIONAL SERVICES* SUMMARY

Item	Qty	Total Price
Implementation WFC SaaS Attachment 7		\$157,628.00
KnowledgePass SaaS WFC		Included
Training Points WFC SaaS	45,250	Included

CLOUD SERVICES SUMMARY

Item	Duration	Total Price
Cloud Hosting Encryption at Rest of Customer at Storage Level		\$0.00

Ninety (90) days following the Effective Date of the Contract, contractor will invoice the Application and rental equipment fees listed in C.3.b. monthly at the commencement of each month. Any credits, if applicable under the Attachment 5, Service Level Agreement,



will be applied to the following month's invoice.

*Professional/Educational Service fees will be made using the following methodology/milestones:

- (1) Delivery and Acceptance of Project Initiation Documents (20%) including
 - i. Kickoff Meeting and Presentation as referenced in Section A.3.g
 - ii. Master Project Management Plan as referenced in Section A.3.h.(1)
 - iii. Implementation Plan as referenced in Section A.3.i
 - iv. Operations Guide as referenced in Section A.3.j
 - v. Security Plan as referenced in Section A.3.k
 - vi. Data Recovery Plan as referenced in Section A.3.l
 - vii. Training Plan as referenced in Section A.3.m
- (2) Delivery and Acceptance of Implementation and Training at the Pilot Regional Mental Health Institute (RMHI) (25%) including: Post Implementation Assessment for the Pilot site as referenced in Section A.3.n
- (3) Delivery and Acceptance of Implementation and Training at the State's remaining three RMHIs (25%) including: Post Implementation Assessment for the three sites as referenced in Section A.3.n
- (4) Final Acceptance / Sign-off of Project (30%) including: Final Project Report as referenced in Section A.3.o

c. The Contractor shall be compensated for changes requested and performed pursuant to Contract Section A.6, without a formal amendment of this Contract based upon the payment rates detailed in the schedule below and as agreed pursuant to Section A.3 and Attachment 2, PROVIDED THAT compensation to the Contractor for such "change order" work shall not exceed \$200,000. If, at any point during the Term, the State determines that the cost of necessary "change order" work based on Attachment 2 would exceed the maximum amount, the State may amend this Contract to address the need.

Service Description	Amount (per compensable increment)
Consulting/Implementation Services	(500 hours x \$200/hour) \$100,000
Optional components (from Attachment 2)	\$100,000

C.4. Travel Compensation. The Contractor shall not be compensated or reimbursed for travel time, travel expenses, meals, or lodging.

C.5. Invoice Requirements. The Contractor shall invoice the State only for goods delivered and accepted by the State or services satisfactorily provided at the amounts stipulated in Section C.3., above. Contractor shall submit invoices and necessary supporting documentation, no more frequently than once a month, and no later than thirty (30) days after goods or services have been provided to the following address (as applicable):

Tennessee Department of Mental Health and Substance Abuse Services
 Fiscal Services
 Andrew Jackson Building, 6th Floor
 500 Deaderick Street
 Nashville, TN 37243

a. Each invoice, on Contractor's letterhead, shall clearly and accurately detail all of the following information (calculations must be extended and totaled correctly):

- (1) Invoice number (assigned by the Contractor);



- (2) Invoice date;
- (3) Contract number (assigned by the State);
- (4) Customer account name: State of Tennessee, Department of Mental Health and Substance Abuse Services;
- (5) Customer account number (assigned by the Contractor to the above-referenced Customer);
- (6) Contractor name;
- (7) Contractor Tennessee Edison registration ID number;
- (8) Contractor contact for invoice questions (name, phone, or email);
- (9) Contractor remittance address;
- (10) Description of delivered goods or services provided and invoiced, including identifying information as applicable;
- (11) Number of delivered or completed units, increments, hours, or days as applicable, of each good or service invoiced;
- (12) Applicable payment methodology (as stipulated in Section C.3.) of each good or service invoiced;
- (13) Amount due for each compensable unit of good or service; and
- (14) Total amount due for the invoice period.

b. Contractor's invoices shall:

- (1) Only include charges for goods delivered or services provided as described in Section A and in accordance with payment terms and conditions set forth in Section C;
- (2) Only be submitted for goods delivered or services completed and shall not include any charge for future goods to be delivered or services to be performed;
- (3) Not include Contractor's taxes, which includes without limitation Contractor's sales and use tax, excise taxes, franchise taxes, real or personal property taxes, or income taxes; and
- (4) Include shipping or delivery charges only as authorized in this Contract.

c. The timeframe for payment (or any discounts) begins only when the State is in receipt of an invoice that meets the minimum requirements of this Section C.5.

C.6. Payment of Invoice. The State payment terms are Net 45 days from the State receipt and the State shall not prejudice the State's right to object to or question any payment, invoice, or other related matter. Unless otherwise set forth in this contract, a payment by the State shall not be construed as acceptance of goods delivered, any part of the services provided, or as approval of any amount invoiced. Payment shall be in accordance with the Prompt Payment Act.

C.7. Invoice Reductions. The Contractor's invoice shall be subject to reduction for amounts included in any invoice or payment that is determined by the State, on the basis of audits conducted in accordance with the terms of this Contract, to not constitute proper compensation for goods delivered or services provided.

C.8. Deductions. The State reserves the right to deduct from amounts, which are or shall become due and payable to the Contractor under this or any contract between the Contractor and the State of Tennessee, any amounts that are or shall become due and payable to the State of Tennessee by the Contractor.

C.9. Prerequisite Documentation. The Contractor shall not invoice the State under this Contract until the State has received the following, properly completed documentation.

- a. The Contractor shall complete, sign, and present to the State the "Authorization Agreement for Automatic Deposit Form" provided by the State. By doing so, the Contractor acknowledges and agrees that, once this form is received by the State, payments to the Contractor, under this or any other contract the Contractor has with the State of Tennessee, may be made by ACH; and



- b. The Contractor shall complete, sign, and return to the State the State-provided W-9 form. The taxpayer identification number on the W-9 form must be the same as the Contractor's Federal Employer Identification Number or Social Security Number referenced in the Contractor's Edison registration information.

D. MANDATORY TERMS AND CONDITIONS:

- D.1. Required Approvals. The State is not bound by this Contract until it is duly approved by the Parties and all appropriate State officials in accordance with applicable Tennessee laws and regulations. Depending upon the specifics of this Contract, this may include approvals by the Commissioner of Finance and Administration, the Commissioner of Human Resources, the Comptroller of the Treasury, and the Chief Procurement Officer. Approvals shall be evidenced by a signature or electronic approval.
- D.2. Communications and Contacts. All instructions, notices, consents, demands, or other communications required or contemplated by this Contract shall be in writing and shall be made by certified, first class mail, return receipt requested and postage prepaid, by overnight courier service with an asset tracking system, or by email or facsimile transmission with recipient confirmation. All communications, regardless of method of transmission, shall be addressed to the respective Party at the appropriate mailing address, facsimile number, or email address as stated below or any other address provided in writing by a Party.

The State:

John Arredondo, Assistant Commissioner
Tennessee Department of Mental Health and Substance Abuse Services
Andrew Jackson Building, 6th Floor
500 Deaderick Street
Nashville, TN 37243
John.Arredondo@tn.gov
Telephone # 615-532-6515

The Contractor:

Kronos Incorporated
297 Billerica Road
Chelmsford, MA 01824
Attn: Kronos Legal
Alyce Moore, Vice President and General Counsel
Alyce.Moore@Kronos.com

All instructions, notices, consents, demands, or other communications shall be considered effective upon receipt or recipient confirmation as may be required.

- D.3. Modification and Amendment. This Contract may be modified only by a written amendment signed by all Parties and approved by all applicable State officials.
- D.4. Subject to Funds Availability. The Contract is subject to the appropriation and availability of State or federal funds. In the event that the funds are not appropriated or are otherwise unavailable, the State reserves the right to terminate this Contract upon a thirty (30) days prior written notice to the Contractor. The State's exercise of its right to terminate this Contract shall not constitute a breach of Contract by the State. Upon receipt of the written notice, the Contractor shall cease all work associated with the Contract. If the State terminates this Contract due to lack of funds availability, the Contractor shall be entitled to compensation for all conforming goods requested and delivered in accordance with the contract as of the termination date. Should the State exercise its right to terminate this Contract due to unavailability of funds, the Contractor shall have no right to recover from the State any actual, general, special, incidental, consequential, or any other damages of any description or amount.



Termination for Convenience. The State may terminate this Contract for convenience without cause and for any reason. The State shall give the Contractor at least thirty (30) days written notice before the termination date. The Contractor shall be entitled to compensation for all conforming goods delivered in accordance with the contract, authorized services completed as of the termination date. In no event shall the State be liable to the Contractor for compensation for any goods neither requested or for any services neither requested by the State nor performed by the Contractor. In no event shall the State's exercise of its right to terminate this Contract for convenience relieve the Contractor of any liability to the State for any damages or claims arising under this Contract.

- D.6. Termination for Cause. If the Contractor fails to properly perform its obligations under this Contract in a material manner, or if the Contractor materially violates any terms of this Contract ("Breach Condition"), the State shall have the right to terminate the Contract if such breach is not cured within fifteen (15) days after the receipt of the contract written notice. The State may withhold payments in excess of compensation for completed services or provided Equipment subject to such breach. Notwithstanding the above, the Contractor shall not be relieved of liability to the State for damages sustained by virtue of any Breach Condition and the State may seek other remedies allowed at law or in equity consistent with the terms of the contract for breach of this Contract. For purposes of this Contract, "material breach" means, with respect to a given breach, that a reasonable person in the position of the nonbreaching party would wish to terminate this agreement because of that breach.

Contractor may terminate the Services and the contract upon a material breach of the contract by the other party if such breach is not cured within thirty (30) days after receipt of written notice.

- D.7. Assignment and Subcontracting. The Contractor shall not assign this Contract or enter into a subcontract for any of the goods or services provided under this Contract without the prior written approval of the State. Notwithstanding any use of the approved subcontractors, the Contractor shall be the prime contractor and responsible for compliance with all terms and conditions of this Contract. The State reserves the right to request additional information or impose additional terms and conditions before approving an assignment of this Contract in whole or in part or the use of subcontractors in fulfilling the Contractor's obligations under this Contract.

- D.8. Conflicts of Interest. The Contractor warrants that no part of the Contractor's compensation shall be paid directly or indirectly to an employee or official of the State of Tennessee as wages, compensation, or gifts in exchange for acting as an officer, agent, employee, subcontractor, or consultant to the Contractor in connection with any work contemplated or performed under this Contract.

The Contractor acknowledges, understands, and agrees that this Contract shall be null and void if the Contractor is, or within the past six (6) months has been, an employee of the State of Tennessee or if the Contractor is an entity in which a controlling interest is held by an individual who is, or within the past six (6) months has been, an employee of the State of Tennessee.

- D.9. Nondiscrimination. The Contractor hereby agrees, warrants, and assures that no person shall be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of this Contract or in the employment practices of the Contractor on the grounds of handicap or disability, age, race, creed, color, religion, sex, national origin, or any other classification protected by federal or state law. The Contractor shall, upon request, show proof of nondiscrimination and shall post in conspicuous places, available to all employees and applicants, notices of nondiscrimination.

- D.10. Prohibition of Illegal Immigrants. The requirements of Tenn. Code Ann. § 12-3-309 addressing the use of illegal immigrants in the performance of any contract to supply goods or services to the state of Tennessee, shall be a material provision of this Contract, a breach of which shall be grounds for monetary and other penalties, up to and including termination of this Contract.

a. The Contractor agrees that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the



performance of this Contract. Upon request from the State, the Contractor shall reaffirm this attestation, in writing, by submitting to the State a completed and signed copy of the document at Attachment 3, semi-annually during the Term. If the Contractor is a party to more than one contract with the State, the Contractor may submit one attestation that applies to all contracts with the State. All Contractor attestations shall be maintained by the Contractor and made available to State officials upon request.

- b. Prior to the use of any subcontractor in the performance of this Contract, and semi-annually thereafter, during the Term, the Contractor shall obtain and retain a current, written attestation that the subcontractor shall not knowingly utilize the services of an illegal immigrant to perform work under this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant to perform work under this Contract. Attestations obtained from subcontractors shall be maintained by the Contractor and made available to State officials upon request.
 - c. The Contractor shall maintain records for all personnel used in the performance of this Contract. Contractor's records shall be subject to review and random inspection at any reasonable time upon reasonable notice by the State.
 - d. The Contractor understands and agrees that failure to comply with this section will be subject to the sanctions of Tenn. Code Ann. § 12-3-309 for acts or omissions occurring after its effective date.
 - e. For purposes of this Contract, "illegal immigrant" shall be defined as any person who is not: (i) a United States citizen; (ii) a Lawful Permanent Resident; (iii) a person whose physical presence in the United States is authorized; (iv) allowed by the federal Department of Homeland Security and who, under federal immigration laws or regulations, is authorized to be employed in the U.S.; or (v) is otherwise authorized to provide services under the Contract.
- D.11. Records. The Contractor shall maintain documentation for all charges under this Contract. The books, records, and documents of the Contractor, for work performed or money received under this Contract, shall be maintained for a period of five (5) full years from the date of the final payment and shall be subject to audit at any reasonable time (not more than once per year) and upon a thirty (30) days prior reasonable notice by the State, the Comptroller of the Treasury, or their duly appointed representatives. The financial statements shall be prepared in accordance with generally accepted accounting principles and may be made available subject to a confidentiality agreement.
- D.12. Monitoring. The Contractor's activities conducted and records maintained pursuant to this Contract shall be subject to monitoring and evaluation by the State, the Comptroller of the Treasury, or their duly appointed representatives in accordance with Section A.
- D.13. Progress Reports. The Contractor shall submit brief, periodic, progress reports to the State as requested in accordance with Section A.
- D.14. Strict Performance. Failure by any Party to this Contract to require, in any one or more cases, the strict performance of any of the terms, covenants, conditions, or provisions of this Contract shall not be construed as a waiver or relinquishment of any term, covenant, condition, or provision. No term or condition of this Contract shall be held to be waived, modified, or deleted except by a written amendment signed by the Parties.
- D.15. Independent Contractor. The Parties shall not act as employees, partners, joint venturers, or associates of one another. The Parties are independent contracting entities. Nothing in this Contract shall be construed to create an employer/employee relationship or to allow either Party to exercise control or direction over the manner or method by which the other transacts its business affairs or provides its usual services. The employees or agents of one Party are not employees or agents of the other Party.



Patient Protection and Affordable Care Act. To the extent applicable and such information is required for the purposes of this Contract, the Contractor agrees that it will be responsible for compliance with the Patient Protection and Affordable Care Act ("PPACA") with respect to itself and its employees, including any obligation to report health insurance coverage, provide health insurance coverage, or pay any financial assessment, tax, or penalty for not providing health insurance. The Contractor shall indemnify the State and hold it harmless for any costs to the State arising from Contractor's failure to fulfill its PPACA responsibilities for itself or its employees.

- D.17. Limitation of State's Liability. The State shall have no liability except as specifically provided in this Contract. In no event will the State be liable to the Contractor or any other party for any lost revenues, lost profits, loss of business, decrease in the value of any securities or cash position, time, money, goodwill, or any indirect, special, incidental, punitive, exemplary or consequential damages of any nature, whether based on warranty, contract, statute, regulation, tort (including but not limited to negligence), or any other legal theory that may arise under this Contract or otherwise. The State's total liability under this Contract (including any exhibits, schedules, amendments or other attachments to the Contract) or otherwise shall under no circumstances exceed the Maximum Liability. This limitation of liability is cumulative and not per incident.
- D.18. Limitation of Contractor's Liability. In accordance with Tenn. Code Ann. § 12-3-701, the Contractor's liability for all claims arising under this Contract shall be limited to an amount equal to two (2) times the Maximum Liability amount detailed in Section C.1. and as may be amended, PROVIDED THAT in no event shall this Section limit the liability of the Contractor for: (i) intellectual property or any Contractor indemnity obligations for infringement for third-party intellectual property rights; (ii) any claims covered by any specific provision in the Contract providing for liquidated damages; or (iii) any claims for intentional torts, criminal acts, fraudulent conduct, or acts or omissions that result in personal injuries or death.
- D.19. Hold Harmless. The Contractor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all claims, liabilities, losses, and causes of action which may arise, accrue, or result to any person, firm, corporation, or other entity which may be injured or damaged as a result of wrongful acts, omissions, or negligence on the part of the Contractor, its employees, or any person acting for or on its or their behalf relating to this Contract. The Contractor further agrees it shall be liable for the reasonable cost of attorneys for the State to enforce the terms of this Contract.

In the event of any suit or claim, the Parties shall give each other immediate notice and provide all necessary assistance to respond. The failure of the State to give notice shall only relieve the Contractor of its obligations under this Section to the extent that the Contractor can demonstrate actual prejudice arising from the failure to give notice. This Section shall not grant the Contractor, through its attorneys, the right to represent the State in any legal matter, as the right to represent the State is governed by Tenn. Code Ann. § 8-6-106.

- D.20. HIPAA Compliance. To the extent applicable under the scope of this Contract, the State and Contractor shall comply with obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Health Information Technology for Economic and Clinical Health ("HITECH") Act and any other relevant laws and regulations regarding privacy (collectively the "Privacy Rules"). The obligations set forth in this Section shall survive the termination of this Contract.
- a. Contractor warrants to the State that it is familiar with the requirements of the Privacy Rules, and will comply with all applicable requirements in the course of this Contract.
 - b. Contractor warrants that it will cooperate with the State, including cooperation and coordination with State privacy officials and other compliance officers required by the Privacy Rules, in the course of performance of the Contract so that both parties will be in compliance with the Privacy Rules.
 - c. The State and the Contractor will sign documents, including but not limited to business associate agreements, as required by the Privacy Rules and that are reasonably



necessary to keep the State and Contractor in compliance with the Privacy Rules. This provision shall not apply if information received or delivered by the parties under this Contract is NOT "protected health information" as defined by the Privacy Rules, or if the Privacy Rules permit the parties to receive or deliver the information without entering into a business associate agreement or signing another document.

- d. The Contractor will indemnify the State and hold it harmless for any violation by the Contractor or its subcontractors of the Privacy Rules in accordance with this Section D.20. This includes the costs of responding to a breach of protected health information, the costs of responding to a government enforcement action related to the breach, and any fines, penalties, or damages paid by the State because of the violation. The Indemnified Party(ies) shall provide written notice to the indemnifying party promptly after receiving notice of such Claim. If the defense of such Claim is materially prejudiced by a delay in providing such notice, the purported indemnifying party shall be relieved from providing such indemnity to the extent of the delay's impact on the defense. The indemnifying party shall have sole control of the defense of any indemnified Claim and all negotiations for its settlement or compromise, provided that such indemnifying party shall not enter into any settlement which imposes any obligations or restrictions on the applicable Indemnified Parties without the prior written consent of the other party. The Indemnified Parties shall cooperate fully, at the indemnifying party's request and expense, with the indemnifying party in the defense, settlement or compromise of any such action. The indemnified party may retain its own counsel at its own expense, subject to the indemnifying party's rights above. The obligations of the Contractor to indemnify the State under this Section shall not exceed the limitation of liability set forth in Section D.18 of this Contract.

D.21. Tennessee Consolidated Retirement System. Subject to statutory exceptions contained in Tenn. Code Ann. §§ 8-36-801, *et seq.*, the law governing the Tennessee Consolidated Retirement System ("TCRS"), provides that if a retired member of TCRS, or of any superseded system administered by TCRS, or of any local retirement fund established under Tenn. Code Ann. §§ 8-35-101, *et seq.*, accepts State employment, the member's retirement allowance is suspended during the period of the employment. Accordingly and notwithstanding any provision of this Contract to the contrary, the Contractor agrees that if it is later determined that the true nature of the working relationship between the Contractor and the State under this Contract is that of "employee/employer" and not that of an independent contractor, the Contractor, if a retired member of TCRS, may be required to repay to TCRS the amount of retirement benefits the Contractor received from TCRS during the Term.

D.22. Tennessee Department of Revenue Registration. The Contractor shall comply with all applicable registration requirements contained in Tenn. Code Ann. §§ 67-6-601 – 608. Compliance with applicable registration requirements is a material requirement of this Contract.

D.23. Debarment and Suspension. The Contractor certifies, to the best of its knowledge and belief, that it, its current and future principals, its current and future subcontractors and their principals:

- a. are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal or state department or agency;
- b. have not within a three (3) year period preceding this Contract been convicted of, or had a civil judgment rendered against them from commission of fraud, or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or grant under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification, or destruction of records, making false statements, or receiving stolen property;
- c. are not presently indicted or otherwise criminally or civilly charged by a government entity (federal, state, or local) with commission of any of the offenses detailed in section b. of this certification; and



- d. have not within a three (3) year period preceding this Contract had one or more public transactions (federal, state, or local) terminated for cause or default.

The Contractor shall provide immediate written notice to the State if at any time it learns that there was an earlier failure to disclose information or that due to changed circumstances, its principals or the principals of its subcontractors are excluded or disqualified.

- D.24. Force Majeure. "Force Majeure Event" means fire, flood, earthquake, elements of nature or acts of God, wars, riots, civil disorders, rebellions or revolutions, acts of terrorism or any other similar cause beyond the reasonable control of the Party except to the extent that the non-performing Party is at fault in failing to prevent or causing the default or delay, and provided that the default or delay cannot reasonably be circumvented by the non-performing Party through the use of alternate sources, workaround plans or other means. A strike, lockout or labor dispute shall not excuse either Party from its obligations under this Contract. Except as set forth in this Section, any failure or delay by a Party in the performance of its obligations under this Contract arising from a Force Majeure Event is not a default under this Contract or grounds for termination. The non-performing Party will be excused from performing those obligations directly affected by the Force Majeure Event, and only for as long as the Force Majeure Event continues, provided that the Party continues to use diligent, good faith efforts to resume performance without delay. The occurrence of a Force Majeure Event affecting Contractor's representatives, suppliers, subcontractors, customers or business apart from this Contract is not a Force Majeure Event under this Contract. Contractor will promptly notify the State of any delay caused by a Force Majeure Event (to be confirmed in a written notice to the State within one (1) day of the inception of the delay) that a Force Majeure Event has occurred, and will describe in reasonable detail the nature of the Force Majeure Event. If any Force Majeure Event results in a delay in Contractor's performance longer than forty-eight (48) hours, the State may, upon notice to Contractor: (a) cease payment of the fees until Contractor resumes performance of the affected obligations; or (b) immediately terminate this Contract or any purchase order, in whole or in part, without further payment except for fees then due and payable. Contractor will not increase its charges under this Contract or charge the State any fees other than those provided for in this Contract as the result of a Force Majeure Event.
- D.25. State and Federal Compliance. The Contractor shall comply with all applicable state and federal laws and regulations in the performance of this Contract.
- D.26. Governing Law. This Contract shall be governed by and construed in accordance with the laws of the State of Tennessee. The Tennessee Claims Commission or the state or federal courts in Tennessee shall be the venue for all claims, disputes, or disagreements arising under this Contract. The Contractor acknowledges and agrees that any rights, claims, or remedies against the State of Tennessee or its employees arising under this Contract shall be subject to a and limited to those rights and remedies available under Tenn. Code Ann. §§ 9-8-101 - 407.
- D.27. Entire Agreement. This Contract is complete and contains the entire understanding between the Parties relating to its subject matter, including all the terms and conditions of the Parties' agreement. This Contract supersedes any and all prior understandings, representations, negotiations, and agreements between the Parties, whether written or oral.
- D.28. Severability. If any terms and conditions of this Contract are held to be invalid or unenforceable as a matter of law, the other terms and conditions of this Contract shall not be affected and shall remain in full force and effect. The terms and conditions of this Contract are severable.
- D.29. Headings. Section headings of this Contract are for reference purposes only and shall not be construed as part of this Contract.
- D.30. Incorporation of Additional Documents. Each of the following documents is included as a part of this Contract by reference. In the event of a discrepancy or ambiguity regarding the Contractor's duties, responsibilities, and performance under this Contract, these items shall govern in order of precedence below:



- a. any amendment to this Contract, with the latter in time controlling over any earlier amendments;
- b. this Contract with any attachments or exhibits (excluding the items listed at subsections c. through f., below), which includes Attachment 1 – System Requirements; Attachment 2 – Pricing List; Attachment 3 – Attestation Re: Personnel Used in Contract Performance; Attachment 4 – Letter of Diversity Commitment; Attachment 5 – Service Level Agreement; Attachment 6 – the Cloud Services Guidelines; Attachment 7 – Description of the Implementation Services; Attachment 8– The Support Policies; Attachment 9 – JBoss End User License terms; Attachment 10 – BAA; Attachment 11 – The Extensions Cloud Services; and Attachment 12 - State Enterprise Security Policy.

D.30. Insurance. Contractor shall provide the State a certificate of insurance (“COI”) evidencing the coverages and amounts specified below. The COI shall be provided ten (10) business days prior to the Effective Date and again ten (10) business days following the renewal or replacement of coverages required by this Contract. If insurance expires during the Term, the State must receive a new COI at least thirty (30) calendar days prior to the insurance’s expiration date. If the Contractor loses insurance coverage, does not renew coverage, or for any reason becomes uninsured during the Term, the Contractor shall notify the State immediately.

The COI shall be on a form of an ACORD certificate and signed by an authorized representative of the insurer. The COI shall list each insurer’s national association of insurance commissioners (also known as NAIC) number or federal employer identification number and list the State of Tennessee, Risk Manager, 312 Rosa L. Parks Ave., 3rd floor Central Procurement Office, Nashville, TN 37243 in the certificate holder section. At any time, the State may require the Contractor to provide a valid COI detailing coverage description; insurance company; policy number; exceptions; exclusions; policy effective date; policy expiration date; limits of liability; and the name and address of insured. The Contractor’s failure to maintain or submit evidence of insurance coverage is considered a material breach of this Contract.

If the Contractor desires to self-insure, then a COI will not be required to prove coverage. In place of the COI, the Contractor must provide a certificate of self-insurance or a letter on the Contractor’s letterhead detailing its coverage, liability policy amounts, and proof of funds to reasonably cover such expenses. Compliance with Tenn. Code Ann. § 50-6-405 and the rules of the TDCI is required for the Contractor to self-insure workers’ compensation.

All insurance companies must be: (a) acceptable to the State; (b) authorized by the TDCI to transact business in the State of Tennessee; and (c) rated A- VII or better by A. M. Best. The Contractor shall provide the State evidence that all subcontractors maintain the required insurance or that the subcontractors are included under the Contractor’s policy.

The Contractor agrees to name the State as an additional insured on any insurance policies with the exception of workers’ compensation (employer liability) and professional liability (errors and omissions) (“Professional Liability”) insurance. Also, all policies shall contain an endorsement for a waiver of subrogation in favor of the State.

The Contractor agrees that the insurance requirements specified in this Section do not reduce any liability the Contractor has assumed under this Contract including any indemnification or hold harmless requirements. The State agrees that it shall give written notice to the Contractor as soon as practicable after the State becomes aware of any claim asserted or made against the State, but in no event later than thirty (30) calendar days after the State becomes aware of such claim. The failure of the State to give notice shall only relieve the Contractor of its obligations under this Section to the extent that the Contractor can demonstrate actual prejudice arising from the failure to give notice. This Section shall not grant the Contractor or its insurer, through its attorneys, the right to represent the State in any legal matter, as the right to represent the State is governed by Tenn. Code Ann. § 8-6-106.

The State, acting reasonably, reserves the right to request amendment or require additional endorsements, types of coverage, and higher or lower limits of coverage depending on the nature of the work. Purchases or contracts involving any hazardous activity or equipment, tenant, concessionaire and lease agreements, alcohol sales, cyber-liability risks, environmental risks,



special motorized equipment, or property may require customized insurance requirements (e.g. umbrella liability insurance) in addition to the general requirements listed below. Any change to the insurance requirement shall be mutually agreed to.

The Contractor shall obtain and maintain, at a minimum, the following insurance coverages and policy limits.

a. Commercial General Liability Insurance

- 1) The Contractor shall maintain commercial general liability insurance, which shall be written on an Insurance Services Office, Inc. (also known as ISO) occurrence form (or a substitute form providing equivalent coverage) and shall cover liability arising from property damage, premises/operations, independent contractors, contractual liability, completed operations/products, personal and advertising injury, and liability assumed under an insured contract (including the tort liability of another assumed in a business contract).
- 2) The Contractor shall maintain bodily injury/property damage with a combined single limit not less than one million dollars (\$1,000,000) per occurrence and two million dollars (\$2,000,000) aggregate for bodily injury and property damage, including products and completed operations coverage with an aggregate limit of at least two million dollars (\$2,000,000).

E. SPECIAL TERMS AND CONDITIONS:

E.1. Conflicting Terms and Conditions. Should any of these special terms and conditions conflict with any other terms and conditions of this Contract, the special terms and conditions shall be subordinate to the Contract's other terms and conditions.

E.2. Confidentiality of Records and Confidential Information. Strict standards of confidentiality of records and information shall be maintained in accordance with applicable state and federal law. All material and information, regardless of form, medium or method of communication and including without limitation State Content and Personally Identifiable Data and PHI, provided to the Contractor by the State or acquired by the Contractor on behalf of the State that is regarded as confidential under state or federal law shall be regarded as State's "Confidential Information." Nothing in this Section shall permit Contractor to disclose any State's Confidential Information. The Application and the Document includes Contractor's trade secret and proprietary information and shall be treated as Contractor's Confidential Information. Confidential Information any non-public information of a party or its Suppliers relating to such entity's business activities, financial affairs, technology, marketing or sales plans that is disclosed pursuant to this contract and reasonably should have been understood by the receiving party, because of (i) legends or other markings, (ii) the circumstances of disclosure or (iii) the nature of the information itself, to be proprietary and confidential to the disclosing party.

Confidential Information will only be disclosed to authorized personnel on a Need-To-Know basis. Both parties shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. Any Confidential Information made available to the receiving party by the disclosing party other party shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. Confidential Information shall not be disclosed by either party except as required or permitted under state or federal law, or authorized by the disclosing party. Contractor shall take all necessary steps to safeguard the confidentiality of such material or information in conformance with the contract and with applicable state and federal law. Upon termination of the Contract, all State's Confidential Information in the Contractor's possession shall be returned to the State or destroyed by the Contractor set forth in the Contract.

The obligations set forth in this Section shall survive the termination of this Contract.



Notwithstanding the foregoing, a party may disclose Confidential Information to the extent required: (a) to any consultants, contractors, and counsel who have a need to know in connection with the Agreement and have executed a non-disclosure agreement with obligations at least as stringent as this Section, or (c) by law (including without limitation the *Tennessee Public Record Act*), or by a court or governmental agency, or if necessary in any proceeding to establish rights or obligations under the Contract; provided, the receiving party shall, unless legally prohibited, provide the disclosing party with reasonable prior written notice sufficient to permit the disclosing party an opportunity to contest such disclosure. If a party commits, or threatens to commit, a breach of this Section, the other party shall have the right to seek injunctive relief from a court of competent jurisdiction.

This Contract imposes no obligation upon either Party with respect to the other Party's Confidential Information which the receiving Party can establish: (a) is or becomes generally known through no breach of the Contract by the receiving party, or (b) is already known or is independently developed by the receiving party without use of or reference to the Confidential Information.

E.3. Security and Standards-Compliance Requirements.

- (a) Data Security. As part of the Services, Contractor shall provide those administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of State data as described in Attachment 6.

State acknowledges that such safeguards endeavor to mitigate security incidents, but such incidents may not be mitigated entirely or rendered harmless. State should consider any particular Contractor supplied security-related safeguard as just one tool to be used as part of State's overall security strategy and not a guarantee of security. Both parties agree to comply with all applicable privacy or data protection statutes, rules, or regulations governing their respective activities of the parties under the Agreement.

As between State and Contractor, all Personally Identifiable Data is State's Confidential Information and will remain the property of State as set forth in section E.2 above. State represents that to the best of State's knowledge such Personally Identifiable Data supplied to Contractor is accurate. State hereby consents to the use, processing or disclosure of Personally Identifiable Data by Contractor and Contractor's Suppliers wherever located only for the purposes described herein and only to the extent such use or processing is necessary for Contractor to carry out Contractor's duties and responsibilities under the Agreement or as required by law.

Prior to initiation of the Services under the Agreement and on an ongoing basis thereafter, State agrees to provide notice to Contractor of any extraordinary privacy or data protection statutes, rules, or regulations which are or become applicable to State's industry and which could be imposed on Contractor as a result of provision of the Services. State will ensure that: (a) the transfer to Contractor and storage of any Personally Identifiable Data by Contractor or Contractor's Supplier's data center is permitted under applicable data protection laws and regulations; and, (b) State will obtain consents from individuals for such transfer and storage to the extent required under applicable laws and regulations.

- (b) Security Certification, Accreditation, Audit. Annually at the State's request, the contractor shall provide proof of any security certifications, accreditation, or audit on a yearly basis to the State to validate the hosting solution security. (Examples: SOC 2 Type II/ SOC 3, ISO 27001). The State shall receive the report of an independent third party auditor attesting to controls in place in the environment, including vulnerability scanning and remediation. In addition, the State may request annually to proceed with an inspection. Such inspections shall be limited to a guided tour of the data center facility, completion of an industry standard questionnaire, examination of the results of the annual AICPA SOC 1 and SOC 2 Type II audit conducted by an independent third party, and reasonable access to knowledgeable personnel to discuss the controls in place. For the avoidance of doubt, in no event shall the State or its designees be permitted to access Processor's systems, network servers, scan summaries or activities logs.



Security Incident and Data Breach

Contractor shall inform the State of any security incident or data breach impacting the State Content. The Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise, defined by laws (including such applicable privacy laws) or contained in the contract. Discussing security incidents with the State should be handled on an urgent as-needed basis, as part of Contractor communication and mitigation processes, defined by law or contained in the contract.

Contractor shall report any security incident to the appropriate State identified contact immediately. If Contractor has actual knowledge of a confirmed data breach that affects the security of any State content that is subject to applicable data breach notification law, Contractor shall:

1. Promptly notify the appropriate State identified contact within 24 hours or sooner, unless shorter time is required by applicable law,
2. Take commercially reasonable measures to investigate perceived security incidents to address the data breach in a timely manner
3. Cooperate with the State as reasonably requested by the State to investigate and resolve the data breach,
4. Promptly implement necessary remedial measures, if necessary, and
5. Document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

Unless otherwise stipulated, if a data breach is a direct result of the Contractor breach of its contract obligation to encrypt personal data or otherwise prevent its release, prevent malicious code as provided in Section A.11 of this Contract, or to protect the credentials of Contractor's employees or subcontractors, the Contractor shall bear the costs of remedial measures as required by laws consistent with the contract which may include: (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state law; (3) a credit monitoring service required by state (or federal) law; (4) a website or a toll-free number and call center for affected individuals required by state law - all not to exceed the average per record per person cost calculated for data breaches in the United States (currently \$201 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause; all [(1) through (5)] subject to this contract's limitation of liability.

- E.4. Software License. Contractor grants a license to the State to use all software provided under this Contract as set forth in Section A. Subject to the terms and conditions of the Contract, Contractor hereby grants State a limited, revocable, non-exclusive, non-transferable, non-assignable right to use during the Term and for internal business purposes only: a) the Applications and related services, including the Documentation; b) training materials and KnowledgePass Content; and, c) any embedded third party software, libraries, or other components, which form a part of the Services. Unauthorized use and/or copying of such technology are prohibited by law, including United States and foreign copyright law. State shall not reverse compile, disassemble or otherwise convert the Applications or other software comprising the Services into uncompiled or unassembled code. State shall not use any of the third party software programs (or the data models therein) included in the Services except solely as part of and in connection with the Services.

State acknowledges and agrees that the right to use the Applications is limited based upon the amount of the Monthly Service Fees paid by State. State agrees to use only the modules and/or features for the number of employees and users as described on the Section C.3. State agrees not to use any other modules or features nor increase the number of employees and users unless State pays for such additional modules, features, employees or users, as the case may be. State may not license, relicense or sublicense the Services, or otherwise permit use of the Services (including timesharing or networking use) by any third party. State may not provide service bureau or other data processing services that make use of the Services without the express prior



written consent of Contractor. No license, right, or interest in any Contractor trademark, trade name, or service mark, or those of Contractor's licensors or Suppliers, is granted hereunder.

State may authorize its third party contractors and consultants to access the Services through State's administrative access privileges on an as needed basis, provided State: a) abides by its obligations to protect Confidential Information as set forth in this Contract; and b) remains responsible for all such third party usage and compliance with the Contract.

State acknowledges and agrees that, as between State and Contractor, Contractor retains ownership of all right, title and interest to the Services, all of which are protected by copyright and other intellectual property rights, and that, other than the express rights granted herein and under any other agreement in writing with State, State shall not obtain or claim any rights in or ownership interest to the Services or Applications or any associated intellectual property rights in any of the foregoing. State agrees to comply with all copyright and other intellectual property rights notices contained on or in any information obtained or accessed by State through the Services.

E.5 Reserved

E.6. Intellectual Property. The Contractor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all claims or suits which may be brought against the State concerning or arising out of any claim of an alleged patent, copyright, trade secret or other intellectual property infringement. In any such claim or action brought against the State, the Contractor shall satisfy and indemnify the State for the amount of any settlement or final judgment, and the Contractor shall be responsible for all legal or other fees or expenses incurred by the State arising from any such claim. The State shall give the Contractor notice of any such claim or suit, however, the failure of the State to give such notice shall only relieve Contractor of its obligations under this Section to the extent Contractor can demonstrate actual prejudice arising from the State's failure to give notice. This Section shall not grant the Contractor, through its attorneys, the right to represent the State of Tennessee in any legal matter, as provided in Tenn. Code Ann. § 8-6-106.

The State may participate in the defense of such action with counsel of its own selection and at its sole cost. Contractor shall have no liability to indemnify or defend State to the extent the alleged infringement is based on: (a) a modification of the Services by anyone other than Contractor; (b) use of the Services other than in accordance with the Documentation for such Service or as authorized by the Contract; (c) use of the Services in conjunction with any data, equipment, service or software not provided or approved by Contractor, where the Services would not otherwise itself be infringing or the subject of the claim; or (d) use of the Services by State other than in accordance with the terms of the contract.

E.7. Extraneous Terms and Conditions. Contractor shall fill all orders submitted by the State under this Contract. No purchase order, invoice, or other documents associated with any sales, orders, or supply of any good or service under this Contract shall contain any terms or conditions other than as set forth in the Contract. Any such extraneous terms and conditions shall be void, invalid and unenforceable against the State. Any refusal by Contractor to supply any goods or services under this Contract conditioned upon the State submitting to any extraneous terms and conditions shall be a material breach of the Contract and constitute an act of bad faith by Contractor.

E.8. Prohibited Advertising or Marketing. The Contractor shall not suggest or imply in advertising or marketing materials that Contractor's goods or services are endorsed by the State. The restrictions on Contractor advertising or marketing materials under this Section shall survive the termination of this Contract.

E.9. Lobbying. The Contractor certifies, to the best of its knowledge and belief, that:

a. No federally appropriated funds have been paid or will be paid, by or on behalf of the Contractor, to any person for influencing or attempting to influence an officer or employee of an agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with the awarding of any federal contract, the making of



any federal grant, the making of any federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative agreement.

- b. If any funds other than federally appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with any contract, grant, loan, or cooperative agreement, the Contractor shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.
- c. The Contractor shall require that the language of this certification be included in the award documents for all sub-awards at all tiers (including subcontracts, sub-grants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into and is a prerequisite for making or entering into this transaction imposed by 31 U.S.C. § 1352.

- E.10. Drug-Free Workplace. The Contractor agrees that it shall provide a drug-free workplace pursuant to the Drug-Free Workplace Act of 1988, Title 41 of the United States Code (41 USC) §§ 701 et seq., and the regulations in Title 45 of the Code of Federal Regulations (45 CFR) Part 82.
- E.11. Rule 2 Compliance. Solely to the extent applicable to the Scope of this Contract, the State and the Contractor shall comply with obligations under Rule 2 of the Confidentiality of Alcohol and Drug Abuse Patient Records, and its accompanying regulations as codified at 42 CFR § 2.1 et seq.
 - a. The Contractor warrants to the State that it is familiar with the requirements of Rule 2 of the Confidentiality of Alcohol and Drug Abuse Patient Records, and its accompanying regulations, and will comply with all applicable requirements in the course of this Contract.
 - b. The Contractor warrants that it will cooperate with the State, including cooperation and coordination with State privacy officials and other compliance officers required by Rule 2 of the Confidentiality of Alcohol and Drug Abuse Patient Records, and its regulations, in the course of performance of the Contract so that both parties will be in compliance with Rule 2 of the Confidentiality of Alcohol and Drug Abuse Patient Records.
 - c. The State and the Contractor will sign documents, including but not limited to business associate agreements, as required by Rule 2 of the Confidentiality of Alcohol and Drug Abuse Patient Records, and that are reasonably necessary to keep the State and the Contractor in compliance with Rule 2 of the Confidentiality of Alcohol and Drug Abuse Patient Records. This provision shall not apply if information received by the State under this Contract is NOT "protected health information" as defined by Rule 2 of the Confidentiality of Alcohol and Drug Abuse Patient Records, or if Rule 2 of the Confidentiality of Alcohol and Drug Abuse Patient Records permits the State to receive such information without entering into a business associate agreement or signing another such document.
- E.12. Professional Practice. The Contractor shall assure that there is a code of conduct in place and applicable to all employees that covers, at a minimum, business practices, , and service recipient/staff interaction/fraternization. Further, Contractor's personnel shall conduct their practice in conformity with all applicable statutes, rules and regulations, and recognized ethical standards of their profession. Procedures for reporting violations of the ethical standards shall be developed and communicated to staff upon hire and annually thereafter, which shall include a non-reprisal approach for persons reporting suspected violations, as well as a description of possible sanctions for violating the standards. Failure to implement a code of conduct in accordance with this section and to adequately address suspected violations of the code of conduct may be cause for termination of this Contractor Contract.



- E.13. Additional Subcontracting Requirements. If subcontracts are approved by the State, they shall contain, in addition to those sections identified in D.5., sections on "Confidentiality of Records", "HIPAA Compliance," and "Rule 2 Compliance" (as identified by the section headings). Notwithstanding any use of approved subcontractors, the Contractor shall be the prime contractor and shall be responsible for all work performed.
- E.14. Contractor Commitment to Diversity. Contractor shall assist the State in monitoring the Contractor's reasonable business efforts of commitment to diversity by providing, as requested, a quarterly report of participation in the performance of this Contract by small business enterprises and businesses owned by minorities, women, and Tennessee service-disabled veterans. Such reports shall be provided to the State of Tennessee Governor's Office of Diversity Business Enterprise in the required form and substance.
- E.15. Additional lines, items, or options. At its sole discretion, the State may make written requests to the Contractor to add lines, items, or options that are needed and within the Scope but were not included in the original Contract. Such lines, items, or options will, once mutually agreed by the parties be added to the Contract through a Memorandum of Understanding ("MOU"), not an amendment.
- a. After the Contractor receives a written request to add lines, items, or options, the Contractor shall have ten (10) business days to respond with a written proposal. The Contractor's written proposal shall include:
 - (1) The effect, if any, of adding the lines, items, or options on the other goods or services required under the Contract;
 - (2) Any pricing related to the new lines, items, or options;
 - (3) The expected effective date for the availability of the new lines, items, or options; and
 - (4) Any additional information requested by the State.
 - b. The State may negotiate the terms of the Contractor's proposal by requesting revisions to the proposal.
 - c. To indicate acceptance of a proposal, the State will sign it. The signed proposal shall constitute a MOU between the Parties, and the lines, items, or options shall be incorporated into the Contract as if set forth verbatim.
 - d. Only after a MOU has been executed shall the Contractor perform or deliver the new lines, items, or options.

IN WITNESS WHEREOF,

KRONOS INCORPORATED:



CONTRACTOR SIGNATURE

November 2, 2016

DATE

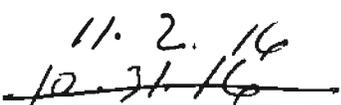
Alyce Moore, VP, General Counsel

PRINTED NAME AND TITLE OF CONTRACTOR SIGNATORY (above)

DEPARTMENT OF MENTAL HEALTH AND SUBSTANCE ABUSE SERVICES:



MARIE WILLIAMS, COMMISSIONER

11.2.16


DATE



SYSTEM REQUIREMENTS

Contractor shall meet the following requirements:

1. Staff shall have the ability to electronically submit leave requests.
2. The system shall disallow leave entries that are greater than the employee's normal work hours (some are 7.5, 8 and some are 12.5, etc.)
3. The system shall support the pre-loading of current year FMLA hours used for transition purposes.
4. The system shall notify supervisors when a leave request has been submitted for approval.
5. Supervisors shall have the ability to approve or deny submitted leave requests for their staff.
6. Supervisors approval/denial on leave requests shall send a notification to the requesting staff member.
7. Staffing Coordinators shall have the ability to view leave requests for the facility.
8. Supervisors shall have the ability to view an historical list of leave requests for their staff.
9. Staff shall have the ability to view their own historical list of leave requests.
10. Staff shall have the ability to retract (delete) a leave request.
11. Supervisors shall have the ability to cancel a staff's leave request after approval.
12. The system shall verify the employee has enough leave before accepting request.
13. Contractor Leave Policies can be configured to allow for leave overdrafts.
14. The system shall have the ability to enter FMLA, Workers' Compensation and Sick Leave Bank requests.
15. The system shall give the Staffing Coordinator the opportunity to add a staff member to the schedule for a deleted leave request.
16. The system shall recognize a schedule needs to be generated for the next cycle (currently one month in advance).
17. Staffing Coordinators shall have the ability to manually generate a schedule.
18. The system shall have the ability to repeat staffing patterns into the future.
19. The system shall support user-defined shifts by facility and by unit.
20. The system shall subtract staff availability for a new schedule based on all leave requests.
21. The system shall use rules to determine the number and type of staff needed per shift based on staff to patient ratio requirements.
22. The system shall observe the limit of the number of hours a job role may work consecutively during schedule creation. (Currently 16 consecutive hours.)
23. The system shall recognize the number and type of workers needed for each shift based on patient needs (i.e., one RN per unit per shift).
24. The system shall allow managers to schedule mandatory requirements.
25. The system shall allow voluntary overtime (amount above mandatory overtime).
26. The system shall support rules regarding mandatory and voluntary overtime.
27. The system will assign workers to their regularly scheduled unit.
28. The system shall track staff availability to assist in automatic schedule generation.
29. The system shall check on gender ratio when creating a default schedule; females cannot work without a male on duty.
30. The system shall check business rules to ensure all staffing needs are met.
31. The system shall recognize workers' have varying lengths to their work day such as 7.5, 8, 12, 12.5.



32. Staffing Coordinators shall have the ability to notify supervisors a new schedule is ready for review via email or kmail.
33. Supervisors shall have the ability to post or unpost of a new schedule.
34. The system shall notify the Staffing Coordinator of the posting/unposting of a new schedule (from the supervisor).
35. The system shall contain a configurable calendar for State holidays.
36. The system shall track which employees have worked holidays historically.
37. The system shall support the ability to require FMLA or Workers' Comp return to work orders before allowing staff to be scheduled.
38. Staff shall have the ability to view all entries on the schedule for their facility.
39. The system shall use notation on the schedule to indicate leave (sick, annual, FMLA) and overtime (mandatory and voluntary).
40. Staffing Coordinators shall have the ability to update scheduled time based on TDMHSAS policy (dates in the past) up to payroll signoff, or by using historical edits.
41. The system shall support twenty four hour scheduling such as: 10:00 p.m. to 6:00 a.m.
42. Staffing Coordinators shall have the ability to communicate shift vacancies to State staff.
43. Staffing Coordinators shall have the ability to see a list of staff members willing to accept extra shifts during shift vacancy reconciliation.
44. The system shall contain an indicator on staff to indicate willingness to work extra shifts.
45. Staff shall have the ability to indicate shifts they would like added to their schedule.
46. Staffing Coordinators shall have the ability to approve/deny extra shift requests.
47. Staffing Coordinators shall have the ability to update schedules in the future.
48. The system shall notify the appropriate staff of a new vacancy when a leave request has been approved after the schedule has been generated.
49. Staffing Coordinators shall have the ability to generate a list of temporary staffing needs for submission to staffing agencies (Knowledge Services).
50. Staffing Coordinators shall have the ability to indicate temporary staff on shift vacancies to complete the schedule.
51. Staff shall have the ability to submit a shift swap request.
52. The system shall notify both staff members of a pending shift swap request.
53. The system shall require both employees to indicate approval of the shift swap.
54. The system shall deny a shift swap for incompatible job roles.
55. The system shall notify the supervisors of staff who have submitted shift swap requests.
56. The system shall run staffing rules on the shift swap request and include results (issues) for the supervisor. (Example: When the swap request is submitted by both employees, the system will know if the request causes an overtime rule violation and indicate on the screen for the supervisor's review.)
57. Supervisors shall have the ability to approve/deny shift swap requests.
58. The system shall notify staff of the shift swap disposition.
59. The system shall update the schedule based on approval of a shift swap.
60. The system shall notify the Staffing Coordinator when a shift swap request is fulfilled (approved).
61. Staffing Coordinators and Nurse Supervisors shall have the ability to record daily escorts (outside appointments) for the day.
62. The system shall run staffing rules when patient census, 1:1 (1 patient to 1 tech), 2:1, GOA (special observation - higher ratio) or daily escort information is added to the schedule.
63. The Staffing Coordinator and Nurse Supervisor will be able to see when a staffing shortage occurs based on daily updates (census, 1:1 (1 patient to 1 tech), GOA (special observation -



- higher ratio) and escorts). Staff shall have the ability to identify themselves electronically or biometrically near their work area for check-in (clocking in) and check-out.
64. Staff shall have the ability to record time away from the unit (paid) such as escorts, training.
 65. The system can be configured to restrict staff from being able to clock in early.
 66. Upon selection of the function by the employee, the system shall display scheduled hours for the employee upon check/in and check/out.
 67. Upon selection of the function by the employee, the system shall display hours worked upon clock/out.
 68. The system shall have the ability to report on temporary employees by date range and by shift, displaying hours worked based on recorded time.
 69. Staff shall have the ability to view leave balances on the timekeeping unit.
 70. Supervisors shall have the ability to approve timesheets for their staff at the end of the pay period based.
 71. The system shall provide a warning to employees clocking in late (as defined by State policy - currently six minutes). The warning/notation will show on the employee's time card.
 72. The system shall provide a warning to employees clocking out early as defined by State policy. The warning/notation will show on the employee's time card.
 73. The system shall suspend notification of an early or late warning when an approved leave request is approved for the date in question.
 74. The system shall provide discrepancy reports of scheduled time versus clock in/out times.
 75. The system shall support configuration of timekeeping screens based on job role without customization.
 76. The system shall retain scheduled versus worked time for an archival period designated by the State.
 77. Supervisors shall have the ability to edit clock in/clock out times based on pay period end rules. Supervisors shall have the ability to record leave information for an absent employee.
 78. The system shall require a reason for and employee editing clock in/clock out times.
 79. The system shall provide a list of values (dropdown) for the reason for editing clock in/clock out times.
 80. The system shall support an unlimited number of job roles, facility areas (units) and facilities.
 81. The system shall provide for unexcused absence reporting.
 82. The system shall have the ability to report statistical information on work and absence trends.
 83. The system shall use various levels of security rules on time entry approval including approval rank and pay period end timeliness.
 84. Supervisors shall have the ability to edit clock in/clock out times during the approval process.
 85. Supervisors shall be locked out of approvals and time entry edits based on State pay period end rules. (Upon "signoff" of the time cards in Kronos).
 86. The system shall notify Staffing Coordinators and time approvers of pay period end approval needs.
 87. The system shall not allow multiple clock-ins or clock-outs by the same employee.
 88. The system shall disallow updates to scheduled and clock in/clock out times after time has been submitted to Edison upon "signoff" of the time cards" in Kronos.
 89. The system shall allow non-State employees to record time (see Interface requirements).
 90. The system shall contain configurable pay periods. (State is twice-monthly.)
 91. The system shall provide the ability to report on non-State staff time entries.
 92. The system shall support the ability to record FMLA hours used.
 93. The system shall retain and display year-to-date FMLA hours used.
 94. The system shall track the number of hours an employee has worked towards FMLA eligibility.



95. The system shall have the ability to disallow an employee from clocking-in when they are not scheduled based on State policy.
96. The system shall disallow clock/in and clock/out for terminated employees; supervisors may enter time for terminated employees.
97. The system shall have the ability to report the exact location where the employee worked their time: unit, infection control, facility, etc.
98. The system shall have the ability to report time for MODs by shift.
99. Physicians who work offsite (physician's row at Western) shall have the ability to report time.
100. Staffing Coordinators shall have the ability to pull recorded time and cost for non-State employees versus State employees, as well as, combined reporting.
101. The system shall compute payroll cost based. (Pay differentials are 5% and 8% currently.) if pay rates are stored in Kronos.
102. Supervisors shall have the ability to report on FMLA hours earned and used by unit, facility and for the State for a specified date range.
103. The system shall have the ability to report on pay differential costs separate from regular (base) costs.
104. The system shall have the ability to report on hours and cost for each type of pay codes such as RegS1, RegS2, RegS3, LWOP, Civil Leave, Assault Leave, etc.
105. The system shall have the ability to compute regular overtime, premium overtime (1.5) and compensatory time. Compensatory time also has a maximum, and then reverts to cash overtime.
106. The system shall have the ability to report payroll costs for both State and temporary staff.
107. The system shall use leave based on policy regarding compensatory, annual and sick leave.
108. The system shall interface credentials and training to the State ERP system.
109. The system shall transmit leave requests, leave approvals, time scheduled and time worked with interfaces utilizing Workforce Integration Manager.
110. The system shall populate staff profiles from the State's ERP system (Edison).
111. The system shall revoke access to a staff member when they are terminated in the State's ERP system (Edison).
112. The system shall support the manual loading of staff profiles in addition to interfaced staff profiles. (temporary staff, etc.)
113. The system shall include only State staff in the time submission to the State's ERP system (Edison).
114. The system shall provide total number of hours worked when reporting to the State's ERP system.
115. The system shall receive patient census information from the department's EMR system.
116. The system shall receive patient census, 1:1 (1 patient to 1 tech) and GOA (special observation - higher ratio) requirements at designated times throughout the day. (note: includes the cumulative effect of discharges)
117. The system shall support a designation of FMLA, intermittent FMLA, workers' compensation, extended leave for a staff member.
118. The system shall provide alerts to staff, supervisors and Staffing Coordinators.
119. Staff shall have the ability to view scheduling and timekeeping information in near real time.
120. The system shall allow rules to be applied at a staff member or job role level. (Example - pay differentials).
121. The system shall have the ability to produce time and attendance reports for a specified date range.



122. The system shall have the ability to produce overtime reports, showing mandatory and voluntary overtime totals by employee and total by unit and facility. Also include breakdown by regular overtime and premium overtime (1.5).
123. The system shall have the ability to report on employees with time infractions as designated by TDMHSAS.
124. The system shall have the ability to report by date range, by facility, by unit and by job class (RN, LPN and Psych Tech) the number of regular, overtime and temporary (agency staff) hours. (Allow option to break out by the day or summary total) (Provide monthly totals).
125. The system shall have the ability to report overtime by facility, by unit, by shift, by category (mandatory and voluntary, include regular overtime and premium overtime) and by staff member for a specific date range.
126. The system shall support exception reporting (time not worked versus scheduled time).
127. The system shall support the display of up to date information for staff (messages, schedules).
128. Supervisors shall be notified when FMLA medical certification and Workers' Compensation return to work orders are due.
129. The system shall have the ability to report on leave abuse, such as taking leave on weekends and State holidays.
130. The system shall have the ability to report on baseline schedules versus actual time worked - show volatility.
131. The system shall provide audits of deletions and updates of system information.
132. TDMHSAS designated staff shall have the ability to view audit data.
133. Supervisors shall have the ability to record required licenses and certifications for their staff members.
134. Supervisors shall have the ability to record effective and expiration dates for licenses and certifications.
135. The system shall provide a notification to staff and their supervisors when a license or certification is about to expire.
136. The system notification timing of expiring licenses and certifications shall be maintainable without custom code.
137. The system shall have the option to prevent clock ins based on expired licenses and credentials by either a manual function or an automated function using Workforce Integration Manager.
138. Supervisors shall have the ability to view a historical list of licenses and certifications for their staff.
139. Managers shall have the ability to view their staff's historical list of licenses and certifications.
140. Supervisors shall have the ability to record the need for required certifications for each staff member.
141. Supervisors shall have the ability to record the date certification was completed for their staff.
142. The system shall notify staff when they have certifications that need to be completed.
143. This is covered in our SaaS terms and conditions. All web-based programs must be compatible with Internet Explorer 11.
144. The system shall be compatible with Windows 7 and greater.
145. The system must support multiple time zones and daylight savings time.
146. The system shall provide the ability to withstand spikes in utilization and maintain peak performance.
147. The system shall provide assurance that system searches and reporting will not degrade performance during high peak periods as long as Kronos best practices recommendations for system searches are reporting are followed, excluding custom reports.



148. The system shall provide layered security for the application.
149. The system shall provide the ability for a authorized TDMHSAS staff to view audit logs and security reports.
150. The system shall provide the ability to require user confirmation prior to deleting data.
151. The system shall provide the ability to require user confirmation prior to changes to user profile.
152. The system shall provide the ability to require confirmation of identity on changes to profile information.
153. The system shall provide encryption of sensitive data as defined by the State. Web/API app interfaces and Kronos SFTP are protected using SSL certs with a minimum Asymmetric 2048-bit keys and a minimum 256-bit Symmetric key Transport Layer Security (TLS) encryption. Customers must have contemporary browser (IE 11, Firefox 35+, or Google Chrome 41+) that support this level of encryption.
154. The system shall provide encryption of all transmitted sensitive data.
155. The system shall provide digital signatures at the State minimum of 256-bit encryption.
156. The system shall provide the ability to lock a user account based on multiple failed logon attempts defined by TDMHSAS staff.
157. The system shall provide the ability to log users out of the system.
158. The system shall mask the characters of sensitive data designated by TDMHSAS.
159. Support double keying for password setting.
160. The system shall restrict the setting of a password to exclude Expiration frequency, Reuse monitoring for password, password complexity (uppercase, lower class, max & min length, numeric & alpha numeric), Max consecutive characters, max sequential numbers, use or not use password history, lockout on number of failed logins & lockout duration.
161. The system shall provide the ability for a user to reset a forgotten password.
162. The system shall provide the ability to display password expiration prompts before expiration.
163. The system shall provide the ability to enforce the changing of passwords on demand.
164. The system shall provide the ability for TDMHSAS staff to define password expiration time frames.
165. The system shall provide the ability for system users to change their password on demand.
166. The system shall not display personal identifying information such as date of birth or SSN on the timekeeping unit.
167. The system shall provide role-based access to specific screens.
168. The system shall provide role-based access to database tables.
169. The system shall provide role-based accessibility at the application module level.
170. The system shall allow the administrator to turn features on and off by job role and/or by individual user.
171. The system shall provide role-based security for viewing.
172. The system shall provide role-based security for updates.
173. The system shall provide role-based security for the creation of records.
174. The system shall provide role-based security for the deletion of records.
175. The system shall support the restriction of TDMHSAS designated leave codes such as administrative leave with pay.
176. The system shall provide the ability for TDMHSAS staff to define user security roles.
177. The system shall provide the ability to assign multiple users to a single role.
178. The system shall provide the ability to define multiple roles for a single user.
179. The system shall support allowing access to employee data based on their position in the organizational hierarchy (supervisors see their employees data, a CEO can see their facility data).



- 180. The system shall provide data access through Secure Socket Layers (SSL).
- 181. The system shall provide security consistent with SOC 1 and SOC 2 certifications.
- 182. The system shall provide authorized TDMHSAS staff the ability to view specific user access rights and levels of security.
- 183. The system shall include a means of system alerts and or email notifications for all users to communicate important system administration, operational or business related information to individual users, user groups or as a universal broadcast.
- 184. The system shall use navigation in a consistent manner throughout the application.
- 185. The system shall display common information with consistency throughout the application (ex., addresses)
- 186. The system shall clearly explain error messages to the user.
- 187. The system shall provide help content that is consistent with the current release level.
- 188. The system shall provide the ability to generate a unique error message for each error.
- 189. The system shall provide the ability to clearly identify which fields are in error.
- 190. The system shall provide processing visual displays indicating that the system is in the process of responding to the user's request.
- 191. The system shall prevent inadvertent multiple processing such as a user clicking a submit button twice or using badge or biometric log in multiple times.
- 192. Any software upgrades will be backward compatible with existing Kronos-created interfaces.
- 193. Manager and staff functionality can be accessed on mobile operating systems including iOS and Android.
- 194. The system shall provide pay rules that are easy to set up and change without programming customizations.
- 195. The system shall support simultaneous calendar and fiscal year configurations for reporting.
- 196. The system shall provide searchable training content. (provided in KnowledgePass).
- 197. The system shall provide on line and/or computer based training that is self-paced and module specific.
- 198. The system shall be capable of exporting to alternate formats such as xls, pdf, csv and other common formats.
- 199. So long as the State reporting tools allow reporting via ODBC connection, the system shall integrate with leading reporting tools for State custom reporting.
- 200. The system shall allow specified users to run on-demand reports.
- 201. The system shall support recurring report and dashboard generation. (scheduling)
- 202. The system shall be built on Windows servers and [REDACTED] database with supported versions listed below:

Supported technology Desktop requirements

Browser			Operating System		
Vendor	Product	Version	Vendor	Product	Version
Microsoft	Internet Explorer	10 and 11	Microsoft	[REDACTED]	[REDACTED]
Google	Chrome	41+	[REDACTED]	[REDACTED]	[REDACTED]
Mozilla	Firefox 32-bit	35+	[REDACTED]	[REDACTED]	[REDACTED]
Apple	Safari	7.x and 8.x	Apple	[REDACTED]	[REDACTED]

Database Server Technology Support

Database	Operating System
----------	------------------



[REDACTED]



All operating systems that [REDACTED] supports for these database versions

[REDACTED]

All operating systems that [REDACTED] supports for these database versions

Standard, Workgroups, Small Business, and Enterprise editions only

- 203. The system shall provide audit trail of user activity, including before/after values from all updates.
- 204. Provide a ability for system administrator (or other authorized user) to modify screen layouts and flow with minimal programming effort.
- 205. Provide ability to store all records on-line for a user-defined number of years.
- 206. The system shall have non-SSN record keys.
- 207. The system shall provide the ability to begin the use of a list of value entry on a specific date for certain tables such as accounts table.
- 208. The system shall provide the ability to stop the use of a list of value entry on a specific date such as accruals tables.
- 209. The system shall contain safeguards to reduce the risk of data loss when staff closes the application.
- 210. Kronos will make the available the VPAT reports and assist the State in making preliminary assessments regarding the availability of commercial "Electronic and Information Technology" products and services with features that support accessibility.
- 211. The system shall provide alerts and logs for system administrators during error conditions.
- 212. The system shall validate field entry according to the associated list of values.
- 213. An interface to Edison shall be provided that includes a time / leave export from Kronos to Edison, a demographics import from Edison to Kronos, and an Accrual import from Edison to Kronos. An example layout is shown in the table below:

Field Name	Short Description	Definition	Description
EMPL_ID		NUMBER(10,0)	Employee Sequence number
EMPL_JJ_NBR		VARCHAR2(10 BYTE)	JJ number
EMPL_UNIT	UNIT	VARCHAR2(4 BYTE)	Unit ID
EMPL_REGN_ID		VARCHAR2(1 BYTE)	Region ID
EMPL_EDISON_ID	EMPLID	VARCHAR2(10 BYTE)	Edison ID number
EMPL_SSN	SSN	CHAR(9 BYTE)	Social Security Number
EMPL_LAST_NME	LAST	VARCHAR2(14 BYTE)	Employee last name
EMPL_FIRST_NME	FIRST	VARCHAR2(14 BYTE)	Employee first name
EMPL_MI	MIDDLE	VARCHAR2(2 BYTE)	Employee middle initial
EMPL_DEPT_ID	DEPTID	VARCHAR2(10 BYTE)	Department ID
EMPL_DEPT_DESC	DEPT_DESCR	VARCHAR2(10 BYTE)	Department
EMPL_WRK_ADDR1	BUSADDRESS1	VARCHAR2(55 BYTE)	Employee Work Address1
EMPL_WRK_ADDR2	BUSADDRESS2	VARCHAR2(55 BYTE)	Employee Work Address2
EMPL_WRK_CITY	BUSCITY	VARCHAR2(30 BYTE)	Employee Work City
EMPL_WRK_STATE	BUSSTATE	VARCHAR2(6 BYTE)	State
EMPL_WRK_ZIP	BUSZIP	VARCHAR2(10 BYTE)	Employee Work Zip
EMPL_APP_CDE		VARCHAR2(5 BYTE)	The last 5 digits of Department ID
EMPL_POSTN_NBR	STAF_POS_NO	VARCHAR2(13 BYTE)	Position Number
EMPL_POSTN_TTL	POS_TITLE	VARCHAR2(12 BYTE)	Position Title



EMPL_PER_TTL_SHR T	PER_TITLE	VARCHAR2(12 BYTE)	Position Title Short Description
EMPL_LAST_PAY_CH NG	LAST_PAY_CHANGE	DATE	Last Pay Change
EMPL_MON_PAY_RTE	MO_PAY_RT	NUMBER(7,0)	Monthly Pay Rate
EMPL_CURR_GROSS	CURR_GROSS	NUMBER(6,0)	Current Gross
EMPL_STAT	STATUS	VARCHAR2(1 BYTE)	Represents Active A Terminate T Inactive I
EMPL_HIRE_DTE	HIRE_DT	DATE	Employee Hire Date
EMPL_REG_OT	REG_OT	NUMBER(5,0)	Regular Overtime
EMPL_PERM_OT	PREM_OT	NUMBER(5,0)	Premium Overtime
EMPL_ACCRD ANN	ACCRD_ANL	NUMBER(6,2)	Accrued Annual Leave
EMPL_ACCRD SICK	ACCRD_SICK	NUMBER(7,2)	Accrued Sick Leave
EMPL_ACCRD COMP	ACCRD_COMP	NUMBER(6,2)	Accrued Comp Time
EMPL_SEX	SEX	CHAR(1 BYTE)	Represents F Female or M Male
EMPL_RACE	RACE	VARCHAR2(1 BYTE)	Race
EMPL_BIRTH_DTE	BIRTHDATE	DATE	Birthdate
EMPL_TERM_DTE	TERM_DT	DATE	Termination Date
EMPL_STR_ADDR	ADDR_ST	VARCHAR2(22 BYTE)	The State in which the Employee Resides
EMPL_CTY_ZIP	ADDR_CITY_ZIP	VARCHAR2(21 BYTE)	The City and Zip Code in which the Employee Resides
EMPL_ANN_DTE	ANL_DT	DATE	Anniversary Date of Employees Employment
EMPL_ANN_GRP	ANL_GRP	NUMBER(1,0)	"Service Months Group (0 - 60 Months = '1' 61 - 120 Months = '3' 121 - 240 Months = '4' 241 and Above = '5')"
EMPL_PS	PS	VARCHAR2(4 BYTE)	Filled with Zeros
EMPL_TOT_SER_MTH S	TOT_SERV_MOS	NUMBER(3,0)	Total Number of Months of Employee's Service
EMPL_WRK_CNTY	WORK_CTY	VARCHAR2(2 BYTE)	County in which Employee Works
EMPL_LGL_CNTY	LEGAL_CTY	VARCHAR2(2 BYTE)	County in which the Employee Legally works
EMPL_DEI	DEI	VARCHAR2(4 BYTE)	Filled with Zeros
EMPL_ACTION_CDE	ACTION	VARCHAR2(3 BYTE)	Action Code
EMPL_ACTION_RSN	ACTION_REASON	VARCHAR2(3 BYTE)	Action Reason
EMPL_POS_TTL_NBR	POS_TITLE_NO	VARCHAR2(5 BYTE)	Position Title Number
EMPL_POS_PAY_GRD E	POS_PAY_GRADE	VARCHAR2(3 BYTE)	Position Pay Grade
EMPL_MAX_STEP	MAX_STEP	VARCHAR2(2 BYTE)	Maximum Step
EMPL_ACTION_EFF_D TE	EFFDT	DATE	Action Effective Date
EMPL_PER_TTL_NBR	PER_TITLE_NO	VARCHAR2(5 BYTE)	Per Title Number
EMPL_CUR_PAY_GRD E	CUR_PAY_GRADE	VARCHAR2(3 BYTE)	Current Pay Grade
EMPL_CUR_STEP	CUR_STEP	VARCHAR2(2 BYTE)	Current Step
EMPL_FLSA	FLSA	VARCHAR2(1 BYTE)	"FLSA Status



			A = '2' E = '2' O = '2' M = '2' C = '2' P = '2' N = '1' X = '3'"
EMPL_WRK_PHNE	WORK_PHONE	VARCHAR2(10 BYTE)	Employee Work Phone
EMPL_CR_DED	CREDIT_UN_DEDUC	VARCHAR2(4 BYTE)	Credit Union Deduction
EMPL_HOME_PHNE	HOME_PHONE	VARCHAR2(10 BYTE)	Employee Home Phone
EMPL_PROB_EXP_DT E	PROBATION_EXP_DT	DATE	Probation Expiration Date
EMPL_INS_SCHD	INS_SCHED	VARCHAR2(4 BYTE)	Insurance Schedule
EMPL_FILL3	FILL3	VARCHAR2(8 BYTE)	Filled with Spaces
EMPL_MAR_STA	MARITAL_STATUS	VARCHAR2(1 BYTE)	Marital Status
EMPL_APP_CUR_CLS DTE	DATE_APPTD_CUR_C LS	DATE	Job Entry Date
EMPL_FILL4	FILL4	VARCHAR2(3 BYTE)	Filled with Spaces
EMPL_ST_MTCH_RET	STATE_MATCH_RETIR	VARCHAR2(7 BYTE)	State Retirement Match
EMPL_ST_MTCH_FIC A	STATE_MATCH_FICA STATE_MATCH_INSU R	VARCHAR2(7 BYTE)	State FICA Match
EMPL_ST_MTCH_INS	STATE_MATCH_INSU R	VARCHAR2(5 BYTE)	State Insurance Match
EMPL_LEAV_USED_A NN	LEAVE_USED_ANL	NUMBER(5,0)	Annual Leave Used
EMPL_LEAV_USED_C OMP	LEAVE_USED_COMP	NUMBER(5,0)	Comp Leave Used
EMPL_LEAV_USED_SI CK	LEAVE_USED_SICK	NUMBER(5,0)	Sick Leave Used
EMPL_LEAV_USED_CI VIL	LEAVE_USED_CIVIL	NUMBER(5,0)	Civil Leave Used
EMPL_LEAV_USED_M LTRY	LEAVE_USED_MIL	NUMBER(5,0)	Military Leave Used
EMPL_LEAV_USED_E DUC	LEAVE_USED_EDUC	NUMBER(5,0)	Educational Leave Used
EMPL_LEAV_USED_H DAY	LEAVE_USED_HOL	NUMBER(5,0)	Holiday Leave Used
EMPL_HR_EQUIV_RT E	HOURLY_EQUIV_RAT E	NUMBER(9,0)	Hourly Equivalent Rate
EMPL_LNGV	LONGEVITY	NUMBER(6,0)	Longevity
EMPL_EEO4_CDE	EE04CODE	VARCHAR2(1 BYTE)	EEO4 Code
EMPL_OFFICER_CDE	OFFICER_CD	VARCHAR2(1 BYTE)	Officer Code
EMPL_DEL		VARCHAR2(1 BYTE)	Employee Deleted
EMPL_CRTE_BY		VARCHAR2(15 BYTE)	Employee Created By
EMPL_CRTE_DTE		DATE	Employee Created Date
EMPL_LAST_EDT_BY		VARCHAR2(15 BYTE)	Employee Last Edited By
EMPL_LAST_EDT_DT E		DATE	Employee Last Edited Date
EMPL_MMS_RCD	EMPL_RCD	NUMBER(1,0)	Employee MMS Record
EMPL_EMAIL	EMAILID	VARCHAR2(50 BYTE)	Employees email address



	APPROP	NUMBER	
	PAY_CENTS	NUMBER	
	UNION_CD	NUMBER	



ATTACHMENT 2

PRICING LIST

Item Description	List Price Base PEPM	Base PEPM = 48% Discount	Required Monthly Host Base Price
Workforce Central SaaS			Single Base Fee Per New SaaS Instance - Non-Discountable
TIMEKEEPER			
WFC Timekeeper Bundle - per employee per month (Timekeeper, Employee, Manager, Integration Manager, Mobile Employee and Mobile Manager) * Timekeeper to Manager Ratio is 10:1	\$5.00	\$2.60	\$1000 BASE + \$1.00 PEPM
Quick Time Stamp Offline - per employee per month	\$0.50	\$0.26	
Workforce Tablet - per employee per month	\$1.00	\$0.52	
Additional Managers for Workforce Central - per Mgr per month	\$25.00	\$13.00	
ARCHIVING			
Workforce Enterprise Archiver - per employee per month	\$0.30	\$0.16	\$1000 BASE
SCHEDULING			
Workforce Scheduler - per employee per month	\$2.50	\$1.30	
Workforce Forecast Manager - per employee per month	\$2.50	\$1.30	
Workforce Budgeting - per employee per month	\$2.50	\$1.30	
Workforce Task Management - per employee per month	\$2.50	\$1.30	
Workforce Forecast Manager for Healthcare - per employee per month	\$0.50	\$0.26	
Workforce Target Intelligence - per employee per month	\$0.75	\$0.39	
Workforce Workload Manager - per employee per month	\$1.25	\$0.65	\$1000 BASE + 1.00 PEPM
ABSENCE MANAGEMENT			
Workforce Absence Manager - per employee per month	\$2.50	\$1.30	
Workforce Accruals - per employee per month	\$1.00	\$0.52	
Workforce Attendance - per employee per month	\$1.00	\$0.52	
Workforce Leave - per employee per month	\$2.00	\$1.04	
OTHER			
Workforce Tips & Tokes - per employee per month	\$0.50	\$0.26	
Workforce Activities - per employee per month	\$2.50	\$1.30	
ANALYTICS			
Workforce Analytics Core - per employee per month	\$2.50	\$1.30	\$1000 BASE + .15 PEPM
Workforce Analytics for Public Sector - per employee per month	\$2.50	\$1.30	
Workforce Analytics for Healthcare - per employee per month	\$3.75	\$1.95	
KSS TOOLS			
KSS Tool Attestation Took Kit - per employee per month	\$0.50	\$0.26	
KSS Tool FT-PT Analysis Report - per month	\$250.00	\$250.00	NON-DISCOUNTABLE
KSS Tool Kronos Time Capture for Cisco - per employee per month	\$1.50	\$0.78	
KSS Timecard Confirmation - per month	\$200.00	\$200.00	NON-DISCOUNTABLE
KSS Tool Scheduling Attestation - per month	\$500.00	\$500.00	NON-DISCOUNTABLE
TELESTAFF			
Workforce TeleStaff Enterprise - per employee per month	\$5.00	\$2.60	\$1250 BASE + .50 PEPM
Workforce TeleStaff Institution Focus - per employee per month	\$0.75	\$0.39	

Item Description	List Price Base PEPM	Base PEPM = 48% Discount	Required Monthly Host Base Price
Workforce Central SaaS			Single Base Fee Per New SaaS Instance - Non-Discountable
Workforce TeleStaff Global Access - per employee per month	\$ 1.00	\$0.52	
Workforce TeleStaff Gateway Manager - per month	\$150.00	\$78.00	



Workforce TeleStaff Gateway Manager V5 Interact to WFC		\$0.00	
Workforce TeleStaff Contact Manager - per employee per month	0.50	\$0.26	
Workforce Integration Manager V8 to TeleStaff		\$0.00	
Workforce TeleStaff Bidding per employee per month	2.00	\$1.04	
TELESTAFF IVR			
Workforce TeleStaff IVR (Per Minute Pricing Based on Usage - Invoices Monthly in Arrears)		\$0.00	.13 PER MINUTE
TELETIME IP			
WORKFORCE TELETIME IP, BASE SYSTEM, 5 LINES - per month	\$1,000.00	\$520.00	\$1,000 Base Plus \$400 Cross-Connect Plus \$500 Per 25 Lines Per Month
WORKFORCE TELETIME IP, ADD'L LINE, LINES 6-10 - per month	\$150.00	\$78.00	
WORKFORCE TELETIME IP, ADD'L LINE, LINES 11+ - per month		\$26.00	
WORKFORCE TELETIME IP, BASE SYSTEM, 5 LINES, 2ND LANGUAGE - per month	\$150.00	\$78.00	
WORKFORCE TELETIME IP, ADD'L LINE, LINES 6-10, 2ND LANGUAGE - per month		\$7.80	
WORKFORCE TELETIME IP, ADD'L LINE, LINES 11+, 2ND LANGUAGE - per month	\$7.50	\$3.90	
ADDITIONAL OPTIONAL SERVICES			
Workforce Timekeeper Bundle with Enhanced Disaster Recovery NOTE - Workforce Analytics, Enterprise Archive, TeleStaff, Workforce TeleTime IP and all non-Production environments are excluded from Enhanced DR	\$5.00	\$2.60	\$2000 BASE + \$1.25 PEPM
Cloud Hosting WFC Add Non Prod Monthly Fee		\$0.00	\$1,000.00
Cloud Hosting Temporary Non-Prod Monthly Fee - 12+ month term		\$0.00	\$1,600.00
Cloud Hosting Temporary Non-Prod Monthly Fee - 6 month term			\$2,700.00
Cloud Hosting Temporary Non-Prod Monthly Fee - 3 month term			\$4,400.00
Cloud Hosting WFC Add One VPN Monthly Fee	-	\$0.00	\$75.00
Cloud Hosting WFC Add One Citrix License Monthly Fee	-	\$0.00	\$50.00
Cloud Hosting WFC Add One SFTP License Monthly Fee	-	\$0.00	\$25.00
Cloud Hosting WFC Add 100GB Storage Monthly Fee	-	\$0.00	\$43.00
Cloud Hosting WFC Add 100GB Backup Monthly Fee	-	\$0.00	\$18.00

Item Description	List Price	Final Price	HDW Annual Support (per Unit)	
Purchased Hardware *Discount based on minimum purchase of 50 Units		*36% Discount	Depot Repair	Depot Exchange
KRONOS INTOUCH H3 Standard Enclosure, with Bar Code Badge Reader	\$3,595.00	\$2,300.80	\$210.00	\$285.00
KRONOS INTOUCH H3, Standard Enclosure, with Magnetic Stripe Card Reader	\$3,745.00	\$2,396.80	\$210.00	\$285.00
KRONOS INTOUCH H3, Standard Enclosure, with HID Proximity Card Reader	\$4,295.00	\$2,748.80	\$210.00	\$285.00
KRONOS INTOUCH H3, Standard Enclosure, with EM4102 Proximity Card Reader	\$4,295.00	\$2,748.80	\$210.00	\$285.00
KRONOS INTOUCH H3, Standard Enclosure, with Smart Card Reader	\$4,395.00	\$2,812.80	\$210.00	\$285.00
KRONOS INTOUCH H3, Slim Enclosure, with Magnetic Stripe Card Reader	\$3,745.00	\$2,396.80	\$210.00	\$285.00
KRONOS INTOUCH H3, Slim Enclosure, with HID Proximity Card Reader	\$4,295.00	\$2,748.80	\$210.00	\$285.00
KRONOS INTOUCH H3, Slim Enclosure, with EM4102 Proximity Card Reader	\$4,295.00	\$2,748.80	\$210.00	\$285.00
KRONOS INTOUCH H3, Slim Enclosure, with Smart Card Reader	\$4,395.00	\$2,812.80	\$210.00	\$285.00
Item Description	List Price	Final Price	HDW Annual Support (per Unit)	
Additional Options Available for Kronos InTouch H3 Standard Enclosure		36% Discount	Depot Repair	Depot Exchange
Kronos Touch ID Plus Biometric Option for InTouch H3	\$1,200.00	\$768.00	\$96.00	\$120.00
Kronos Touch ID Biometric Option for InTouch H3	\$1,200.00	\$768.00	\$96.00	\$120.00
Biometric Enrollment PreScan Pad for Touch ID Plus	\$15.00	\$9.60	N/A	N/A



Wi-Fi Option Kit for H3 InTouch	\$250.00	\$160.00	N/A	N/A
InTouch Linear Imager Bar Code Scanner Option	\$735.00	\$470.40	\$58.80	\$73.50
InTouch Battery Backup Option	\$290.00	\$185.60	N/A	N/A
InTouch H3 Transition Board Option (required if ordering one or more of the following options)	\$100.00	\$64.00	N/A	N/A
InTouch Remote Bar Code Reader Option	\$450.00	\$288.00	\$36.00	\$45.00
Universal Relay Option	\$215.00	\$137.60	N/A	N/A
InTouch Remote HID MiniProx Reader Option	\$525.00	\$336.00	\$42.00	\$52.50
InTouch Remote HID ProxPro Reader Option	\$525.00	\$336.00	\$42.00	\$52.50
Item Description	List Price	Final Price	HDW Annual Support (per Unit)	
Additional Options Available for Kronos InTouch H3 Slim Enclosure		36% Discount	Depot Repair	Depot Exchange
Kronos Touch ID Plus Biometric Option for InTouch H3	\$1,200.00	\$768.00	\$96.00	\$120.00
Kronos Touch ID Biometric Option for InTouch H3	\$1,200.00	\$768.00	\$96.00	\$150.00
Biometric Enrollment PreScan Pad for Touch ID Plus	\$15.00	\$9.60	N/A	N/A
InTouch Linear Imager Bar Code Scanner Option	\$735.00	\$470.40	\$58.80	\$73.50
Item Description	List Price	Final Price	HDW Annual Support (per Unit)	
Spare Parts - Kronos InTouch		36% Discount	N/A	N/A
InTouch H3 Replacement Front Cover Filler Plates	\$5.00	\$3.20	N/A	N/A
InTouch H3 Replacement Enclosure Back Cover - Standard	\$67.00	\$42.88	N/A	N/A
InTouch H3 Replacement Transformer/Battery Holder Plate -Standard Enclosure	\$6.00	\$3.84	N/A	N/A
InTouch Replacement Terminal Block Connector for Transition Board : 6-pin	\$19.00	\$12.16	N/A	N/A
InTouch Replacement Terminal Block Connector for Transition Board : 8-pin	\$20.00	\$12.80	N/A	N/A
InTouch H3 Replacement Enclosure Back Cover - Slim	\$67.00	\$42.88	N/A	N/A
InTouch Replacement Security Screw Removal Tool	\$4.00	\$2.56	N/A	N/A
InTouch Replacement Hardware Accessory Packet for Standard and Slim Enclosures	\$7.00	\$4.48	N/A	N/A
InTouch Replacement Internal Power Transformer for Standard Enclosure	\$130.00	\$83.20	N/A	N/A

Item Description	List Price	Final Price	HDW Annual Support (per Unit)	
InTouch Replacement NA 12" Power Cord for Mount Over AC Outlet - Standard Enclosure	\$12.00	\$7.68	N/A	N/A
InTouch Replacement NA 6' Power Cord for external AC Outlet - Standard Enclosure	\$12.00	\$7.68	N/A	N/A
InTouch Replacement North America Power Kit for external AC Outlet - Slim Enclosure	\$130.00	\$83.20	N/A	N/A
InTouch Replacement International Power Kit for external AC Outlet - Slim Enclosure	\$130.00	\$83.20	N/A	N/A
Cable, Morpho CBM-E2 Sensor to Main Bd (for Touch ID Plus)	\$17.00	\$10.88	N/A	N/A
Touch ID for InTouch H3 Adapter Kit	\$12.00	\$7.68	N/A	N/A

Item Description	List Price	Discount %	HDW Annual Support (per Unit)	
Rented Hardware <i>*Discount based on minimum rental of 50 Units</i>		*36% Discount	Depot Repair	Depot Exchange
Kronos InTouch 9000 H3, Standard, KR, B/C - per unit per month	\$150.00	\$96.00	N/A	Included
Kronos InTouch 9000 H3, Standard, Mag - per unit per month	\$150.00	\$96.00	N/A	Included
Kronos InTouch 9000 H3, Standard, HID Prox - per unit per month	\$160.00	\$102.40	N/A	Included
Kronos InTouch 9000 H3, Standard, EM4102 Prox - per unit per month	\$160.00	\$102.40	N/A	Included
Kronos InTouch 9000 H3, Standard, Smart Card - per unit per month	\$170.00	\$108.80	N/A	Included
Kronos InTouch 9000 H3, Slim, Mag - per unit per month	\$150.00	\$96.00	N/A	Included
Kronos InTouch 9000 H3, Slim, HID Prox - per unit per month	\$160.00	\$102.40	N/A	Included
Kronos InTouch 9000 H3, Slim, EM4102 Prox - per unit per month	\$160.00	\$102.40	N/A	Included
Kronos InTouch 9000 H3, Slim, Smart Card - per unit per month	\$160.00	\$102.40	N/A	Included
Touch ID Plus Option for H3 InTouch - per unit per month	\$50.00	\$32.00	N/A	Included
Touch ID Option for H3 InTouch - per unit per month	\$50.00	\$32.00	N/A	Included
Linear Images, InTouch - per unit per month	\$30.00	\$19.20	N/A	Included



Remote HID MiniProx Reader, InTouch - per unit per month	\$25.00	\$16.00	N/A	Included
Remote HID ProxPro Reader, InTouch - per unit per month	\$25.00	\$16.00	N/A	Included

Item Description	Pricing
Professional Services	
Professional Services (Cost per Hour) Blended Rate	\$200.00
Professional Services Billing Roles - Project Manager	\$200.00
Professional Services Billing Role - Application Consultant	\$200.00
Professional Services Billing Role - Technical Consultant	\$200.00
Professional Services Billing Role - Education Consultant	\$200.00
Professional Services Billing Role - Integration Consultant	\$200.00
Professional Services Billing Role - Solution Consultant	\$200.00
Professional Services Billing Role - Solution Developer	\$200.00

Item Description	Pricing
Training	
Training Points - per Point	\$1.00
Knowledge Pass 0-150ee	\$575.00
Knowledge Pass 151-299ee	\$1,050.00
Knowledge Pass 300-349ee	\$1,750.00
Knowledge Pass 350-399ee	\$2,050.00
Knowledge Pass 400-1500ee	\$2,325.00
Knowledge Pass 1501-2500ee	\$4,625.00
Knowledge Pass 2501-5000ee	\$8,675.00
Knowledge Pass 5001-20000ee	\$10,975.00
Knowledge Pass 20000+ee	\$22,000.00

Onsite Fixed-Fee Professional Services Bundle*	
*NOTE - Services Below are FIXED-FEE and Include Travel for (1) Kronos Resource	
2-Day Onsite Professional Services Engagement	\$5,610.00
3-Day Onsite Professional Services Engagement	\$7,904.00
5-Day Onsite Professional Services Engagement	\$12,614.00

A La Carte Fixed Fee Service Options	
TIMEKEEPER	
WF Timekeeper Additional Employee Group	4,000.00
WF Timekeeper Additional Assessment Group - Application Configuration Assessment	2,500.00
WF Timekeeper Additional Testing & Deployment Group	8,000.00
WIM Interface - Labor Level Import	2,500.00
WIM Interface - Basic Interface	2,500.00
WIM Interface - Complete Interface	CUSTOM \$

Item Description	Pricing
CMS-PBJ WIM Interface for Skilled Nursing Facilities (SNFs)	\$1,600.00
WF Timekeeper - Long Term Care: Patient Per Day (PPD)	\$2,500.00
WF Timekeeper - Long Term Care Key Factor	\$2,500.00
WF Timekeeper - Long Term Care CMS 671	\$2,500.00
WF Timekeeper - Onsite Assessment - per day	\$800.00



Single Sign On Authentication Requires a SAML 2.0 Compatible Customer Solution	\$2,400.00
ACCRUALS	
Workforce Absence Manager - Calculated Accruals Standard Configuration	\$1,000.00
ATTENDANCE	
Workforce Absence Manager - Attendance Program Planning	\$4,000.00
SCHEDULER	
Additional Scheduling Unit/Group Bundle	\$12,000.00
Employee Self Scheduling	\$2,400.00
Workload Generator Configurations (Required for Healthcare Customers)	\$4,000.00
Volume Import	\$1,000.00
Onsite Assessment (travel not included)	\$2,400.00
Auto-Scheduler // Schedule Generator / Priority Scheduling Engine	\$2,000.00
SCHEDULER EXTENSIONS	
EMR Integration	\$4,000.00
Onsite Assessment	\$2,400.00
Additional Extensions Unit/Group Bundle	\$6,000.00
ACTIVITIES	
Additional Phase Go Live Support	\$1,600.00
Add Cells	\$2,000.00
Add Resources and Reason Codes	\$2,000.00
ANALYTICS CORE	
Workforce Analytics, report development support session	\$4,000.00
Workforce Analytics, personalization, customer specific	\$3,600.00
ANALYTICS HEALTHCARE	
WAH, Configure skill/workgroup-based productivity	\$15,500.00
WAH, Productivity historical data add-on	\$1,600.00
WAH, Productivity add-on, MC-led, End-user training	\$800.00
WAH, Variance Improvement Planning add-on	\$27,900.00
WAH, Variance Improvement Planning add-on, MC-led, End-user training	\$800.00
WAH, Labor Cost Management add-on	\$35,000.00
WAH, Labor Cost Management add-on, MC-led, End-user training	\$800.00
WAH, Report development support session	\$4,000.00
WAH, Personalization dashboard	\$2,400.00
ANALYTICS PUBLIC SECTOR	

Item Description	Pricing
WFANPS, Report development support session	\$4,000.00
WFANPS, Personalization dashboard	\$2,400.00
ENHANCED REPORTING	
WF TK - Custom Hours by Labor Account	\$5,000.00
WF TK - Timecard Audit Trail	\$5,000.00
WF TK - Time Detail - Portrait	\$5,000.00
WF TK - Long Term Care Patient Per Day (PPD)	\$5,000.00
WF TK - Long Term Care Key Factor	\$5,000.00
WF TK - Long Term Care CMS 671	\$5,000.00
WF Accruals - Custom Accruals	\$5,000.00
WF Activities - Activity Audit	\$5,000.00



ATTACHMENT 3

ATTESTATION RE PERSONNEL USED IN CONTRACT PERFORMANCE

SUBJECT CONTRACT NUMBER:	
CONTRACTOR LEGAL ENTITY NAME:	Kronos Incorporated
EDISON VENDOR IDENTIFICATION NUMBER:	196888

The Contractor, identified above, does hereby attest, certify, warrant, and assure that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Contract.

CONTRACTOR SIGNATURE

NOTICE: This attestation MUST be signed by an individual empowered to contractually bind the Contractor. Attach evidence documenting the individual's authority to contractually bind the Contractor, unless the signatory is the Contractor's chief executive or president.

Alyce Moore, VP, General Counsel

PRINTED NAME AND TITLE OF SIGNATORY

November 2, 2016

DATE OF ATTESTATION



ATTACHMENT 4



Kronos Incorporated
297 Billerica Road
Chelmsford, MA 01824

phone +1 978 250 9600
fax +1 978 367 5900
url www.kronos.com

To Whom It May Concern

Re: Kronos Commitment Statement to Supplier Diversity

Kronos recognizes its obligation to give certified diversity business fair opportunities to solicit their goods and services in a fair and competitive manner and currently has 8% of its annual spend placed with business enterprises that are owned by minority, women, small business and service-disabled veterans.

Kronos has experienced the exceptional benefits of utilizing small business vendors in the past and is taking proactive measures to locate more of these providers for future needs. Although it is not always practical or feasible to establish a business relationship with every solicitor, Kronos is firmly committed to create the means by which business enterprises that are owned by minority, women, small business and service-disabled veterans may be given every consideration.

We confirm our commitment of maintaining diversity spend of 8% and growing that share as the opportunity to do so presents itself.

Regards,

Vince Devlin | Chief Procurement Officer | Kronos Incorporated
tel: +1 978 947 6774

Kronos | Time & Attendance • Scheduling • Absence Management • HR & Payroll • Hiring • Labor Analytics



ATTACHMENT 5

SERVICE LEVEL AGREEMENT (SLA)

Service Level Agreement: The Services, in a production environment and as described in the Statement of Work (aka Services Scope Statement), are provided with the service levels described in this Attachment 5. SLAs are only applicable to production environments. SLAs will be available upon Customer's signature of Kronos' Go Live Acceptance Form for Customer's production environment.

99.75% Application Availability

Actual Application Availability % = (Monthly Minutes (MM) minus Total Minutes Not Available (TM)) multiplied by 100 and divided by Monthly Minutes (MM), but not including Excluded Events

Service Credit Calculation: An Outage will be deemed to commence when the Applications are unavailable to State in Customer's production environment hosted by Kronos and end when Kronos has restored availability of the Services. Failure to meet the 99.75% Application Availability SLA, other than for reasons due to an Excluded Event, will entitle State to a credit as follows:

Actual Application Availability % (as measured in a calendar month)	Service Credit to be applied to Customer's monthly invoice for the affected month
<99.75% to 98.75%	10%
<98.75% to 98.25%	15%
<98.25% to 97.75%	25%
<97.75 to 96.75%	35%
<96.75	50%

"Outage" means the accumulated time, measured in minutes, during which State is unable to access the Applications for reasons other than an Excluded Event.

"Excluded Event" means any event that results in an Outage and is caused by (a) the acts or omissions of Customer, its employees, customers, contractors or agents; (b) the failure or malfunction of equipment, applications or systems not owned or controlled by Kronos, including without limitation State Content, failures or malfunctions resulting from circuits provided by Customer, any inconsistencies or changes in Customer's source environment, including either intentional or accidental connections or disconnections to the environment; (c) Force Majeure events; (d) scheduled or emergency maintenance, alteration or implementation provided during the Maintenance Period defined below; (e) any suspension of the Services in accordance with the terms of the Agreement to which this Attachment 4 is attached; (f) the unavailability of required State personnel, including as a result of failure to provide Kronos with accurate, current contact information; or (g) using an Application in a manner inconsistent with the product documentation for such Application.

"Maintenance Period" means scheduled maintenance periods established by Kronos to maintain and update the Services, when necessary. During these Maintenance Periods, the Services are available to Kronos to perform periodic maintenance services, which include vital software updates. Kronos will use its commercially reasonable efforts during the Maintenance Period to make the Services available to Customer; however, some changes will require downtime. Kronos will provide notice for planned downtime via an email notice to the primary State contact at least one day in advance of any known downtime so planning can be facilitated by Customer.



Currently scheduled Maintenance Periods for the Services are:

Monday through Friday 04:00 am – 06:00 am (U.S. eastern time)

Saturday and Sunday 12:00 am – 06:00 am (U.S. eastern time)

Maintenance Periods include those maintenance periods mutually agreed upon by State and Kronos.

“Monthly Minutes (MM)” means the total time, measured in minutes, of a calendar month commencing at 12:00 am of the first day of such calendar month and ending at 11:59 pm of the last day of such calendar month.

“Total Minutes Not Available (TM)” means the total number of minutes during the calendar month that the Services are unavailable as the result of an Outage.

Limitations: Service Credits will not be provided if: (a) State is in breach or default under the Agreement at the time the Outage occurred; or (b) the Outage results from an Excluded Event. If Kronos does not provide the appropriate Service Credit as due hereunder, State must request the Service Credit within sixty (60) calendar days of the conclusion of the month in which the Service Credit accrues. State waives any right to Service Credits not requested within this time period. All performance calculations and applicable Service Credits are based on Kronos records and data unless State can provide Kronos with clear and convincing evidence to the contrary.

The Service Level Agreements in this Exhibit, and the related Service Credits, apply on a per production environment basis. For the avoidance of doubt, Outages in one production environment may not be added to Outages in any other production environment for purposes of calculating Service Credits.

State acknowledges that Kronos manages its network traffic in part on the basis of Customer’s utilization of the Services and that changes in such utilization may impact Kronos’ ability to manage network traffic. Therefore, notwithstanding anything else to the contrary, if State significantly changes its utilization of the Services than what is contracted with Kronos and such change creates a material and adverse impact on the traffic balance of the Kronos network, as reasonably determined by Kronos, the parties agree to cooperate, in good faith, to resolve the issue.



ATTACHMENT 6

Kronos® Workforce Central & Workforce TeleStaff Cloud Guidelines – Single Tenant

The following guidelines and services apply to Workforce Central and Workforce Telestaff applications that are deployed in the Kronos Cloud:

Cloud Services

Environments:

Included.

One standard Production and one Non-Production (Development) environment.

Additional non-production environments are available for additional fees.

Environment restoration:

Included.

Services to restore Production environment to one Non-Production environment up to one time per week, if requested.

More frequent restores or additional environments will be subject to additional time and material fees.

Customer is responsible for requesting data to be moved from the Production environment to the Non-Production environment and for the contents of the data moved from the Production environment to the Non-Production environment.

Connectivity to Service:

Included

Customer's users connect to application via secure SSL/TLS connection over the internet. Cooperative efforts with customer IT staff may be required to enable access. Kronos will assist with validating site connectivity but assumes no responsibility for customer internet connection or ISP relationships. Kronos related Internet traffic cannot be filtered by proxy or caching devices on the client network. Exclusions must be added for the fully qualified domain names and public IP addresses assigned to the environments in the Kronos Cloud.

Device Initiated Terminal Connectivity:

Included

All terminals that are compatible with Device Initiated communication mode must use this mode of communication. With the Device Initiated mode of communication, the Kronos terminal initiates all communications with the Device Manager Server at the Kronos Cloud over the internet. In cases where Network Address Translation is required for terminals, the customer is responsible for applying the translations on their network. Kronos Cloud does not support terminals prior to Kronos 4500 series and does support certain models released thereafter. Please see product documentation support matrix for details.

Note: Server Initiated terminal communication, if permitted, requires a VPN and is not the preferred communication method when connecting terminals to the Kronos Cloud.

Remote Access to Non-Web Kronos Applications:

2 named users included



Cloud Services

Remote access to non-web Applications (e.g. Kronos Workforce Integration Manager) using a remote access tool such a Citrix® Receiver. Limited Kronos Applications require the use of these remote access accounts.

SFTP Accounts:

2 logins included

SFTP accounts are provided to customers to push files to the Kronos Cloud and to pull files from the Kronos Cloud for designated integration points (e.g. Kronos Workforce Integration Manager input/output folders). The Kronos SFTP folder location is not designed for long-term storage and files stored longer than 30 days may be deleted.

Operating System and Database Software Management:

Included

Includes the required O/S and [REDACTED] licenses, as well as services for Kronos to apply critical security patches, service packs and hot-fixes for the software running in Kronos Cloud.

Server Maintenance:

Included

All server maintenance, including repair and replacement of defective or failed hardware and the installation of hardware upgrades for the software running in Kronos Cloud.

Kronos Application Updates:

Included

Services to perform technical tasks required to apply application service packs, legislative updates (if applicable), point releases and version upgrades.

Backup:

Included

Customer data is backed up daily. Database backups are replicated via encrypted connections to a second Kronos Cloud datacenter. Backups are retained for the prior 28 days on a rotating basis. All historical employee and configuration data is stored in the rotating backups.

Security:

Included

For customers that choose datacenters in the United States of America:

Kronos maintains a hosting environment that undergoes examinations from an independent auditor in accordance with the American Institute of Certified Public Accounts SSAE 16 (i.e. SOC 1) and the AICPA Trust Services Principles Section 100a, Trust Services for Security, Availability, Processing Integrity, Confidentiality and Privacy (i.e. SOC 2). The Kronos Private Cloud (KPC) is evaluated for the principles of Security, Availability and Confidentiality by the independent auditor. The Kronos Private Cloud is located in data centers that undergo SSAE 16 examinations. Management access to the KPC is limited to authorized Kronos support staff and customer authorized integrations. The security architecture has been designed to control appropriate logical access to the KPC to meet the Trust Services Principles of Security, Availability and Confidentiality. The Applications provide the customer with the



Cloud Services

ability to configure application security and logical access per the customer's business processes.

In the event the customer identifies a security issue, the customer agrees to notify Kronos.

For security purposes customers are restricted from directly accessing the desktop, file systems, databases and operating system of the environments.

Customer agrees not to upload payment card information, as the service is not certified for PCI DSS.

Customer agrees not to upload health information that falls under the United States HIPAA law.

For customers that choose in datacenters outside the United States of America:

For any outsourced (subcontracted) infrastructure (e.g. co-location provider, public cloud provider) Kronos will provide Customer a copy of its subcontractor's AICPA SSAE 16 SOC 1 Type II and/or AT101 SOC 2 Type II reports, published and attested to by an independent third party auditing firm, if applicable. Kronos is not required to utilize any outsourced (subcontracted) infrastructure (e.g. co-location provider, public cloud provider) as part of this agreement to deliver services. If Kronos does not use outsourced (subcontracted) infrastructure (e.g. co-location provider, public cloud provider) customer will be entitled to receive a copy, if made available from Kronos at a future date, of a Kronos published AICPA SSAE 16 SOC 1 Type II and AT101 SOC 2 Type II reports published and attested to by an independent third party auditing firm, if made available.

The Kronos applications provide the customer with the ability to configure application security and logical access per the customer's business processes.

In the event the customer identifies a security issue, the customer agrees to notify Kronos.

For security purposes customers are restricted from directly accessing the desktop, file systems, databases and operating system of the environments.

Customer agrees not to upload payment card information as the service is not certified for PCI DSS.

Customer agrees not to upload health information that falls under the United States HIPAA law.



Cloud Services

Read-Only ODBC Access:

If selected on Section C.3

Kronos will provide customer with read-only ODBC access into customer's Production and Non-Production databases for Timekeeper/HRMS over secure connection (e.g. VPN). Customer is responsible for establishing this secure connection to the Kronos Cloud and for any additional fees for that connection that may apply. Kronos may, but is not obligated to, limit or block customer's database read-only ODBC queries in order to prevent failure of the database due to overload. Kronos will not pay SLA credits for any Outage that is the result of overloading the database during read-only ODBC access. Customer understands that overall performance may be reduced during peak processing periods, and customer may need to limit resource intensive read-only ODBC queries to off-peak periods. Customer acknowledges that read-only ODBC access over a long distance secure connection is not a reliable protocol, as it does not have built-in retry logic to handle connectivity issues. Kronos is not responsible for any changes that may be required to customer's internal systems due to read-only ODBC access.

Disaster Recovery Services:

Included

Basic Disaster Recovery services are provided to all hosted customers at no additional fee and include:

Customer environment and all customer data in the Kronos Cloud are replicated to a secondary Kronos Cloud data center. Disaster Recovery Services provide for a Recovery Point Objective (RPO) of 24 hours and Kronos strives to restore application availability in a commercially reasonable timeframe. The customer will be down until the Production environment is restored in the primary or secondary data center, if needed, as an application environment is not readily available at the alternate site to process data. Customers are expected to use fully qualified domain names (FQDNs) to access the service given that IP address of the service may change.

Any issues arising out of the disaster recovery event due to customer configuration/customization and/or customer third party software outside of the Kronos Cloud is the responsibility of the customer to resolve.

Disaster Recovery Services (fee-based):

If selected on Section C.3

Kronos offers enhanced Disaster Recovery services at an additional fee, as they provide for a secondary environment at a secondary Kronos datacenter to be used for customer recovery. With this offering the Customer environment and all customer data in the Kronos Cloud are replicated to a secondary Kronos Cloud datacenter. This service provides for a RPO (Recovery Point Objective) of 24 hours and a RTO (Recovery Time Objective) of 72 hours.



Cloud Services

In the unlikely event that Kronos declares a disaster in the primary datacenter, Kronos will notify the customer and activate the Disaster Recovery steps necessary to restore application availability within the RTO defined. As part of this enhanced service, Kronos will conduct an annual Disaster Recovery Process test, which has the objectives to 1) test backups 2) train Kronos employees 3) verify and improve internal Kronos procedures. The annual Disaster Recovery Process test may be live or simulated. Customers are expected to use fully qualified domain names (FQDNs) to access the service given that IP address of the service may change.

Any issues arising out of the disaster recovery event due to customer configuration/customization and/or customer third party software outside of the Kronos Cloud is the responsibility of the customer to resolve.

The following services are not included in this service, but they may be purchased from Kronos on a time and material basis, and are subject to additional fees: a customer specific DR plan with annual review.

*Note that Workforce Analytics, Workforce Record Manager, Enterprise Archive, Workforce TeleStaff, Workforce TeleTime IP and all non-Production environments are excluded from the RTO.

Temporary Environments:

If selected on Section C.3

Temporary Environments are designed for classroom training for no more than 40 people and/or functional application testing for approximately five to ten simultaneous users. Temporary environments are only available to those customers whose Production environment is hosted in the Kronos Cloud in a United States datacenter.

Third Parties:

If Customer uses 3rd party resources to configure/implement Kronos applications

If Customer uses a third party to configure and/or implement Customer's applications, the following applies:

The third party must be authorized by Kronos as part of the Kronos Connect Partner Program prior to accessing Customer's development and testing environments in the Kronos Cloud. Third parties will not be granted access to Customer's Production environment for purposes of configuring the applications. Customer understands that although Kronos Connect Partners are subject to Kronos policies and procedures, such Partners are not subject to SOC audits by Kronos or its representatives. As such, Kronos' SSAE16 SOC 1 and AT101 SOC 2 reports are applicable to the Production environment only and are not applicable to third parties' activities.

Applicable to customers that choose datacenters in the United States of America only.



Cloud Services

Encryption at rest of Customer Content at storage level Included

For each of the customer's production and non-production environments in a data center in the United States of America, Customer Content will be encrypted at rest at the storage level. Encryption at rest is defined as Customer Content is made unreadable on disk via encryption technology when the Kronos Cloud computing environment hardware is powered off.

Guidelines and Assumptions:

Category	Assumption
	Estimated availability of production server hardware is approximately 30 days after the Contract is processed.
	Customer agrees to receive automatic updates to the applications.
	Use of the Workforce Central translation toolkit requires a Kronos Professional Services engagement to import/export the translation file(s) into a test environment and into the Production environment.
	Connecting modem clocks to the Kronos Cloud is not supported.
	Applications will support English only unless stated on the Attachment 7 and Section C.3.
	Customer agrees not to conduct security testing, which includes, but is not limited to penetration testing and vulnerability scanning.
	Customer agrees not to conduct any sort of automated or manual performance testing of the Service.
	Offering includes system resources to process the equivalent of five WIM interfaces using up to 10 links with a maximum of five megabytes of data per link. In addition, systems resources for the integration between Workforce Central and Workforce TeleStaff for People, Punch, and Accrual interfaces are included assuming product documentation is followed for setup and runtime scheduling. Additional processing requirements may incur additional fees associated with corresponding system resources. Custom developed functionality outside of WIM that runs in the Kronos Cloud may incur additional fees.
	Retention policies must be configured in the application(s). Setting retention policies will ensure that unnecessary system data (e.g. temp files, deleted records, empty rows, etc.) is routinely purged from the system and will help in managing database growth. Retention policies do not apply to configuration and/or historical data. Historical employee data can be maintained for the duration of the agreement and renewal periods, per customer business requirements.
	Sizing considerations are based on a three year growth projection of the Production database environment. After three years, an archiving strategy may be reviewed with the customer for Service performance.
	Custom reports for Workforce Central are created using Microsoft Visual Studio. HR/Payroll reports are created using Crystal Reports. If made available from the vendors, the free versions of these tools will be made available to the customer in their development environment. Customer will have read-only ODBC access to their development database for modifying and/or creating reports. Customer is limited to two named users for report creation, as access requires the use of one of the two included user licenses for remote access to non-web applications (e.g. Citrix Receiver). Note that Customer created reports for Workforce HR and Payroll may have reduced functionality from Kronos product documentation due to security restrictions in Kronos Cloud.



Category	Assumption
	Customer will be required to sign a go live milestone document confirming customer has completed their testing and is ready to go live with the Workforce Central application(s) and/or TeleStaff.

Product Specific Considerations

Workforce Record Manager/ Kronos Enterprise Archive (if included on order form):

If Workforce Record Manager or Kronos Enterprise Archive is included, note that Setup Data Manager will only support import and export of configurations via XML file transfers between Production and Non-Production environments, as a direct connection between Production and Non-Production environments is not provided.

If an environment is available for the use of archiving functionality, compared to the used of just Setup Data Manager, this additional environment for archiving will be noted on the order form if it is included.

Workforce TeleTime IP:

Customer is responsible for procuring the phone lines (SIP trunks) required for their Workforce TeleTime IP system. Customer should work with their ISP/telco provider to procure a private circuit (specifically MPLS) with adequate bandwidth to support the number of SIP trunks (phone lines) needed for their use case, SIP calls per second required, along with a router and cross-connects to terminate the circuit in the Kronos Cloud. Kronos will provide detailed information to Customer on Kronos Cloud connectivity requirements. Cross-connects can be also purchased directly from Kronos, and would be indicated on order form if included.

This offering is only available to customers who chose Kronos datacenters in the United States.

Upgrade Services

The Service includes services for Kronos to execute tasks to apply point releases and version upgrades to customer’s Kronos Applications in the Kronos Cloud. Services are limited to those tasks which apply these updates to the Applications.

The table below reflects the included upgrade tasks.

Project Coordination:	Included
Project Manager to coordinate the upgrade project.	
Up to eight 30-minute weekly status calls (one per week)	
Coordinate Kronos resources	
Send meeting invites	
Provide Project Timeline and expected customer commitment at the start of the project	
Provide initial Project Schedule and communicates progress during weekly status calls	
Provide Communication Plan and Contact List	
Planning Phase	
Customer/ Kronos Introduction Call – up to one hour	Included
Technical readiness & architecture review – Kronos Cloud Environment	Included
Assessment Phase	
Assessment of WIM interfaces to be upgraded	Included



Assessment of new features or changes to configurations	Not included
Assessment of customs and custom reports and development activities related thereto	Not included
Solution Upgrade / Build Phase	
One (1) restore of Production database to NON-Production environment for the purpose of upgrade testing. Additional restores, if requested, shall be subject to additional time and material fees.	Included
Upgrade Non-Production and Production environments to new point release or version.	Included
Upgrade of Workforce Integration Manager (WIM) interfaces due to product changes introduced as part of the technical upgrade, as defined in product documentation. For Workforce Central this includes XML export/imports and database views as defined in the "Workforce Central Import User Guide" and "Workforce Central Data View Reference Guide".	Included
Upgrade of non-WIM interfaces in Non-Production environment and Production environment.	Not Included
Upgrade of customs and custom reports. This includes upgrade of Workforce Integration Manager (WIM) interfaces that use table import batch functionality, read/write directly to database tables or require changes due to new/changed customer requirements.	Not Included
Upgrade of interfaces and reports created or provided by customer	Included
Update of terminal firmware managed by Kronos	Not Included
Configuration of new features or functionality or changes to existing configuration	Available for Purchase
Test & Certify Phase	
System test upgraded environments by verifying a user can log in	Included
User acceptance testing (UAT) of upgraded environments, interfaces, custom reports, new features, etc.	Not Included
Develop customer-specific test cases	Included
Sign-off on upgraded Non-Production and Production Environments	Not Included
Sign-off on upgraded Non-Production and Production Environments	Customer
Deploy & Support Phase	
Deployment Readiness Call – up to one hour	Included

Note that new feature configuration, project management services, other Professional, Managed and Educational Services and training are not included as part of Upgrade Services, but may be purchased independently, if desired.

Project coordination lasts for no more than eight weeks. At the end of this time, Kronos will complete the production upgrade. If for any reason Kronos cannot complete the technical upgrade steps within eight weeks due to a Kronos caused delay, project coordination will continue proportionally to cover the Kronos caused delay. For example if Kronos causes a two week delay due to Kronos resource unavailability, project coordination will last no more than 10 weeks.

If not specifically noted, the customer should assume responsibility of the task and/or deliverable.

Rev 2016-04-04



Attachment 7 Statement of Work

Description of the Implementation Services

The following table represents the set up services that are included in Implementation Services.

Workforce Central	
Project Support	Weekly status calls or report Project workbook updates (including schedule maintenance and budget report)
Technical Architecture Assessment	2 environments (1 PROD, 1 DEV)
Database	
Onsite visits	4 onsite visits are included. A visit is a single resource onsite at the customer location for up to 4 consecutive business days.
Training Points	51,750 training points are included
Transition Customer to KGS	1 transition phase
Workforce Timekeeper	
Application Configuration Assessment	4 Assessment Groups
Interface Design Assessment	Up to 3 Timekeeper
Application Install	2 environments (1 PROD, 1 DEV)
Data Collection Standard + Features (Touch ID)	Configure up to 5 terminals with Touch ID, Client completes the rest.
Data Collection Features (Workforce Employee)	Global Setting configuration in PROD and DEV environments.
Workforce Timekeeper Standard Configuration	5 Employee Groups (Profiles) *An employee group is defined as a set of employees that share the same pay statuses, including, but not limited to, Overtime Rules, Holidays, Shift Differentials, Accrual Profiles and Pay Periods.
Workforce Timekeeper Standard Integration	1 Standard person import interface 1 Standard payroll export interface 1 Standard accruals import interface
Single Sign on Authentication	Requires a SAML 2.0 compatible customer solution
Standard Testing Guidance and Support	1 testing cycle – including unit testing, system and integration testing and user acceptance testing.
Deployment Planning and Go-live support	2 deployment date 2 deployment group 2 application deployment 2 go-live date 2 application or technical resource
Workforce Scheduler Extensions for Healthcare	
Application Configuration Assessment	1 Assessment Group



Product Design Workshop	A single assessment activity for up to 5 Groups/Units Create Workforce Scheduler Extensions Design Specification
Application Install	2 environments (1 PROD, 1 DEV)
Workforce Scheduler Extensions Standard Configuration	Standard system configuration Minimal requirements from the customer (i.e. budgets) Set up capture of historical volume-based census by shift and day of week for future schedule planning
Integration	ADT and WFC (volumes)
Additional Items	<ul style="list-style-type: none"> • Employee Self Scheduler • Workload Generator Configuration • Volume Import • Auto-Scheduler • Schedule Generator • Priority Scheduling Engine
Standard Testing Guidance and Support	1 testing cycle
Deployment Planning and Go-live support	Centralized deployment to include up to 5 Units/Groups Workforce Forecast Manager use to begin following sampling collection period 1 go-live date 1 Kronos application resource
Workforce Attendance – Leave	
Application Configuration Assessment	1 Assessment Group
Interface Design Assessment	Up to 1 Leave
Application Install	2 environments (1 PROD, 1 DEV)
Workforce Absence Manager Leave Standard Configuration	State and FMLA
Workforce Absence Manager Leave Historical Data Imports	1 data load
Standard Testing Guidance and Support	1 testing cycle
Deployment Planning and Go-live support	1 deployment date 1 deployment group 1 application deployment 1 go-live date 1 application or technical resource
Workforce Attendance – Attendance	
Application Configuration Assessment	1 Assessment Group
Interface Design Assessment	Up to 1 Attendance
Application Install	2 environments (1 PROD, 1 DEV)
Workforce Absence Manager Attendance	Unlimited



Standard Configuration	
Workforce Absence Manager Attendance Balance Data Imports	1 data load
Standard Testing Guidance and Support	1 testing cycle
Deployment Planning and Go-live support	1 deployment date 1 deployment group 1 application deployment 1 go-live date 1 application or technical resource
Workforce Attendance – Accruals	
Application Configuration Assessment	1 Assessment Group
Interface Design Assessment	Up to 1 Accruals
Application Install	2 environments (1 PROD, 1 DEV)
Workforce Absence Manager Calculated Accruals Standard Configuration	Up to 10 calculated accrual policy
Workforce Absence Manager Accrual Balance Data Imports	1 data load
Standard Testing Guidance and Support	1 testing cycle
Deployment Planning and Go-live support	1 deployment date 1 deployment group 1 application deployment 1 go-live date 1 application or technical resource
Workforce KSS Attestation Tool Kit	
Attestation Installation & Configuration	Kronos will install, configure, and test the Attestation Tool Kit in the customer’s environment. This includes: <ul style="list-style-type: none"> • Survey the customer and gather their specific Attestation Tool Kit Requirements. • Provide a Software Tool Design document. • Provide and install the Attestation Tool Kit components. • Configure the installation and a sample employee and test configuration. • Configure the installation of sample Kronos terminals if Kronos terminal Smart Views are requested. • Provide user configuration and maintenance training for the Tool
Deployment Planning and Go-live support	1 deployment group 1 application server deployment 1 go-live date 1 application or technical resource
Workforce Analytics	
Application Configuration Assessment	1 assessment group
Application Install	2 environments (1 PROD, 1 TEST)



Workforce Analytics Core Standard Configuration	Up to 200 WTK Pay Codes Up to two (2) analytics servers 1 currency 1 language 1 standard installation WFAN ETL, WFAN Metadata, WFAN Ad hoc reporting templates, 1 standard installation WFAN dashboard and reports, 1 Initial data load of 1 year of historical WTK data loaded 1 8-hour System Administrator mentoring session for up to 2 participants (analytics system training session)
Workforce Analytics Core Standard Integration	1 standard WTK ETL import interface
Standard Testing Guidance and Support	1 testing cycle
Deployment Planning and Go-live support	1 deployment date 1 deployment group 1 application deployment 1 go-live date 1 application or technical resource



ATTACHMENT 8

SUPPORT POLICIES

Product Coverage

For Customer SaaS installation, Customers must purchase the same [software support service](#) type for all software and equipment support services for all equipment of the same type.. The latest Supported Product List is available at <http://customer.kronos.com/support/status/index.htm>. Equipment support is not included.

Workforce Central suite

Kronos only provides service packs for the current release and the two immediately prior releases of the Application(s). We currently publish new releases approximately every twelve to eighteen months. Resolution of an issue may require that you upgrade to the current release of the Application(s).

Workforce Analytics (WFAN) – supported product components include:

All procedures and Database Objects associated with the Workforce Analytics databases.

All WFAN for Healthcare Reports accessible through the “WFAN Advanced Reporting” link from the SharePoint Home Page that were delivered through the Core Product.

All Analysis Services Cubes found in the Workforce Analytics databases.

Kronos defines Version, Release, and Service Pack as follows:

Version: A software product upgrade that includes major new features or functionality.

Release: A software product upgrade that includes minor new features or functionality.

Service Pack: One or more defect repairs bundled into a single update. Service packs are cumulative — Service Pack N will, at minimum, include all of the changes delivered in Service Pack N-1.

The software product hierarchy is: Version . Release . Service Pack

Support Exclusions

1. Customer's improper use, management or supervision of the Application(s) or other failure to use the Application in accordance with Kronos' specifications; or
2. Customer's repair, attempted repair or modification of the Application without prior authorization from Kronos; or
3. Customer's use of the Application for purposes other than those for which they are designed or the use of accessories or supplies not approved by Kronos; or
4. Customer's computer or operating system malfunctions; or
5. Services required for application programs and/or conversions from products or software not supplied by Kronos; or
6. Reprogramming, including reconfiguration of the Application(s) by Customer.

In addition to the Support exclusions section above the following Services are NOT covered by your Kronos Support Service Agreement and are subject to the applicable Kronos Service rates.

1. Configuration Changes, Reprogramming, New Programming such as, but not limited to, Work Rules, Pay Rules, Accrual Rules, Profiles, Dashboards and Fields
2. Creating New Schedules
3. Terminal Programming and Cold Start
4. Pay Period Changes
5. Programming, modifying, implementing, training or troubleshooting the following:
 - a. Data integration interfaces (i.e. Connect, Integration Manager, Analytics)



- b. Custom Reports
- c. Custom Application extensions
6. Editing Process Manager templates and creating new templates
7. Installing or reinstalling Applications such as, but not limited to,
 - a. Adding a Workstation
 - b. Moving the Application
8. Writing or customizing database scripts for data reporting and/or retrieval
9. Custom Reports or Custom Application Extensions
10. Service to Kronos custom software is not provided, unless otherwise specified on the applicable Order Form for such custom software.
11. Importing new data i.e. from acquisitions or purchasing of another company.

Service Coverage Period

Platinum Level

24 hours a day, seven days a week, 365 days a year, with access to Kronos' technical support staff

Priority Based Support and Kronos Support Response Time are set forth in section A.4

Critical Outages

Kronos Support will provide continuous effort on all high priority events through either bug identification, the development of a workaround or problem resolution. If this effort goes beyond normal hours, the case may be passed to the after hours team or to the mission critical support engineer on duty. *On-going continuous effort may also be dependent on the customer's ability to provide a resource to work with the Kronos Support engineer during this period. Support outside the scope of the services agreement is billable.*

Technical Escalation

Our case resolution process is a Team based approach structured around specific products of the Application suite and staffed by Support Engineers covering the full spectrum of skill sets and technical expertise. The Teams are empowered to dynamically apply the appropriate resources to a case based on severity and complexity to ensure the fastest resolution time possible.

The Teams are also integrated with the Development Engineering staff and engage their assistance and technical guidance when necessary and/or directly escalate depending on case severity and time to resolve considerations.

For situations that contain multiple cases an Account Manager may be assigned to act as a single point of contact and communication regarding case resolution status, action plan development, resource integration and implementation coordination. The Account Manager remains engaged until the situation has been successfully remediated.

Management Escalation

Customers may, at any time, ask to speak to a Kronos manager if they experience dissatisfaction with the level of service received with respect to a specific case or service in general. To contact a Kronos Global Support manager, please telephone your Kronos Support Services center and ask to speak to a manager. Phone numbers are listed on the Customer Portal at <http://customer.kronos.com/ContactUs.htm>.

Software Support Services and Features



Kronos provides different levels of support offerings through our Platinum *Plus*, Platinum, Gold *Plus*, and Gold support services.

Platinum Plus Support Service (If selected by Customer on the Contract)

Platinum Plus Support customers have access to the same features as the Platinum Support customers and access to the Technical Account Manager (TAM). The TAM is a seasoned service professional that will draw upon a vast knowledge of Kronos products and services to provide you with proactive, consultative expertise. For Platinum Plus customers, a TAM is available *24 hours per day, 7 days per week*. Platinum Plus customers can designate *5 named contacts*, and also enjoy one on-site visit per year.

Platinum Support Service*

Platinum Support customers have access to the same service features as Gold Support customers and the following additional entitlements:

- 24 x 7 x 365 telephone access to Kronos Global Support

- Access to Senior Support Engineers

- Response time of 1 hour or less for High, 4 hours or less for Medium, and 1 business day or less for Low Priority calls.

Platinum Support customers also have the option of upgrading to Platinum Plus.

*All Workforce Central SaaS Customers have platinum support service included.

All customers receive the following as part of support.

SuperSearch (Available to all Support Agreement customers)

The Search engine searches the following data sources* and includes Basic and Advanced filters to search by product.

- Knowledge base

- Documentation (Manuals and User Guides)

- Service packs

- Customer forums

- Technical Advisories and Technical Insiders

- Frequently asked questions (FAQs)

*Access to data sources is limited by type of support service.

Technical Advisories (Available to all Support Agreement customers)

Kronos Global Support Center personnel are a valuable source of knowledge and experience. That's why we give you access to the same vast repositories of information that they use. You have access to these technical alerts located on the Kronos customer portal. *Please sign up for email alerts to get notified of the release of new technical advisories on the Kronos customer portal.*

Service Case Studies (Available to Gold and Platinum level customers)

When you want an in-depth understanding of technology and how Kronos applications incorporate that technology, you'll enjoy reading and learning from these case studies.

Learning Quick Tips (Available to Gold and Platinum level customers)

Enjoy the convenience of web-based, self-paced recorded training modules for your Kronos application. These training recordings are short in duration and you can take them anytime and anywhere that you have access to the Web.



Technical Insider (Available to Gold and Platinum level customers)

Learn from the experts here at Kronos and become an expert yourself. The Technical Insider offers best practices, procedures, and tools and is available through our customer portal.

Brown Bag Sessions (Available to Gold and Platinum level customers)

Experience training over the Internet on a variety of topics pertaining to your Kronos system. Kronos Global Support offers these Brown Bag workshops in a structured online format without costly travel or interruption to your busy schedule. These sessions are one hour in length and are FREE for all Kronos customers with Gold or Platinum support agreements.

HR and Payroll Answerforce (Available to Gold and Platinum level customers)

HR and Payroll Answerforce enables you to facilitate communication between employees, managers and HR professionals. It provides managers and employees with current HR information they need to make effective decisions. Experience an award-winning user interface which delivers up-to-date human resources, employee benefits, compensation, employment and regulatory information directly to your desktop.

SHRM e-Learning (Available to Gold and Platinum level customers)

SHRM e-Learning is an online educational environment that delivers just-in-time training to HR professionals through a series of HR-related mini-courses. Browse the courses in the SHRM e-learning catalog <http://www.shrm.org/elearning/> to create a learning journey that is unique to you. SHRM e-Learning courses are facilitated by leading industry experts and presentations range from sixty to ninety minutes in length.

Interactive Forms (Available to Platinum level customers)

Instant access to a comprehensive and easy-to-use library of HR and Employment & Payroll Tax forms and instructions. You can access, fill out, save, print, and maintain over 730 HR forms and 2500 Payroll forms.

Service Packs (Available to all Support Agreement customers)

Kronos Support Services entitles all customers who purchase a support agreement or SaaS, to the latest available product version upgrades, updates and enhancements, and documentation released during the agreement period, available on CD or downloadable from the Kronos customer portal. Protecting your investment is where our coverage for you begins as you embark on your journey to increased knowledge and improved business performance.

This service feature entitles you to the latest available product releases, updates/patches. For many products, the latest support releases (service packs) or legislative updates are posted on the customer portal for you to download and install. *Please sign up for email alerts to get notified of the release of new service packs on the Kronos customer portal.*

Knowledge Base (Available to all Support Agreement customers)

Accessed by our customers thousands of times per month, this online database currently contains thousands of answers to questions about Kronos products. Type in a question and the knowledge base suggests a solution. It is tightly integrated with our Global Support case management system and captures the real-world experience of our support engineers. The knowledge base is constantly updated. When our support engineers encounter and resolve new situations, they can automatically submit new solutions to the knowledge base.

Frequently Asked Questions (Available to all Support Services customers)

Conveniently organized and continuously populated from the knowledge base, FAQs truly represent those issues that customers ask about most. Before querying the knowledge base, try the FAQs to find your answers or get ahead of issues you may not be aware of.



eCase management (Available to all Support Agreement customers)

For your convenience, we give you direct access to our electronic case management system. Make your own notes to help explain what you are encountering. Your case is formally assigned a number and subject to all the normal tracking and routing mechanisms. Cases are reviewed Monday–Friday, during the business hours of your Kronos support center, excluding Kronos holidays. Should you require assistance outside the described hours, please telephone your Kronos support center.

Documentation (Available to all Support Agreement customers)

Online access to documentation for most of Kronos' products, for example:

- Installation guides
- Configuration guides
- Database administrators guides
- User guides
- System administrators guides
- Database views reference guides.

Customer Forums (Available to all Support Agreement customers)

Our Customer forums provide a unique opportunity to connect with other Kronos customers and to benefit from their real-world experiences. Organized by product platform and using threaded messaging, the Forums allow you to post questions to other forum visitors — or provide advice to someone else's query. A chance to go beyond simple product "how to," many customers have commented on how the forums have helped them gain a broader understanding of how to leverage their Kronos applications.

Remote Support (Available to all Support Agreement customers)

A web-based screen-sharing application that enables Kronos to support you by empowering our support representatives to remotely view your computer. By connecting through the Internet or via intranets and extranets, support representatives will work in real time with your users and quickly escalate to desktop sharing, which features mutual mouse and keyboard control and whiteboard capability.

Equipment / Hardware Support Services

Depot Exchange Service

The premium hardware service option: Kronos sends a replacement unit on an advance exchange basis by next-business day delivery if request is received prior to 2:00 p.m. Kronos recommends that Depot Exchange customers procure the appropriate number of spare units to maintain adequate coverage while a unit is out of service.

How it works:

You contact Kronos to troubleshoot the problem. If unable to resolve the issue, you are issued a Return Material Authorization (RMA) Case number to return the unit to Kronos for repair.

You install your spare unit from your inventory.

Kronos sends a replacement unit on an advance exchange basis by next-business day delivery if request is received prior to 2:00 p.m.

Upon receipt of replacement, you send the terminal needing service back to the Kronos Equipment Services Center.

Availability:

Currently ONLY available in Australia, Canada, China, Mexico, New Zealand, and United States.

**Conditions:**

Batching (defined as 2 or more terminals) voids the turn-around time.

You will be charged Kronos' current time and materials rate for the installation (professional services) of any software or firmware upgrades, if available, and if requested.

Equipment Support Services do NOT include the replacement of "consumables." In addition, Depot Support Services do NOT include the repair of damages, and Customer will not attempt to return damaged Product, resulting from:

- a. Any cause external to the Products including, but not limited to, electrical work, fire, flood, water, wind, lightning, transportation, or any act of God;
- b. Customer's failure to continually provide a suitable installation environment (as indicated in Kronos' published installation guidelines) including, but not limited to, adequate electrical power;
- c. Customer's improper use, relocation, packaging, refinishing, management or supervision of the Product(s) or other failure to use Products in accordance with Kronos' published specifications;
- d. Customer's use of the Products for purposes other than those for which they are designed or the use of accessories or supplies not approved by Kronos;
- e. Government imposed sanctions, rules, regulations or laws preventing the shipment of the Products; or
- f. Customer's repair, attempted repair or modification of the Products.

Terminals are warranted for 90 days from date of shipment.

This service includes access to equipment service packs / firmware updates available on the Kronos customer portal. Please sign up for email alerts to get notified of the release of new service packs on the Kronos customer portal.

Depot Repair Service

This service was designed for those who keep their own inventory of spare terminals and options.

How it works:

You contact Kronos to troubleshoot the problem. If unable to resolve the issue, you are issued a Return Material Authorization (RMA) Case number to return the unit to Kronos for repair.

You install your spare unit from your inventory.

You send the terminal needing service back to the Kronos Equipment Services Center.

Upon receipt of product, Kronos shall repair the product within ten (10) business days and return to you by regular surface transportation.

Availability:

NOT available from the Australia and China Support Services groups.

Conditions:

Batching (defined as 2 or more terminals) voids the turn-around time.

You will be charged Kronos' current time and materials rate for the installation (professional services) of any software or firmware upgrades, if available, and if requested.

Equipment Support Services do NOT include the replacement of "consumables." In addition, Depot Support Services do NOT include the repair of damages, and Customer will not attempt to return damaged Product, resulting from:

- a. Any cause external to the Products including, but not limited to, electrical work, fire, flood, water, wind, lightning, transportation, or any act of God;



- b. Customer's failure to continually provide a suitable installation environment (as indicated in Kronos' published installation guidelines) including, but not limited to, adequate electrical power;
- c. Customer's improper use, relocation, packaging, refinishing, management or supervision of the Product(s) or other failure to use Products in accordance with Kronos' published specifications;
- d. Customer's use of the Products for purposes other than those for which they are designed or the use of accessories or supplies not approved by Kronos;
- e. Government imposed sanctions, rules, regulations or laws preventing the shipment of the Products; or
- f. Customer's repair, attempted repair or modification of the Products.

Repairs are warranted for 90 days from date of shipment.

This service includes access to equipment service packs / firmware updates available on the Kronos customer portal. Please sign up for email alerts to get notified of the release of new service packs on the Kronos customer portal.

Device Software Maintenance

Device Software Maintenance is designed for those Kronos customers who choose to manage time clock repair themselves and just want access to device software updates. This service option lets you download equipment service packs from the Customer Portal to ensure that your time clock is always up to date with:

- The latest security enhancements
- Communication protocols
- Fixes and terminal software feature updates
- Compatibility updates with Kronos software or other terminals

Device Software Maintenance is included with Depot Exchange and Depot Repair.

Device Software Maintenance does NOT include any repair or exchange services.

How it works:

Go to the Customer portal at <http://customer.kronos.com>.

Register or log in to the Customer Portal. An email address and Kronos Solution ID are required to register for access to the customer portal.

Go to the Support page to access the equipment service packs.

Availability:

The Device Software Maintenance offering is available worldwide.

NOT available for the 100, 400, 500, Century and Cyber series terminals

This service includes access to equipment service packs / firmware updates available on the Kronos customer portal. Please sign up for email alerts to get notified of the release of new service packs on the Kronos customer portal.

Per-event Repair Service

Per-event rates apply to customers without an equipment support agreement. The Kronos Equipment Services center will attempt to repair any repairable defective item within 15 business days after receipt at the current Per-event pricing. The product will be returned by regular surface transportation.

How it works:

You contact Kronos to get a Return Material Authorization (RMA) Case number to return the unit to Kronos for repair.



You install your spare unit from your inventory

You send the terminal needing service back to the Kronos Equipment Services Center.

Upon receipt of product, Kronos shall repair the product within fifteen (15) business days and return to the customer by regular surface transportation.

Conditions:

Batching (defined as 2 or more terminals) voids the turn-around time.

You will be charged Kronos' current time and materials rate for the installation (professional services) of any software or firmware upgrades, if available, and if requested.

Equipment Support Services do NOT include the replacement of "consumables." In addition, Depot Support Services do NOT include the repair of damages, and Customer will not attempt to return damaged Product, resulting from:

- a. Any cause external to the Products including, but not limited to, electrical work, fire, flood, water, wind, lightning, transportation, or any act of God;
- b. Customer's failure to continually provide a suitable installation environment (as indicated in Kronos' published installation guidelines) including, but not limited to, adequate electrical power;
- c. Customer's improper use, relocation, packaging, refinishing, management or supervision of the Product(s) or other failure to use Products in accordance with Kronos' published specifications;
- d. Customer's use of the Products for purposes other than those for which they are designed or the use of accessories or supplies not approved by Kronos;
- e. Government imposed sanctions, rules, regulations or laws preventing the shipment of the Products; or
- f. Customer's repair, attempted repair or modification of the Products.

Repairs are warranted for 90 days from date of shipment.

*This service does **NOT** include access to equipment service packs / firmware updates.*



ATTACHMENT 9

JBOSS

Contractor represents and warrants to the State that it possesses all license agreements and use rights required for the State to have full functionality and use of the Application and that the State shall not be bound by the terms and conditions which are inconsistent with the terms of the Contract, including any obligation of the State to indemnify and applicable laws..

END USER LICENSE AGREEMENT
JBoss © ENTERPRISE MIDDLEWARE

PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY BEFORE USING SOFTWARE FROM RED HAT. BY USING RED HAT SOFTWARE, YOU SIGNIFY YOUR ASSENT TO AND ACCEPTANCE OF THIS END USER LICENSE AGREEMENT AND ACKNOWLEDGE YOU HAVE READ AND UNDERSTAND THE TERMS. AN INDIVIDUAL ACTING ON BEHALF OF AN ENTITY REPRESENTS THAT HE OR SHE HAS THE AUTHORITY TO ENTER INTO THIS END USER LICENSE AGREEMENT ON BEHALF OF THAT ENTITY. IF YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT, THEN YOU MUST NOT USE THE RED HAT SOFTWARE. THIS END USER LICENSE AGREEMENT DOES NOT PROVIDE ANY RIGHTS TO RED HAT SERVICES SUCH AS SOFTWARE MAINTENANCE, UPGRADES OR SUPPORT. PLEASE REVIEW YOUR SERVICE OR SUBSCRIPTION AGREEMENT(S) THAT YOU MAY HAVE WITH RED HAT OR OTHER AUTHORIZED RED HAT SERVICE PROVIDERS REGARDING SERVICES AND ASSOCIATED PAYMENTS.

This end user license agreement ("EULA") governs the use of the JBoss Enterprise Middleware and any related updates, source code, appearance, structure and organization (the "Programs"), regardless of the delivery mechanism.

1. License Grant. Subject to the following terms, Red Hat, Inc. ("Red Hat") grants to you a perpetual, worldwide license to the Programs (each of which may include multiple software components) pursuant to the GNU Lesser General Public License v. 2.1. With the exception of certain image files identified in Section 2 below, each software component is governed by a license that permits you to run, copy, modify, and redistribute (subject to certain obligations in some cases) the software component. This EULA pertains solely to the Programs and does not limit your rights under, or grant you rights that supersede, the license terms applicable to any particular component.

2. Intellectual Property Rights. The Programs and each of their components are owned by Red Hat and other licensors and are protected under copyright law and under other laws as applicable. Title to the Programs and any component, or to any copy, modification, or merged portion shall remain with Red Hat and other licensors, subject to the applicable license. The "JBoss" trademark, "Red Hat" trademark, the individual Program trademarks, and the "Shadowman" logo are registered trademarks of Red Hat and its affiliates in the U.S. and other countries. This EULA does not permit you to distribute the Programs using Red Hat's trademarks, regardless of whether they have been modified. You may make a commercial redistribution of the Programs only if (a) permitted under a separate written agreement with Red Hat authorizing such commercial redistribution or (b) you remove and replaced all occurrences of Red Hat trademarks and logos. Modifications to the software may corrupt the Programs. You should read the information found at <http://www.redhat.com/about/corporate/trademark/> before distributing a copy of the Programs.

3. Limited Warranty. Except as specifically stated in this Section 3, a separate agreement with Red Hat, or a license for a particular component, to the maximum extent permitted under applicable law, the Programs and the components are provided and licensed "as is" without warranty of any kind, expressed or implied, including the implied warranties of merchantability, non-infringement or fitness for a particular purpose. Red Hat warrants that the media on which the Programs and the components are provided will be free from defects in materials and manufacture under normal use for a period of 30 days from the date of delivery to you. Neither Red Hat nor its affiliates warrant that the functions contained in the Programs will meet your requirements or that the operation of the Programs will be entirely error free, appear or perform precisely as described in the accompanying documentation, or comply with regulatory requirements. This warranty extends only to the party that purchases subscription services for the Programs from Red Hat and/or its affiliates or a Red Hat authorized distributor.

4. Limitation of Remedies and Liability. To the maximum extent permitted by applicable law, your exclusive remedy under this EULA is to return any defective media within 30 days of delivery along with a copy of your payment receipt and Red Hat, at its option, will replace it or refund the money you paid for the media. To the maximum extent permitted under applicable law, under no circumstances will Red Hat, its affiliates, any Red Hat authorized distributor, or the licensor of any component provided to you under this EULA be liable to you for any incidental or consequential damages, including lost profits or lost savings arising out of the use or inability to use the Programs or any component, even if Red Hat, its affiliates, an authorized distributor, and/or licensor has been advised of the possibility of such damages. In no event shall Red Hat's or its affiliates' liability, an authorized distributor's liability or the liability of the licensor of a component provided to you under this EULA exceed the amount that you paid to Red Hat for the media under this EULA.

5. Export Control. As required by the laws of the United States and other countries, you represent and warrant that you: (a) understand that the Programs and their components may be subject to export controls under the U.S. Commerce Department's Export Administration Regulations ("EAR"); (b) are not located in a prohibited destination country under the EAR or U.S. sanctions regulations (currently Cuba, Iran, Iraq, North Korea, Sudan and Syria, subject to change as posted by the United States government); (c) will not export, re-export, or transfer the Programs to any prohibited destination, persons or entities on the U.S. Bureau of Industry and Security Denied Parties List or Entity List, or the U.S. Office of Foreign Assets Control List of Specially Designated Nationals and Blocked Persons, or any similar lists maintained by other countries, without the necessary export license(s) or authorization(s); (d) will not use or transfer the Programs for use in connection with any nuclear, chemical or biological weapons, missile technology, or military end-uses where prohibited by an applicable arms embargo, unless authorized by the relevant government agency by regulation or



specific license; (e) understand and agree that if you are in the United States and export or transfer the Programs to eligible end users, you will, to the extent required by EAR Section 740.17(e), submit semi-annual reports to the Commerce Department's Bureau of Industry and Security, which include the name and address (including country) of each transferee; and (f) understand that countries including the United States may restrict the import, use, or export of encryption products (which may include the Programs and the components) and agree that you shall be solely responsible for compliance with any such import, use, or export restrictions.

6. Third Party Programs. Red Hat may distribute third party software programs with the Programs that are not part of the Programs. These third party software programs are not required to run the Programs, are provided as a convenience to you, and are subject to their own license terms. The license terms of the third party software programs or can be viewed at <http://www.redhat.com/licenses/thirdparty/eula.html>. If you do not agree to abide by the applicable license terms for the third party software programs, then you may not install them. If you wish to install the third party software programs on more than one system or transfer the third party software programs to another party, then you must contact the licensor of the applicable third party software programs.

7. General. If any provision of this EULA is held to be unenforceable, the enforceability of the remaining provisions shall not be affected. Any claim, controversy or dispute arising under or relating to this EULA shall be governed by the laws of the State of New York and of the United States, without regard to any conflict of laws provisions. The rights and obligations of the parties to this EULA shall not be governed by the United Nations Convention on the International Sale of Goods.

Copyright © 2010 Red Hat, Inc. All rights reserved. "Red Hat," "JBoss" and the JBoss logo are registered trademarks of Red Hat, Inc. All other trademarks are the property of their respective owners



ATTACHMENT 10

BUSINESS ASSOCIATE AGREEMENT COMPLIANCE WITH PRIVACY AND SECURITY RULES

THIS BUSINESS ASSOCIATE AGREEMENT (hereinafter “ Agreement”) i s bet ween **The State of Tennessee, Department of Mental Health and Substance Abuse Services** (hereinafter “Covered Entity”) and **Kronos Incorporated** (hereinafter “Business Associate”). Covered Entity and Business Associate may be referred to herein individually as “Party” or collectively as “Parties.”

BACKGROUND

Parties acknowledges that they are subject to the Privacy and Security Rules (45 CFR Parts 160 and 164) promulgated by the United States Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191 as amended by Public Law 111-5, Division A, Title XIII (the HITECH Act), in certain aspects of its operations.

Business Associate provides services to Covered Entity pursuant to one or more contractual relationships detailed below and hereinafter referred to as “Service Contracts.”

The Contract for the provision of a Time Keeping System, executed concurrently with this Agreement. In the course of executing Service Contracts, Business Associate may come into contact with, use, or disclose Protected Health Information (“PHI”). Said Service Contract(s) are hereby incorporated by reference and shall be taken and considered as a part of this document the same as if fully set out herein.

In accordance with the federal privacy and security regulations set forth at 45 C.F.R. Part 160 and Part 164, Subparts A, C, D and E , which require Covered Entity to have a written memorandum with each of its Business Associates, the Parties wish to establish satisfactory assurances that Business Associate will appropriately safeguard PHI and, therefore, make this Agreement.

DEFINITIONS

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in 45 CFR §§ 160.103, 164.103, 164.304, 164.501 and 164.504.

- 1.1 “Breach of the Security of the Business Associate’s Information System” shall have the meaning set out in its definition at T.C.A. § 47-18-2107
- 1.2 “Business Associate” shall have the meaning set out in its definition at 45 C.F.R. § 160.103.
- 1.3 “Covered Entity” shall have the meaning set out in its definition at 45 C.F.R. § 160.103.
- 1.4 “Designated Record Set” shall have the meaning set out in its definition at 45 C.F.R. § 164.501.
- 1.5 “Electronic Protected Health Care Information” shall have the meaning set out in its definition at 45 C.F.R. § 160.103.
- 1.6 “Genetic Information” shall have the meaning set out in its definition at 45 C.F.R. § 160.103.
- 1.7 “Health Care Operations” shall have the meaning set out in its definition at 45 C.F.R. § 164.501.
- 1.8 “Individual” shall have the same meaning as the term “individual” in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).
- 1.9 “Information Holder” shall have the meaning set out in its definition at T.C.A. § 47-18-2107



- 1.10 "Marketing" shall have the meaning set out in its definition at 45 C.F.R. § 164.501.
- 1.11 "Personal information" shall have the meaning set out in its definition at T.C.A. § 47-18-2107
- 1.12 "Privacy Official" shall have the meaning as set out in its definition at 45 C.F.R. § 164.530(a)(1).
- 1.13 "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, subparts A, and E.
- 1.14 "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
- 1.15 "Required by Law" shall have the meaning set forth in 45 CFR § 164.512.
- 1.16 "Security Incident" shall have the meaning set out in its definition at 45 C.F.R. § 160.304.
- 1.17 "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Parts 160 and 164, Subparts A and C.

2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE (Privacy Rule)

- 2.1 Business Associate is authorized to use PHI for the purposes of carrying out its duties under the Services Contract. In the course of carrying out these duties, including but not limited to carrying out the Covered Entity's duties under HIPAA, Business Associate shall fully comply with the requirements under the Privacy Rule applicable to "business associates," as that term is defined in the Privacy Rule and not use or further disclose PHI other than as permitted or required by this Agreement, the Service Contracts, or as Required By Law. Business Associate is subject to requirements of the Privacy Rule as required by Public Law 111-5, Section 13404 [designated as 42 U.S.C. 17934] in case of any conflict between this Agreement and the Service Contracts, this Agreement shall govern.
- 2.2 The Health Information Technology for Economic and Clinical Health Act (HITECH) was adopted as part of the American Recovery and Reinvestment Act of 2009. HITECH and its implementing regulations impose new requirements on Business Associates with respect to privacy, security, and breach notification. Business Associate hereby acknowledges and agrees that to the extent it is functioning as a Business Associate of Covered Entity, Business Associate shall comply with HITECH. Business Associate and the Covered Entity further agree that the provisions of HIPAA and HITECH that apply to business associates and that are required to be incorporated by reference in a business associate agreement have been incorporated into this Agreement between Business Associate and Covered Entity. Should any provision not be set forth specifically, it is as if set forth in this Agreement in its entirety and is effective as of the Applicable Effective Date, and as amended.
- 2.3 Business Associate shall use appropriate administrative, physical, and technical safeguards to prevent use or disclosure of PHI other than as provided for by this Agreement, Services Contract(s), or as Required By Law. This includes the implementation of Administrative, Physical, and Technical Safeguards to reasonably and appropriately protect the Covered Entity's PHI against any reasonably anticipated threats or hazards, utilizing the technology commercially available to the Business Associate. The Business Associate shall maintain appropriate documentation of its compliance with the Privacy Rule, including, but not limited to, its policies, procedures, records of training and sanctions of members of its Workforce.
- 2.4 Business Associate shall require any agent, including a subcontractor, to whom it provides PHI received from, maintained, created or received by Business Associate on behalf of Covered Entity or that carries out any duties for the Business Associate involving the use, custody, disclosure, creation of, or access to PHI or other confidential information, to agree, by written contract with Business Associate, to similar restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.



- 2.5 Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.
- 2.6 Business Associate shall require its employees, agents, and subcontractors to promptly report, to Business Associate, immediately upon becoming aware of any use or disclosure of PHI in violation of this Agreement. Business Associate shall report to Covered Entity any use or disclosure of the PHI not provided for by this Agreement. Business Associate will also provide additional information reasonably requested by the Covered Entity related to the breach.
- 2.7 As required by the Breach Notification Rule, Business Associate shall, and shall require its subcontractor(s) to, maintain systems to monitor and detect a Breach of Unsecured PHI, whether in paper or electronic form.
 - 2.7.1 Business Associate shall provide to Covered Entity notice of an Actual Breach of Unsecured PHI immediately upon becoming aware of the Breach.
 - 2.7.2 Business Associate shall cooperate with Covered Entity in timely providing the appropriate and necessary information to Covered Entity.
 - 2.7.3 Covered Entity shall make the final determination whether the Breach requires notification and whether the notification shall be made by Covered Entity or Business Associate.
- 2.8 If Business Associate receives PHI from Covered Entity in a Designated Record Set, Business Associate shall provide access, at the request of Covered Entity, to PHI in a Designated Record Set to Covered Entity, in order to meet the requirements under 45 CFR § 164.524, provided that Business Associate shall have at least 30 business days from Covered Entity notice to provide access to, or deliver such information.
- 2.9 If Business Associate receives PHI from Covered Entity in a Designated Record Set, then Business Associate shall, to the extent applicable, make any amendments to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to the 45 CFR § 164.526 at the request of Covered Entity or an Individual, and in the time and manner designated by Covered Entity, provided that Business Associate shall have at least 30 business days from Covered Entity notice to make an amendment.
- 2.10 Business Associate shall make its internal practices, books, and records including policies and procedures, relating to the use and disclosure of PHI received from, created by or received by Business Associate on behalf of, Covered Entity available to the Secretary of the United States Department of Health in Human Services or the Secretary's designee, in a time and manner designated by the Secretary, for purposes of determining Covered Entity's or Business Associate's compliance with the Privacy Rule.
- 2.11 Business Associate shall 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 disclosure of PHI in accordance with 45 CFR § 164.528.
- 2.12 Business Associate shall provide Covered Entity or an Individual, in time and manner designated by Covered Entity, information collected in accordance with this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528, provided that Business Associate shall have at least 30 business days from Covered Entity notice to provide access to, or deliver such information which shall include, at minimum to the extent known, (a) date of the disclosure; (b) name of the third party to whom the PHI was disclosed and, if known, the address of the third party; (c) brief description of the disclosed information; and (d) brief explanation of the purpose and basis for such disclosure. Business Associate shall provide an accounting of disclosures directly to an individual when required by section 13405(c) of Public Law 111-5 [designated as 42 U.S.C. 17935(c)].



- 2.13 Business Associate agrees it must limit any use, disclosure, or request for use or disclosure of PHI to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request in accordance with the requirements of the Privacy Rule.
- 2.13.1 Business Associate represents to Covered Entity that all its uses and disclosures of, or requests for, PHI shall be the minimum necessary in accordance with the Privacy Rule requirements.
- 2.13.2 Covered Entity may, pursuant to the Privacy Rule, reasonably rely on any requested disclosure as the minimum necessary for the stated purpose when the information is requested by Business Associate.
- 2.13.3 Business Associate acknowledges that if Business Associate is also a covered entity, as defined by the Privacy Rule, Business Associate is required, independent of Business Associate's obligations under this Memorandum, to comply with the Privacy Rule's minimum necessary requirements when making any request for PHI from Covered Entity.
- 2.14 Business Associate shall adequately and properly maintain all PHI received from, or created or received on behalf of, Covered Entity
- 2.15 If Business Associate receives a request from an Individual for a copy of the individual's PHI, and the PHI is in the sole possession of the Business Associate, Business Associate will provide the requested copies to the individual and notify the Covered Entity of such action. If Business Associate receives a request for PHI in the possession of the Covered Entity, or receives a request to exercise other individual rights as set forth in the Privacy Rule, Business Associate shall notify Covered Entity of such request and forward the request to Covered Entity. Business Associate shall then assist Covered Entity in responding to the request.
- 2.16 Business Associate shall fully cooperate in good faith with and to assist Covered Entity in complying with the requirements of the Privacy Rule.

3 OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE (Security Rule)

- 3.1 Business Associate shall fully comply with the requirements under the Security Rule applicable to "business associates," as that term is defined in the Security Rule. In case of any conflict between this Agreement and Service Agreements, this Agreement shall govern.
- 3.2 Business Associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that it receives, maintains, or transmits on behalf of the covered entity as required by the Security Rule and Public Law 111-5. This includes specifically, but is not limited to, the utilization of technology commercially available at the time to the Business Associate to protect the Covered Entity's PHI against any reasonably anticipated threats or hazards. The Business Associate understands that it has an affirmative duty to perform a regular review or assessment of security risks, conduct active risk management and supply best efforts to assure that only authorized persons and devices access its computing systems and information storage, and that only authorized transactions are allowed. The Business Associate will maintain appropriate documentation to certify its compliance with the Security Rule.
- 3.3 Business Associate shall ensure that any agent, including a subcontractor, to whom it provides electronic PHI received from or created for Covered Entity or that carries out any duties for the Business Associate involving the use, custody, disclosure, creation of, or access to PHI supplied by Covered Entity, to agree, by written contract (or the appropriate equivalent if the agent is a government entity) with Business Associate, to substantially the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.
- 3.4 Business Associate shall require its employees, agents, and subcontractors to report to Business Associate within ten (10) business days, any Security Incident (as that term is defined in 45 CFR §



164.304) of which it becomes aware. Business Associate shall promptly report any Security Incident of which it becomes aware to Covered Entity. For purposes of this Agreement, Security Incident shall exclude (i) "pings" on an information system firewall; (ii) port scans; (iii) attempts to log on to an information system or enter a database with an invalid password or user name; (iv) denial-of-service attacks that do not result in a server being taken offline; or (v) "malware" (e.g., a worm or a virus) that does not result in unauthorized access, use, disclosure, modification or destruction of PHI.

- 3.5 Business Associate shall make its internal practices, books, and records including policies and procedures relating to the security of electronic PHI received from, created by or received by Business Associate on behalf of, Covered Entity available to the Secretary of the United States Department of Health and Human Services or the Secretary's designee, in a time and manner designated by the Secretary, for purposes of determining Covered Entity's or Business Associate's compliance with the Security Rule.
- 3.6 Business Associate shall fully cooperate in good faith with and to assist Covered Entity in complying with the requirements of the Security Rule.
- 3.7 Notification for the purposes of Sections 2.8 and 3.4 shall be in writing made by email/fax, certified mail or overnight parcel immediately upon becoming aware of the event, with supplemental notification by facsimile and/or telephone as soon as practicable, to:

John Arredondo, Assistant Commissioner
Tennessee Department of Mental Health and Substance Abuse Services
Andrew Jackson Building, 6th Floor
500 Deaderick Street
Nashville, TN 37243
John.Arredondo@tn.gov
Telephone # 615-532-6515

- 3.8 Business Associate identifies the following key contact persons for all matters relating to this Agreement:

Kronos Incorporated
297 Billerica Road
Chelmsford, MA 01824
Attn: Kronos Legal

Business Associate shall notify Covered Entity of any change in the key contact during the term of this Agreement in writing within ten (10) business days.

4. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

- 4.1 Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in Service Contract(s), provided that such use or disclosure would not violate the Privacy and Security Rule, if done by Covered Entity. Business Associate's disclosure of PHI shall be subject to the limited data set and minimum necessary requirements of Section 13405(b) of Public Law 111-5, [designated as 42 U.S.C. 13735(b)]
- 4.2 Except as otherwise limited in this Agreement, Business Associate may use PHI as required for Business Associate's proper management and administration or to carry out the legal responsibilities of the Business Associate.
- 4.3 Except as otherwise limited in this Agreement, Business Associate may disclose PHI for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or provided that, if Business Associate discloses any PHI to a third party for such a



purpose, Business Associate shall enter into a written agreement with such third party requiring the third party to: (a) maintain the confidentiality, integrity, and availability of PHI and not to use or further disclose such information except as Required By Law or for the purpose for which it was disclosed, and (b) notify Business Associate of any instances in which it becomes aware in which the confidentiality, integrity, and/or availability of the PHI is breached immediately upon becoming aware.

- 4.4 Except as otherwise limited in this Agreement, Business Associate may use PHI to provide data aggregation services to Covered Entity as permitted by 42 CFR § 164.504(e)(2)(i)(B).
- 4.5 Business Associate may use PHI to report violations of Law to appropriate Federal and State Authorities consistent with 45 CFR 164.502(j)(1).
- 4.6 Business Associates shall not use or disclose PHI that is Genetic Information for underwriting purposes. Moreover, the sale, marketing or the sharing for commercial use or any purpose construed by Covered Entity as the sale, marketing or commercial use of member's personal or financial information with affiliates, even if such sharing would be permitted by federal or state laws, is prohibited.
- 4.7 Business Associate shall enter into written agreements that are substantially similar to this Business Associate Agreements with any Subcontractor or agent which Business Associate provides access to Protected Health Information.
- 4.8 Business Associates shall implement and maintain information security policies that comply with the HIPAA Security Rule.

5. OBLIGATIONS OF COVERED ENTITY

- 5.1 Covered Entity shall provide Business Associate with the Notice of Privacy Practices that Covered Entity produces in accordance with 45 CFR § 164.520, as well as any changes to such notice. Covered Entity shall notify Business Associate of any limitations in its notice that affect Business Associate's use or disclosure of PHI.
- 5.2 Covered Entity shall provide Business Associate with 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.
- 5.3 Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use of PHI.

6. PERMISSIBLE REQUESTS BY COVERED ENTITY

Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy or Security Rule, if done by Covered Entity.

7. TERM AND TERMINATION

- 7.1 **Term.** This Agreement shall be effective as of the date on which it is signed by both parties and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy PHI, Section 7.3. below shall apply.

7.2 Termination for Cause.

- 7.2.1 This Agreement authorizes and Business Associate acknowledges and agrees Covered Entity shall have the right to immediately terminate this Agreement and Service Contracts in the event Business



Associate fails to comply with, or violates a material provision of, requirements of the Privacy and/or Security Rule or this Memorandum.

7.2.2 Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

7.2.2.1 Provide a reasonable opportunity for Business Associate to cure the breach or end the violation, or

7.2.2.2 If Business Associate has breached a material term of this Agreement and cure is not possible or if Business Associate does not cure a curable breach or end the violation within a reasonable time as specified by, and at the sole discretion of, Covered Entity, Covered Entity may immediately terminate this Agreement and the Service Agreement.

7.2.2.3 If neither cure nor termination is feasible, Covered Entity shall report the violation to the Secretary of the United States Department of Health and Human Services or the Secretary's designee.

7.3 Effect of Termination.

7.3.1 Except as provided in Section 7.3.2. below, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of, Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.

7.3.2 In the event that Business Associate determines that returning or destroying the PHI is not feasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction unfeasible. Upon mutual agreement of the Parties that return or destruction of PHI is unfeasible; Business Associate shall extend the protections of this Memorandum to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction unfeasible, for so long as Business Associate maintains such PHI.

8. MISCELLANEOUS

8.1 Regulatory Reference. A reference in this Agreement to a section in the Privacy and or Security Rule means the section as in effect or as amended.

8.2 Indemnity. The Business Associate shall indemnify the Covered Entity and hold it harmless for any claims, losses or other damages arising from or associated with any act or omission of Business Associate under this Agreement. This includes the costs of responding to a breach of the Agreement or the release of PHI contrary to the terms and conditions of this Agreement, the costs of responding to a government enforcement action related to the breach, and any resultant fines, penalties, or damages paid by the Covered Entity as a result of a breach of this Agreement by Business Associate. The obligations of the Business Associate to indemnify the Covered Entity under this Section 8.2 shall not exceed the limitation of liability of the Contract in accordance with this Agreement.

8.3 Amendment. The Parties agree to take such action as is reasonably necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy and Security Rules and the Health Insurance Portability and Accountability Act, Public Law 104-191, including any amendments required by the United States Department of Health and Human Services to implement the Health Information Technology for Economic and Clinical Health and related regulations upon the effective date of such amendment, regardless of whether this Agreement has been formally amended, including, but not limited to changes required by the American Recovery and Reinvestment Act of 2009, Public Law 111-5. In the event the Parties are



unable to enter into an amendment of this Agreement by mutual agreement, either Party may terminate the Agreement for cause in accordance with Article 7.

- 8.4 Survival. The respective rights and obligations of Business Associate under Section 7.3. of this Memorandum shall survive the termination of this Agreement.
- 8.5 Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity and the Business Associate to comply with the Privacy and Security Rules.
- 8.6 Notices and Communications. All instructions, notices, consents, demands, or other communications required or contemplated by this Agreement shall be in writing and shall be delivered by electronic mail with a hard copy provided by hand, by facsimile transmission, by overnight courier service, or by first class mail, postage prepaid, addressed to the respective party at the appropriate facsimile number or address as set forth below, or to such other party, facsimile number, or address as may be hereafter specified by written notice.

COVERED ENTITY:

John Arredondo, Assistant Commissioner
Tennessee Department of Mental Health and
Substance Abuse Services
Andrew Jackson Building, 6th Floor
500 Deaderick Street
Nashville, TN 37243
John.Arredondo@tn.gov
Telephone # 615-532-6515

BUSINESS ASSOCIATE:

Kronos Incorporated
Kronos Legal
297 Billerica Road
Chelmsford, MA 01824

All instructions, notices, consents, demands, or other communications shall be considered effectively given as of the date of hand delivery; as of the date specified for overnight courier service delivery; as of three (3) business days after the date of mailing; or on the day the facsimile transmission is received mechanically by the facsimile machine at the receiving location and receipt is verbally confirmed by the sender.

- 8.7 Strict Compliance. No failure by any Party to insist upon strict compliance with any term or provision of this Agreement, to exercise any option, to enforce any right, or to seek any remedy upon any default of any other Party shall affect, or constitute a waiver of, any Party's right to insist upon such strict compliance, exercise that option, enforce that right, or seek that remedy with respect to that default or any prior, contemporaneous, or subsequent default. No custom or practice of the Parties at variance with any provision of this Agreement shall affect, or constitute a waiver of, any Party's right to demand strict compliance with all provisions of this Agreement
- 8.8 Severability. With respect to any provision of this Agreement finally determined by a court of competent jurisdiction to be unenforceable, such court shall have jurisdiction to reform such provision so that it is enforceable to the maximum extent permitted by applicable law, and the Parties shall abide by such court's determination. In the event that any provision of this Agreement cannot be reformed, such provision shall be deemed to be severed from this Agreement, but every other provision of this Agreement shall remain in full force and effect.
- 8.9 Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the State of Tennessee except to the extent that Tennessee law has been pre-empted by HIPAA.
- 8.10 Compensation. There shall be **no** remuneration for performance under this Agreement except as specifically provided by, in, and through, existing administrative requirements of Tennessee State government and services contracts referenced herein.
- 8.11 Security Breach. A violation of HIPAA or the Privacy or Security Rules constitutes a breach of this Business Associate Agreement and a breach of the Service Contract(s) listed on page one of this agreement, and shall be subject to all available remedies for such breach as specified in the Service Contracts.



IN WITNESS WHEREOF,

Tennessee Department of Mental Health and Substance Abuse Services:

Marie Williams 11.2.16
MARIE WILLIAMS, COMMISSIONER Date:

BUSINESS ASSOCIATE LEGAL ENTITY NAME: KRONOS INCORPORATED

Alyce Moore November 2, 2016
NAME AND TITLE - Alyce Moore, VP, General Counsel Date:



ATTACHMENT 11

EXTENSION CLOUD SERVICES

Cloud Services for Extension Applications

Cloud Offering	
<p>Environments:</p> <p>One standard Production and one Non-Production (Development) environment.</p> <p>Excludes encryption gateway software running at a location in customer's control outside of Kronos Cloud.</p>	<p>Included. More non-production environments are available for additional fees.</p>
<p>Environment restoration:</p> <p>Restore of Production environment to one Non-Production environment once per week.</p> <p>Customer is responsible for requesting data to be moved from the Production environment to the Non-Production environment and for the contents of the data moved from the Production environment to the Non-Production environment.</p> <p>Excludes encryption gateway software running at a location in customer's control outside of Kronos Cloud.</p>	<p>Included. More frequent restores or additional environments will be subject to additional time and material fees.</p>
<p>Connectivity to Service:</p> <p>Customer's users connect to application via secure TLS connection over the internet. Cooperative efforts with customer IT staff may be required to enable access. Kronos will assist with validating site connectivity but assumes no responsibility for customer internet connection or ISP relationships. Kronos related Internet traffic cannot be filtered by proxy or caching devices on the client network. Exclusions must be added for the fully qualified domain names and public IP addresses assigned to the environments in the Kronos Cloud. Applicable ports must be opened from customer network as described in product documentation.</p>	<p>Included</p>
<p>Operating System and Database Software Management: Includes application of critical security patches, service packs and hot-fixes; maintenance of servers.</p> <p>Excludes encryption gateway software running at a location in customer's control outside of Kronos Cloud.</p>	<p>Included</p>
<p>Server Maintenance: Repair and replacement of defective or failed</p>	<p>Included</p>



Cloud Offering	
<p>hardware and the installation of hardware upgrades.</p> <p>Excludes encryption gateway software running at a location in customer's control outside of Kronos Cloud.</p>	
<p>Application Updates: Services to perform technical tasks required to apply application service packs, legislative updates (if applicable), point releases and version upgrades.</p> <p>Excludes encryption gateway software running at a location in customer's control outside of Kronos Cloud.</p>	Included
<p>Backup:</p> <p>Customer data is backed up daily. Database backups are replicated via encrypted connections to a second Kronos Cloud datacenter. Backups are retained for the prior 28 days on a rotating basis. All historical employee and configuration data is stored in the rotating backups.</p> <p>Excludes encryption gateway software running at a location in customer's control outside of Kronos Cloud.</p>	Included
<p>Security:</p> <p>Kronos maintains a hosting environment that undergoes examinations from an independent auditor in accordance with the American Institute of Certified Public Accounts (AICPA) Trust Services Principles Section 100a, Trust Services for Security, Availability, Processing Integrity, Confidentiality and Privacy (i.e. SOC 2). The Kronos Private Cloud (KPC) is evaluated for the principles of Security, Availability and Confidentiality by the independent auditor. The Kronos Private Cloud is located in data centers that undergo SSAE 16 examinations. Management access to the KPC is limited to authorized Kronos support staff and customer authorized integrations. The security architecture has been designed to control appropriate logical access to the KPC to meet the Trust Services Principles of Security, Availability and Confidentiality. The Applications provide the customer with the ability to configure application security and logical access per the customer's business processes. Additionally the independent auditor will provide an opinion on the design and operating effectiveness of controls to meet the security requirements of the Health Insurance Portability and Accountability Act Security Rule, which will be first issued by end of calendar year 2016.</p> <p>In the event the customer identifies a security issue, the customer will notify Kronos. For security purposes, customers are restricted from accessing the desktop, file systems, databases and operating system of the environments.</p> <p>Customer agrees not to upload payment card information as the service is not certified for PCI DSS.</p>	Included



Cloud Offering	
<p>For each of the customer's production and non-production environments in a data center in the United States of America, Customer Content will be Encrypted at rest at the storage level for the Extension Application(s). Encryption at rest is defined as Customer Content is made unreadable on disk via encryption technology when the Kronos Cloud computing environment hardware is powered off. For clarity this storage level of Encryption within the Kronos Private Cloud is independent of the Encryption at the Encryption Gateway Tool located at the customer's location, thus providing a second layer of encryption at rest.</p>	
<p>Basic Disaster Recovery Services:</p> <p>Customer environment and all customer data in the Kronos Cloud are replicated to a secondary Kronos Cloud data center. Basic Disaster Recovery Services provides a Recovery Point Objective (RPO) of 24 hours and Kronos strives to restore Application Availability in a commercially reasonable timeframe.</p> <p>The customer will be down until production processing is restored in the primary or secondary data center if needed. No application environment is readily available at the alternate site to process data. Customers are expected to use fully qualified domain names (FQDNs) to access the service given that IP address of the service may change.</p> <p>Any issues arising out of the disaster recovery event due to customer configuration/customization and/or customer third party software outside of the Kronos Cloud is the responsibility of the customer to resolve.</p> <p>Excludes encryption gateway software running at a location in customer's control outside of Kronos Cloud.</p>	Included
<p>Enhanced Disaster Recovery Services:</p> <p>Customer environment and all customer data in the Kronos Cloud are replicated to a secondary Kronos Cloud datacenter. Enhanced Disaster Recovery Services provide an RTO (Recovery Time Objective) of 72 hours and a RPO (Recovery Point Objective) of 24 hours.</p> <p>In the unlikely event that Kronos declares a disaster in trest</p> <p>he primary datacenter, Kronos will notify the customer and activate the Disaster Recovery steps necessary to restore application availability within the RTO defined.</p> <p>As part of the enhanced service, Kronos will conduct an annual Disaster Recovery Process test which has the objectives to 1) test backups 2) train Kronos employees 3) verify and improve internal Kronos procedures. The annual Disaster Recovery Process test may be live or simulated test.</p> <p>Customers are expected to use fully qualified domain names (FQDNs) to</p>	If purchased on Section C.3



Cloud Offering	
<p>access the service given that IP address of the service may change. Any issues arising out of the disaster recovery event due to customer configuration/customization and/or customer third party software outside of the Kronos Cloud is the responsibility of the customer to resolve.</p> <p>Excludes encryption gateway software running at a location in customer's control outside of Kronos Cloud.</p>	

Guidelines and Assumptions:

Category	Assumption
	Estimated availability of production server hardware in Kronos Cloud is approximately 30 days after the Order Form is processed.
	Customer agrees to receive automatic updates to the Applications.
	Applications will support English only.
	Customer agrees not to conduct security testing, which includes but is not limited to penetration testing and vulnerability scanning.
	Customer agrees not conduct any sort of automated or manual performance testing of the Service.
	Retention policies must be configured in the Application(s). Setting retention policies will ensure that unnecessary system data (e.g. temp files, deleted records, empty rows, etc.) is routinely purged from the system and will help in managing database growth. Additionally application audit log will retained for 30 days.
	Customer will be required to sign a go live milestone document confirming customer has completed its testing and is ready to go live with the Workforce Central Application EHC module(s).

Workforce Central EHC Upgrade Services

The Service includes services for Kronos to execute tasks to apply point releases and version upgrades to customer's Kronos Applications in the Kronos Cloud. Services are limited to those tasks which apply these



updates to the Applications. Services related to upgrade of Encryption Gateway Environment and encryption gateway software running at a location in customer's control outside of Kronos Cloud are not included.

The table below reflects the included upgrade tasks.

Planning Phase	
Customer/ Kronos Introduction Call – up to 30 minutes	Included
Technical readiness & architecture review – Kronos Cloud Environment	Included
Technical readiness & architecture review – Encryption Gateway environment	Not Included
Assessment Phase	
Assessment of Interface Upgrade to WFC	Included
Assessment of new features or changes to configuration	Not included
Assessment of customs, custom interfaces and custom reports and development activities related thereto	Not included
Solution Upgrade / Build Phase	
One (1) restore of Production database to Pre-Production environment for the purpose of upgrade testing. Additional restores, if requested, shall be subject to additional time and material fees.	Included
Upgrade Non-Production and Production environments to new point release or version.	Included
Upgrade of interface integration to Workforce Central per features in product documentation.	Included
Upgrade of integrations beyond integration to Workforce Central per features in product documentation.	Not Included
Upgrade of any customs, custom interfaces and custom reports and development activities related thereto	Not Included
Configuration of new features or functionality or changes to existing configuration	Available for Purchase
Upgrade of Encryption Gateway Environment and encryption gateway software running at a location in customer's control outside of Kronos Cloud.	Not Included



Test & Certify Phase	
User acceptance testing (UAT) of upgraded environments, interfaces, custom reports, new features, etc.	Not Included
Develop customer-specific test cases	Not Included
Sign-off on upgraded Non-Production and Production Environments	Customer
Deploy & Support Phase	
Deployment Readiness Call – up to 30 minutes	Included

Note that new feature configuration, project management services, other Professional, Managed and Educational Services and training are not included as part of Upgrade Services, but may be purchased independently, if desired.

If not specifically noted, the customer should assume responsibility of the task and/or deliverable.