Department of Information Resources

Software, including Software as a Service, Products and Related Services

Bid Package 7

Software as a Service Questionnaire

Request for Offer DIR-TSO-TMP-225

Note: Complete a Questionnaire for each proposed Software as a Service (SaaS) solution product family.

SaaS Solution: AppBase Dynamic Case Management System

Technical/Functional Response

TECHNICAL - Basic Requirements

Explain how your company provides these basic requirements:

1. Data hosted off site is accessible 99.5% including all planned and unplanned downtime. Planned downtime must be coordinated.

   ANSWER: Provider offers all services load balanced and replicated across at least two geographical locations with warm and hot failover offerings, as well as full Disaster Recovery. Network connections are also redundant. Special Service Levels Agreements may be independently negotiable with each customer.

2. All data is backed up every 24 hours at Vendor's site. Backup information will be stored in a different location from the computer center where the hosting servers are located. If restoration of data is required, can the Vendor upon notification restore the data within one business day?

   ANSWER: All data is backed up incrementally and daily, and all files are replicated in the Cloud across geographical locations on a near real time basis. Data restoration can be accomplished in one business day or less.

3. The Customer is involved in and informed of any operational changes made that affect access to the data. That includes but is not limited to:

   - Migration, upgrades or other changes to the server that require downtime or a server reboot must be coordinated at least 10 working days in advance. Security patches and other emergency requirements can be coordinated with less notice but a designated Customer representative must be contacted prior to rebooting the server.

     ANSWER: Provider maintains a 24 hour monitoring and notification center, and any emergency downtime is performed after full customer notification. For those customers under 24/7 support plans, our Notification Center ensures live contact is made prior to emergency downtime if it can be accomplished. Other maintenance activities are scheduled regularly in accordance with customer SLAs and customers are duly notified.

   - A designated Customer representative must be notified within 30 minutes of an unplanned outage and must be given an estimated recovery time or hourly status updates until the recovery time is known.

     ANSWER: Eccentex maintains a 24 hour monitoring and notification center, and any emergency or unplanned downtime occurs only after full customer notification. Status reports are made in near real-time

   - Is there a Customized error page (other than the standard page cannot be found 404 error) during outages (planned or otherwise)? Is prior notice included on the page to visitors of planned outages?

     ANSWER: Yes

4. Can Customer data under the protection of the Vendor (under its care, custody and control) be returned to the Customer upon notice, with the data/ metadata transferred in Comma Separated Value (CSV) file format that can be recovered for use within an Oracle or SQL database environment?

   ANSWER: Yes

5. Is the SaaS Solution available and accessible to all users 24 hours a day, 7 days a week, except for prescheduled maintenance periods?

6. **ANSWER:** Yes

7. Data protection controls comply with the requirements of Texas Administrative Code § 202, Information Security. Customers have the capability to ensure compliance through audit of the environment.

   ANSWER: Yes.

Response Codes: Provided, Modified, or Not Provided.

Provided	The requirement is satisfied by the SaaS solution proposed with no modification to the source code. The requirement is met either "out-of-the box" or through configuration of the application. Yes
Modified	A modification to the SaaS solution is required to satisfy this requirement.
Not Provided	The SaaS solution will not satisfy the requirement.

Detailed Technical Requirements

Respond with detailed answers where indicated. Otherwise provide the appropriate response of **Provided, Modified** or **Not Provided as defined above**.

	Technical Requirements:	Response Code
	Security	
1.	For a hosted environment, fully describe the physical security. (Detailed response)	**24 hour monitored physical security:** Datacenters are physically constructed, managed, and monitored to shelter data and services from unauthorized access as well as environmental threats. **Zero standing privileges.** Access to customer data by data center operations and support personnel is denied by default. When granted, access is carefully managed and logged. Data center access to the systems that store customer data is strictly controlled via lock box processes. For enterprise customers, only specific, pre-identified personnel have access to

		support specific customer applications. **Restricted data access and use:** Access to customer data by support personnel is restricted. Customer Data is only accessed when necessary to support the customer's use of data center. This may include troubleshooting aimed at preventing, detecting or repairing problems affecting the operation of data center and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam). When granted, access is carefully controlled and logged. Strong authentication, including the use of multi-factor authentication, helps limit access to authorized personnel only. Access is revoked as soon as it is no longer needed. **Personnel Screening:** Depending on the customer use case, specific personnel undergo enhanced background checks to comply with clearance requirements of specific lines of business (i.e. Law Enforcement, Intelligence).

		Otherwise, all designated personnel are screened for honesty and integrity and criminal background checks.
2.	Describe assurance of security from (1) the SaaS software and (2) personnel aspects. (Detailed response)	Vendor offers an extensible compliance framework across a diverse set of regulations and is able to rapidly adapt to changes in the regulatory landscape. Specific Compliance Programs are: •ISO 27001/27002 •SOC 1/SSAE 16/ISAE 3402 and SOC 2 •Cloud Security Alliance CCM •FedRAMP •FISMA •FBI CJIS (Azure Government) •PCI DSS Level 1 •United Kingdom G-Cloud •Australian Government IRAP •Singapore MTCS Standard •HIPAA •EU Model Clauses •Food and Drug Administration 21 CFR Part 11 •FERPA •FIPS 140-2 •CCCPPF •MLPS
3.	How will the vendor respond if a security breach is identified, whether caused by a vulnerability in the application code, in the hosted environment, or otherwise? (Detailed response)	Vendor complies with all federal and state reporting requirements covering suspected and/or actual breaches of systems and/or data.

		Based on the broad range of potential breaches, Vendor will respond accordingly, including: Legally mandated notifications, remediation and patching, emergency audit, customer training if needed, participation in security audit/investigations and others.
4.	Describe how the software addresses security issues, including personnel, access rights, encryptions/SSL, firewall and protocol conflicts, database security, and conflicts with standard OS. (Detailed response)	Software maintains a completely role based security model, which applies to all levels of data and application layers, including field levels. Complete logging of all actions is provided and vendor also provides log monitoring services where requested. **Monitoring and logging**. Security is monitored with the aid of centralized monitoring, correlation, and analysis systems that manage the large amount of information generated by devices within the environment and providing timely alerts. In addition, multiple levels of monitoring, logging, and reporting are available to provide visibility to customers. **Intrusion detection and DDoS.** Intrusion detection and prevention systems, denial of service attack

		prevention, regular penetration testing, and forensic tools help identify and mitigate threats from both outside and inside of data center. **Isolation.** Vendor uses network isolation to prevent unwanted communications between deployments, and access controls block unauthorized users. Virtual Machines do not receive inbound traffic from the Internet unless we configure them to do so. **Virtual Networks.** Customers can choose to assign multiple deployments to an isolated Virtual Network and allow those deployments to communicate with each other through private IP addresses. **Encrypted communications.** Built-in SSL and TLS cryptography enables customers to encrypt communications within and between deployments, from data center to on-premises datacenters, and from data center to administrators and users. **Private connection.** Customers can establish a private connection to datacenters, keeping their traffic off the Internet. **Data encryption.** Vendor offers a wide range of encryption capabilities up to AES-256, giving customers the

		flexibility to implement the methods that best meets their needs. Data is offered as encrypted in transit and encrypted at rest. **Identity and access**. Active Directory enables customers to manage access to data center and their cloud apps. Multi-Factor Authentication and access monitoring offer enhanced security.
5.	Explain the software's quarantine functions and /or strategy, including how files and attachments are scanned for viruses. (Detailed response)	Antimalware is built-in to Cloud Services and is enabled for each Virtual Machine to help identify and remove viruses, spyware and other malicious software and provide real time protection. Customers can also run antimalware solutions from own partners on their Virtual Machines if the customer is running dedicated VMs in our data center. Various levels of additional virus scanning is offered where appropriate.
6.	Explain whether the software was developed by a third party and if yes, whether the third party is contractually obligated to maintain security controls. (Detailed response)	Software is developed and maintained completely by Eccentex Corporation. Datamatix is the local reseller and integrator. Eccentex license agreements deliver on such obligations direct to each customer that Datamatix sells to.

7.	Explain whether the software has been assessed for security by an objective third party. If yes, please provide the results. (Detailed response)	Yes. Both Data Center and Software have been assessed multiple times. Due to sensitive nature of these reports, full reports are made available direct to customers or potential customers upon request with the execution of a non-disclosure agreement. Data Center audits are extensive based on the various compliance standards noted above and can be provided if customer would identify which standard they would be operating under based on the specific use case (FedRAMP, HIPPA, CJIS, etc). **Testing summary of applications is as follows:** Lateral Security performed testing on the application from the perspective of an attacker with network access to the application. The methodology used for the testing of applications platform was as follows: •Application functionality identification •Attack surface discovery •Vulnerability identification •Vulnerability exploitation •Post-exploitation information gathering Testing was conducted against the OWASP testing framework.

		Examples of areas tested include: •Information gathering •Authentication •Session management •Authorisation •Data validation •Business logic Scope: •External network penetration test of internet facing network infrastructure •External network penetration test of internet facing service infrastructure •Unauthenticated web application penetration test •Authenticated web application penetration test Summary Results: 9 Severity Low 1 Severity Med 0 Severity High Action: Remediation was performed and Severity Medium items were addressed, and 8 of 9 Severity items were addressed and re-audited. Remediation assessed as successful.
8.	The software has the ability for multiple concurrent users to access the system.	Provided
9.	The software is scalable to handle increased loads.	Provided
10.	The software inherently has health performance tools.	Provided

11.	The software has the ability to detect and recover from file integrity issues (e.g., data corruption).	Provided. This assumes files arrive with integrity intact.
12.	The software has protection in place to prevent users from changing application code or data without proper authorization.	Provided
13.	Vendor warrants that all provided software does not contain any known viruses, or undocumented security codes that could prevent effective and secure use of the software.	Provided
14.	Network security audits are conducted annually or more frequently.	Provided
Hosted Implementation		
1.	All data center employees and subcontractors are subjected to background checks.	Provided
2.	A data backup and recovery system is in place.	Provided
3.	A disaster recovery plan is in place. (Detailed response)	Business Continuity and Disaster Recovery plans address the following: **Local Failures:** Physical hardware (for example drives, servers, and network devices) can all fail and resources can be exhausted when load spikes. **Regional Failures:** Widespread failures are rare but possible. Entire regions can become isolated due to network failures, or be physically damaged due to natural disasters. **Data Corruption and Accidental Deletion:** Bugs or other accidents or user errors result in data corruption and/or loss

		Vendor often serves very large enterprise customers with Hybrid cloud configurations and business continuity requirements that require customer by customer configurations and SLAs. However, in a general sense, vendor deploys all applications and data across at least two geographies, and provides auto-failover and auto-scaling of application servers. Dual or multiple dedicated redundant network connections can also be provided, though redundant network connections are standard with all vendor offerings. Data loss and/or corruption is recovered via data roll-back, restoration, or in the case of high-availability requirements, replicated failover services.
4.	Customer data can be exported to SQL or Oracle from your system upon termination of the contract. (Detailed response)	There are no proprietary data or file storage methodologies utilized in vendor's solution. Customer can be provided export of data into any standard formats required, can be provided an actual copy of database, or entire application and data can be exported for re-use.

		Meta data definition and business object model are readily documented for each customer application so customer can easily understand their data configuration
5.	The software is able to work through web proxy.	Provided
6.	The data center, including data backup storage, is located in the Continental US.	Provided
7.	The data center, including data backup storage, is located in the State of Texas.	Provided. Customer may choose data location
8.	The personnel accessing customer data, including data backup storage, are located in the Continental US / Texas. (Detailed response)	Unless required by customer, all data and vendor personnel directly accessing any customer data or backups are located in the continental united states. For vendor's 24-hour monitoring and notification service customers, vendor uses Europe based personnel for after hour's notification. These personnel do not access customer systems, data or backups.
9.	The personnel accessing customer data, including data backup storage, are located outside the Continental US.	Not unless requested by customer.
10.	Describe the software's multi-tenant architecture as it relates to performance monitoring, scalability and hardware provisioning to maintain effective separation of customer data and application. (Detailed response)	Scalability is accomplish by the addition of nodes to high-load services. AppBase is a Service Oriented Architecture solution and as such is scaled through the provisioning of additional load balanced services.

		Eccentex 24 hour monitoring center views all performance metrics continuously, and auto-provisioning of additional VMs is configured to spin up additional application servers dynamically the instant performance falls below defined levels. The multi-tenancy model of AppBase is segmented at the application level, with no comingling of customer specific data. Each tenant receives their own underlying schema with unique service accounts, separate from other customers.

General Technical		
1.	All network ports and protocols utilized by the software are documented and will be provided to Customer.	Provided
2.	The vendor provides remote customer support through telephone, email, and the web.	Provided
3.	The system complies with the ANSI 1989 standards for SQL (e.g., support transaction logging with commit, rollback, and roll forward facilities for restores, referential integrity and table driven coding structures).	Provided
4.	All software is free of date related defects (e.g., four digit years).	Provided
5.	System data is accessible 24/7.	Provided
6.	Describe Service Level Agreement (SLA) for resolving customer reported defects (e.g. high, medium and low severities). (Detailed response)	Customer may negotiate additional SLA or hours of support where appropriate, but vendor offers the

		following standard SLA during business hours of operation in local time zone, or in 24/7 mode for certain applications. Vendor shall use commercially reasonable efforts to respond to problems in accordance with the "Priority Codes" set forth below. The Priority Codes below depict the priority level to be assigned by Vendor to each issue or problem reported by Customer. "A Priority" - Licensed IP is completely inoperable. Resources assigned within one (1) hour after notice. "B Priority" - Licensed IP error is detected for a system module, which seriously impairs system operations, but does not render it inoperable. Resources assigned within four (4) hours after notice during standard support hours. "C Priority" – Customer has a problem with Licensed IP but there is a known workaround which does not seriously impair the operation of Licensed IP. Resources assigned within eight (8) hours after notice during standard support hours. "D Priority" - Minor problems which Eccentex plans, or will plan to

		incorporate into a future release of the Licensed IP, to be resolved in connection with the general commercial availability of such future release.

Technical Architecture

Using the questions and tables in this form, please indicate the technical requirements for implementing your SaaS solution. Where the tables request recommended configurations, specify hardware capable of supporting performance and scalability requirements identified elsewhere in this RFO.

1. Please complete the following table to specify the minimum and recommended workstation configuration required to run your client software.

Workstation	Minimum	Recommended
Operating system(s) with version number	The Windows family of operating system • Windows XP SP3 • Windows Vista SP2 • Windows 7 family • Windows 8 family	Windows 7 family or higher
Hard drive free space	100GB	100GB or higher
RAM	4GB	4GB or higher
Processor and speed	Pentium Dual-Core, 2.00 Ghz	Intel i5, 2.6Ghz or higher
Monitor size	14''	19'' or higher
taaLAN speed	100 m/b	100 m/b or higher
Other software with version number (e.g., plug-in, etc.) – please list	Net Framework 3.5 SP1	Net Framework 3.5 SP1 or higher

1. What browsers are supported?

Browser	Supported
Microsoft Internet Explorer (current and prior versions)	Internet Explorer 8.x or higher
FoxPro (current and prior versions)	FireFox 3.5 or higher
Google Chrome (current and prior versions)	Google Chome 5.0.375 or higher
Opera (current and prior versions)	Opera 11 or higher
Safari (current and prior versions)	Safari 3.0 or higher