Enterprise Password Management

REQUEST FOR PROPOSAL
#R14013

JOLIET JUNIOR COLLEGE
1901

Joliet Junior College
Request for Proposal

Enterprise Password Management

RFP Opening October 28, 2014

Background

Joliet Junior College is a comprehensive community college. The college offers pre-baccalaureate programs for students planning to transfer to a four-year university, occupational education leading directly to employment, adult education and literacy programs, work force and workplace development services, and support services to help students succeed. The College has a combined total of 15,516 full time and part time students enrolled in Spring 2014 classes on its main campus located within the city of Joliet, and its five extension campuses located in Romeoville, Morris, Frankfort, Weitendorf, and City Center in downtown Joliet.

Vision Statement

Joliet Junior College, the nation's first public community college, will be a leader in teaching and learning, and the first choice for post-secondary education.

Mission Statement

Joliet Junior College enriches people's lives through affordable, accessible, and quality programs and services. The college provides transfer and career preparation, training and workforce development, and a lifetime of learning to the diverse community it serves.

I. OVERVIEW

The Board of Trustees of Joliet Junior College (hereinafter, "JJC") is requesting proposals from Providers for software solutions relating to Enterprise Password Management.

Additional scope is discussed in the **SCOPE OF WORK** section of this proposal.

II. RFP SCHEDULE

Date **(2014)**	**Event**
October 16, 2014	Vendors contacted via email / advertised
October 21, 2014 @ Noon	Last date/time for submission of written questions via email to purchasing@jjc.edu
October 22, 2014 – end of business day	Responses to questions emailed
October 28, 2014 @ 2:00 p.m.	Proposals must be submitted to the attention of: Janice Reedus, Director of Business & Auxiliary Service, Campus Center Building A, Room 3100, 1215 Houbolt Road, Joliet, IL 60431
October 28-29 , 2014	JJC Evaluation Team reviews proposal
November 13, 2014	Notification of Award

III. INSTRUCTIONS TO VENDORS

ADVICE: The department responsible for this RFP is the Business and Auxiliary Services located at Campus Center, Building A, Room 3100, 1215 Houbolt Rd., Joliet, IL 60431-8938. The JJC contact will be Janice Reedus, Director of Business & Auxiliary Services, telephone (815) 280-6640; fax (815) 280-6631.

Questions concerning this RFP will be answered if sent to the Purchasing Department via email to purchasing@jjc.edu on or before **October 21, 2014 at 12:00 p.m.**

All questions and answers will be published and provided to all potential suppliers by end of business day on **October 22, 2104 by the end of the business day**.

SUBMISSION: the submission of a response shall be prima facie evidence that the supplier has full knowledge of the scope, nature, quality of work to be performed, the detailed requirements of the project, and the conditions under which the work is to be performed.

Faxed proposals ARE NOT acceptable. All RFP's must be submitted by the date and time of public opening (see above). RFP's must be submitted on the forms provided in a sealed envelope clearly marked (typed or blocking lettering only) with the vendor's name, return address, RFP for Enterprise Password Management, the opening date and time. **An original and eight (8) copies of the RFP shall be provided; along with a digital copy (PDF).**

RFPs must be addressed to: Joliet Junior College, Janice Reedus, Director of Business & Auxiliary Services, Campus Center Room A3102, 1215 Houbolt Rd., Joliet, IL 60431-8938.

RFPs not submitted in the format as instructed by this RFP will not be accepted. Addendums to this RFP, once filed, may be submitted in a sealed envelope only, and properly identified prior to the opening hour.

Receipt of RFP / Late RFP: Sealed RFPs shall be received at the place and until the time indicated in this RFP. It is the sole responsibility of the vendors to ensure timely delivery of the RFP. JJC will not be responsible for failure of service on the part of the U.S. Postal Service, courier companies, or any other form of delivery service chosen by the vendor.

RFPs received after the date and time specified shall be considered LATE, and shall not be opened.

Accuracy of Proposals / Withdrawal of Proposals prior to RFP Opening: Proposals will represent a true and correct statement and shall contain no cause for claim of omission or error. Proposals may be withdrawn in writing or by facsimile (provided that the facsimile is signed and dated by vendor's authorized representative) at any time prior to the opening hour. However, no proposal may be withdrawn for a period of one hundred twenty (120) days subsequent to the opening of the RFP without the prior written approval of the Director of Business and Auxiliary Services or Joliet Junior College.

ADDENDA: The only method by which any requirement of this solicitation may be modified is by written addendum.

PROPOSAL DUE DATE: The proposal must be received on or before **2:00 p.m. October 28, 2014** at the Business and Auxiliary Services Department, Campus Center, Room A3100, 1215 Houbolt Rd., Joliet, IL 60431-8938

INSURANCE:
The supplier performing services for JJC shall:

Maintain worker's compensation insurance as required by Illinois statutes, for all employees engaged in the work.

Maintain commercial liability, bodily injury and property damage insurance against any claim(s), which might occur in carrying out the services, referenced in this RFP. Minimum coverage will be **ONE MILLION DOLLARS ($1,000,000)** liability for bodily injury and property damage including product liability and completed operations.

Provide motor vehicle insurance for all owned, non-owned and hired vehicles that are used in carrying out the services described in this RFP. Minimum coverage shall be **ONE MILLION DOLLARS ($1,000,000)** per occurrence combined single limit for automobile liability and property damage.

Maintain umbrella liability coverage OF ONE MILLION DOLLARS ($1,000,000).

Maintain professional liability insurance of $1,000,000 for each claim/loss, bodily injury and which might occur in carrying out the services, referenced in this RFP.

Joliet Junior College, its affiliated organizations, successors, or assignees, its officials, trustees, employees, agents, and volunteers shall be named as additional insureds with respect to liability arising out of the activities performed by, or on behalf of, the Contractor.

TAXES:

JJC is exempt from all federal excise, state and local taxes unless otherwise stated in this document. In the event taxes are imposed on the services purchased, JJC will not be responsible for payment of the taxes. The supplier shall absorb the taxes entirely. Upon request, JJC's Tax Exemption Certificate will be furnished.

INDEMNIFICATION:

The supplier shall protect, indemnify and hold JJC harmless against any liability claims and costs of whatsoever kind and nature for injury to or death of any person or persons and for loss or damage to any property occurring in connection with or in any incident to or arising out of occupancy, use, service, operations or performance of work in connection with the contract, resulting in whole or in part from the negligent acts or omissions of the supplier.

DISCLOSURE:

Vendor shall note any and all relationships that might be a conflict of interest and include such information with the bid.

TERM OF CONTRACT:

Any contract, which results from this RFP, shall be for a period of one year from the date of the contract award. Assuming continued availability of funding; JJC may, at its sole option and with the consent of the supplier renew the contract for up to an additional four (4) one-year terms.

BLACKOUT PERIOD:

After the College has advertised for proposals, no pre-proposal vendor shall contact any College officer(s) or employee(s) involved in the solicitation process, except for interpretation of specifications, clarification of bid submission requirements or any information pertaining to prebid conferences. Such vendors making such request shall email Janice Reedus, Director of Business & Auxiliary Services, at purchasing@jjc.edu No vendor shall visit or contact any College officers or an employee until after the proposal is awarded, except in those instances when site inspection is a prerequisite for the submission of a proposal. During the black-out period, any such visitation, solicitation or sales call by any representative of a prospective vendor in violation of this provision may cause the disqualification of such bidder's response.

IV. GENERAL TERMS AND CONDITIONS

Applicability: These general terms and conditions will be observed in preparing the proposal to be submitted.

Purchase: After execution of the contract, purchases will be put into effect by means of purchase orders or suitable contract documents executed by the Director of Business and Auxiliary Services.

Right to Cancel: JJC may cancel contracts resulting from this RFP at any time for a breach of any contractual obligation by providing the contractor with thirty-calendar days written notice of such cancellation. Should JJC exercise its right to cancel, such cancellation shall become effective on the date as specified in the notice to cancel.

Governing Law and Venue: This contract shall be construed in and governed under and by the laws of the State of Illinois. Any actions or remedies pursued by either party shall be pursued in the State and Federal Courts of Will County, Illinois, only after Alternate Dispute resolution (ADR) has been exhausted.

Dispute Resolution: JJC and the contractor shall attempt to resolve any controversy or claim arising from any contractual matter by mediation. The parties will agree on a mediator and shall share in the mediation costs equally.

Costs: All costs directly or indirectly related to preparation of a response or oral presentation, if any, required to supplement and/or clarify a proposal shall be the sole responsibility of and shall be borne by the vendor.

Proprietary Information: Vendor should be aware that the contents of all submitted proposals are subject to public review and will be subject to the Illinois Freedom of Information Act. All information submitted with your proposal will be considered public information unless vendor

identifies all proprietary information in the proposal by clearly marking on the top of each page so considered, "Proprietary Information." The Illinois Attorney General shall make a final determination of what constitutes proprietary information or trade secrets.
While JJC will endeavor to maintain all submitted information deemed proprietary within JJC, JJC will not be liable for the release of such information.

Negotiation: JJC reserves the right to negotiate all elements, which comprise the vendor's proposal to ensure the best possible consideration, be afforded to all concerned. JJC further reserves the right to waive any and all minor irregularities in the proposal, waive any defect, and/or reject any and all proposals, and to seek new proposals when such an action would be deemed in the best interest of JJC.

Award: The successful vendor, as determined by JJC, shall be required to execute a contract for the furnishing of all services and other deliverables required for successful completion of the proposed project. The supplier may not assign, sell, or otherwise transfer its interest in the contract award or any part thereof without written permission from JJC.

Retention of Documentation: All proposal materials and supporting documentation that is submitted in response to this proposal becomes the permanent property of JJC.

Opening of Proposals: Proposals will be opened in a manner that avoids disclosure of the contents to competing vendors. Contents for proposals will remain confidential during the negotiations period. Only the proposal number and the identity of the vendor submitting the proposal response will be made available to the public.

The College reserves the right to:

- Reject any or all offers and discontinue this RFP process without obligation or liability to any potential Vendor,
- Accept other than the lowest priced offer,
- Award a contract on the basis of initial offers received, without discussions or requests for best and final offers, and

V. FORMAT FOR RESPONSE

To achieve a uniform review process and obtain the maximum degree of comparability, it is required that the proposal be organized in the format specified.

An original and eight (8) copies of the proposal will be required. Each shall be submitted in a binder. The original copy should be so noted and signed along with a digital copy (PDF).

1. **Title Page**

   Show the RFP subject, the name of the vendor's firm, address, telephone number, name of contact person, and date.

2. Table of Contents

Clearly identify the materials by sections and page number(s).

3. Letter of Transmittal

Limit to one or two pages.

a. Briefly state the vendor's understanding of the scope of services to be provided and make a commitment to provide the services within the time period.
b. List the names of the persons who will be authorized to make representations for the vendor, their titles, address, and telephone numbers.

4. Profile of the Vendor

A corporate profile of their firm outlining its history, philosophy and target market; including office location(s), contact numbers.

a. Provide a list of the vendor's top ten current and prior two-year clients indicating the type of services the organization has performed for each client.
b. Submit independently audited financial statements (one copy only). Such information will be considered in strict confidence.
c. Indicate any third-party firms involved with your program and state their role(s).
d. Provide a complete listing of all key personnel who will be assigned to this project. This will include their relevant experience, qualifications for this project, roles and responsibilities, leadership, etc., in addition to the percentage of their time that will be dedicated to this process.

5. References

a. Provide accurate contact names and phone numbers of references.
b. References should be capable of speaking to a firm's capability in performing the services required.

6. Scope Section

Clearly describe the scope of services to be provided based upon the information in the scope section. Respond to each item listed including the expected outcome and benefits to the College.

Provide a detailed schedule of all activities, including milestones, project meetings, interim reports and progress reports required for this project.

7. Responses to Addendum

8. Prices Responses

Provision of a priced methodology complete with a time allotment and cost for each phase (each identified task you propose to employ) to carry out the work.

9. Invoicing Procedure

a. Describe the firm's invoicing procedures.
b. Include documentation identifying all of the vendor's fees.

10. Pro forma Contract

The terms and conditions included in the *Pro forma* Contract apply to any contract resulting from this RFP. In this section of your proposal state any clarifications to the proposed document and your reasons for clarifications. No exceptions are allowed. However, alternative suggestions are encouraged. Please list any alternative suggestions for improvement in costs and/or services provided as an alternative.

11. Bidder's Certification Statement

VI. EVALUATION

In evaluating the proposals submitted, JJC will apply the "Best Value" standard in selecting the supplier to be awarded a contract for this project. Purchase price is not the only criteria that will be used in the evaluation process. Any award resulting from this RFP will be made to that vendor whose offer conforms to the RFP and it is determined to be the most advantageous, of "best value" to JJC, in the sole judgment of JJC. The selection process will include, but not be limited to, the following considerations:

1. The provider's ability to assist JJC in meeting the overall goals of project.
2. The quality and range of services the firm proposes to provide.
3. The extent to which the goods or services meet JJC needs.

4. The firm's overall experience, reputation, expertise, stability and financial responsibility.
5. Feedback from references provided by the vendor.
6. The vendor's past relationship with JJC, if any.
7. The experience and qualifications of the staff that will be assigned to service JJC's account.
7 The ability to provide service in an expedient and efficient manner.
8. Vendor's financial terms offered to JJC.
9. The training options available.
10. The total, long-term cost to JJC to acquire the service.

11. Any other relevant factor that a private business entity would consider in selecting a supplier.

SCOPE OF WORK

Joliet Junior College (JJC) invites your firm to participate in a Request for Proposal (RFP) to acquire an Enterprise Password Management Solution to continue to improve student, faculty, and employee on-site and online experience. The objective of this RFP is to provide the College with qualified proponents capable of carrying out the work herein defined. The subsequent proponent submissions will form the basis for evaluation, interview and selection. The information that should be included in your response is outlined later in this request.

General

The JJC Information Security Office (JJC-ISO) is seeking a vendor to provide an Enterprise Password Management Solution. As part of the proposed solution, implementation services may be necessary and can be proposed as part of the solution.

JJC-ISO has identified the need for an enterprise password management solution for several reasons.

- Currently, JJC is using multiple systems, applications, and password repositories, making compliance and auditing difficult.
- Second, JJC's current password management processes are no longer sufficient or aligned with JJC's technology. They rely on manual processes and user communication channels that are not easily scalable.
- Finally, the JJC-ISO has found the need to control access to IT Admin critical passwords in one centralized, web-based repository which offers permissioned users secure access to passwords and other privileged information. The JJC-ISO would like to provide IT personnel:
    1. The ability to create, share and manage enterprise passwords. Assign user permissions at any level, and track password usage with full audit reports.
    2. Notifications in real time when network passwords are changed and customize alerts.
    3. The possibility for two-factor authentication when logging into mission critical systems.

The College has identified the following criteria for a new enterprise password management solution:

Web Application for Password Change

The password management solution must meet the following web application criteria:

- Provide a web interface for all users to interact with the system. The web interface should not require plugins or additional software, use secure connections for all user activity, and support mobile devices for self-service functions.
- The web application should support all major browsers, including but not limited to prevalent versions of Microsoft Internet Explorer, Apple Safari, Google Chrome, Mozilla Firefox, and work regardless of operating system.
- The solution must also support access via mobile devices and tablets.

- The solution must be able to integrate with JJC's single sign on infrastructure (MS-ADFS). The vendor should describe how they have integrated with this solution in the past both in terms of password-change workflows and being an SSO protected system.
- The solution must be able to work over a geographically dispersed user population, and support low bandwidth connections.
- The solution must be configurable to use JJC's style guides for branding, color schemes, and logos. JJC would prefer to not display details on the product name.

Password Quality Enforcement

The solution must support a self-service password reset/recovery process. Provide detail as to how the solution meets the following:

- Enable JJC to meet all relevant federal, state, and College password procedure requirements around password quality, re-use, and expiration.
- Enforce a minimum and maximum configurable password length. JJC currently requires a minimum length of 8 characters and a maximum of 16 characters.
- Capability to warn users before their password will expire via email or other alert mechanisms.
- Capability to issue pre-expired or temporary passwords in the event of a reset, meaning a user must change a system supplied password at their first login.
- Configurable to require complex passwords. JJC currently requires that passwords must contain a mix of alphanumeric and special characters, mixed case, and must contain at least one of each character type (alpha (upper or lower case) , number (0 thru 9) and special (No spaces allowed)).
- Configurable to prohibit certain password characteristics. JJC requires that passwords must not contain spaces or blanks, contain more than two consecutive identical characters, or cannot contain any portion of a user's first, last or login name.
- Configurable to prohibit commonly used passwords, or patterns, or the use of common terms that could be exploited via a dictionary-style attack (e.g., passw0rd as a commonly used password, password123 as a commonly used pattern, baseball as an uncommon but dictionary-discoverable password).
- Ability to assign different password policies based on a user's primary role/affiliation with JJC. For example: require staff passwords to expire every 90 days, and students, faculty, and alumni to expire every 180 days.
- Ability to lock an account after 6 consecutive recovery failures, and notify the user and JJC IT personnel via email or another alert mechanism.
- Ability to disable, flag, or report on accounts that have 180 days of inactivity.

Password Synchronization

Provide detail as to how the solution meets the following:

- The ability to publish password changes to multiple resources (UNIX AIX, Active Directory (preferably ADFS), People Admin (hosted), O365 (hosted)). Vendors should supply a list of identity connectors supported.
- The ability to be integrated with a Microsoft SharePoint Enterprise Portal and/or a LMS (e.g., Instructure Canvas) to allow a user to change his/her password from a portal interface.

Self-Service Password Reset/Recovery

Provide detail as to how the solution meets the following:

- Support a self-service password reset/recovery process. This process must be able to support password reset/recovery for all JJC students, faculty, staff, and alumni on and off-site.
- Use challenge questions, one-time tokens or other mechanisms to support the recovery process, provided they meet the other technical requirements.
- Detect and prevent various password cracking routines, including dictionary attacks, brute force attacks, or other mechanisms.
- Temporarily lock an account based on a configurable number of failed recovery attempts and notify administrators.
- Solution for users to repudiate a recovery by an unauthorized person.
- Recover a username/user ID.

Administrative Password Reset

Provide detail as to how the solution meets the following:

- Support a help-desk style account reset process.
- Provide an administrative role that allows appropriate personnel to reset a user password.
- Log all administrator/help desk activity.
- Have an ability to initiate a password reset from an external application, such as a ticketing/help desk management solution. JJC uses Microsoft SCSM for contact and issue management.

Password History/Audit/Security

The Password Management Solution will be a key component of JJC's security compliance infrastructure. It must provide history and audit reporting capabilities such as the ability to trace user password events and to enforce relevant password policies.

Provide detail on the ability to report the following metrics:

- Number of password change requests per hour, day, week and month
- Number of forgotten password change requests per hour, day, week and month
- Number of administrative password resets per hour, day, week, and month
- Number of unsuccessful password resets per hour, day, week and month
- A log of any and all password change activities, including:
    - Date of change
    - Time of change
    - Username of user (person, help desk personnel or administrator) who initiated the change
    - Session information including IP address, machine name, browser type and any other relevant information
- Number of users enrolled in the application
- Names of all users and number of users assigned the administrator or help desk roles

The vendor solution must be hosted in a secure environment, see Appendix A regarding security requirements. The vendor must respond to this information security third party assessment questionnaire and submit in the Proposal.

Software-as-a-Service

JJC desires a solution that does not require an onsite installation (Software-as-a-Service model). Any on premise components must be self-contained and not require any additionally licensed software or hardware. The vendor should detail whether or not the solution is available via a Software-as-a-Service (SaaS) or hosted model.

Password Management Enrollment

The solution must provide an enrollment capability to allow JJC users with valid passwords in the Enterprise LDAP (or ADFS) to establish their challenge questions. The enrollment procedure will depend on the solution chosen, and the vendor should provide details and a project methodology for enrolling users. In addition, describe a typical/sample implementation project, including level of effort, typical customer vs. vendor responsibilities, and timelines.

Automated Account Provisioning/De-Provisioning

The solution should provide capabilities to perform account provisioning in JJC systems.

JJC currently has homegrown automated provisioning processes that use data in our ERP (HR and Student Information System) to create accounts across our enterprise applications through Microsoft FIM. While JJC does not intend to immediately leverage functionality in the solution to re-engineer or replace its existing processes, the vendor should describe capabilities in the solution around automated provisioning, de-provisioning, and target systems supported for future use.

Ideally, the password management capabilities requested will be part of a comprehensive identity management solution.

Describe any account provisioning/de-provisioning capabilities in the product, either delivered or via additional licensing, including:

- The ability to integrate with multiple sources of data including Student Information, HR, CRM, and LMS entry points,
- The ability to manage a typical Higher Education student lifecycle from prospective student to alumnus,
- Source and target systems supported,
- Custom configuration, including roles, groups, account policies,
- Custom integration capabilities, ideally via web services for different events in the account provisioning lifecycle.
- The ability to deliver password management and identity management modularly or iteratively
- Account management should not be a required precursor for JJC to implement password management.

Implementation Services

If available by your firm, provide a proposed implementation timeline, level of effort and approach. If not available by your firm, provide a listing of possible implementation partners that you have worked with in the past that have experience with similar projects.

References

Specifically, provide references where Password Management technology is implemented in a cloud/SaaS model, preferably for higher education customers. Please include name, title, role on the contract, phone number (including area code and extension numbers) and e-mail address. Proposers are to provide this information as part of the proposal. JJC reserves the right to verify all information given if it so chooses, as well as, to check any other sources available.

The contact person should be capable of speaking to a firm's capability in performing the services required.

It is imperative that the contact names and phone numbers given for the contracts/clients listed are accurate.

References will be held in the strictest of confidence by the College.

QUANTITY

There is no guaranteed amount of services intended either expressly or implied, to be purchased or, contracted for by JJC. However the supplier awarded the contract shall furnish all required services to JJC at the stated price, when and if required.

JJC reserves the right to purchase one or more phases of the offering depending on cost and budget constraints.

OPTIONS

JJC will consider all proposals that adhere to commonly accepted best practices for Enterprise Password Management even if they deviate from the stated scope of services described in this RFP. The vendor is encouraged to provide technical and pricing information for any options or alternate services that will provide the College the same or a better grade of services.

PROPOSED PRICING

The vendor should furnish a list of proposed prices for all services and materials to be used during the term of the contract. The list of proposed prices should be structured to allow for the calculation of unit cost analyses. The prices included herein are to be firm through the contract term, unless noted otherwise by the vendor.

.

JOLIET JUNIOR COLLEGE
1901

CERTIFICATION OF CONTRACT/BIDDER

The below signed contractor/bidder hereby certifies that it is not barred from bidding on this or any other contract due to any violation of either Section 33E-3 or 33E-4 of Article 33E, Public Contracts, of the Illinois Criminal Code of 1961, as amended. This certification is required by Public Act 85-1295. This Act relates to interference with public contracting, bid rigging and rotating, kickbacks and bribery.

_____
SIGNATURE OF CONTRACTOR/BIDDER

_____
TITLE

_____
DATE

THIS FORM **MUST** BE RETURNED WITH YOUR BID TO:

Joliet Junior College District #525
Director of Business & Auxiliary Services, H-1019
1215 Houbolt Road
Joliet IL 60431

JOLIET JUNIOR COLLEGE
1901

APPENDIX A

JJC INFORMATION SECURITY THIRD-PARTY ASSESSMENT QUESTIONNAIRE

NOTE: Prior to finalizing business agreements involving confidential data, this completed form should be submitted with Vendor's RFP response to JJC's Request for Proposal #R14013 for an Enterprise Password Management Solution.

Third-Party Provider

Name: _____ Date: _____

Address: _____

Website: _____

IT Security Contact: _____Email:_____

Phone: _____

Location of Data Center: _____Contact:_____

Phone: _____

Location of Recovery Center: _____Contact:_____

Phone: _____

JJC Sponsoring Dept.: _Information Security Office _____Contact: Armando D'Onorio, CISO__

Phone: __815-280-2689_____

Description of Service/Product: _____

Users of the System: _____

Technical Description (client, agent, SSL, SFTP transmission, hosted website, ASP, etc.):

_____

_____

_____

Describe Pertinent Outsourced/Contracted Service Arrangements: (such as: onsite support, remote support, temporary access, database management, etc.):

_____

_____

_____

_____

DATA REQUIREMENTS

A. Company Information. The vendor:

Answer (0, 1, 2, or 3)	Question:	Comment:
	1. Will accommodate an onsite visit for a security audit within 24 hours' notice.	
	2. Will store all JJC confidential data within US - incl. backups.	
	3. Maintains an audit log for the location of all JJC confidential data and their backups, to identify where it is located at any point in time, in order to address privacy laws for storage within United States	
	4. Will not access JJC confidential data from outside of United States.	
	Total Company Controls	

Answer: 0 = Not Applicable, based on service provided; 1 = Yes; 2 = Partially; 3 = No
Comments: are optional, but may be used to explain answers.

B. Policies, Standards and Procedures. The vendor:

Answer (0, 1, 2, or 3)	Question:	Comment:
	1. Has formal written Information Security Policies?	
	2. Will provide copies of their Information Security Policies?	
	3. Can provide summary results of a 3rd-party external Information Security assessment conducted w/in the past 2 years (Pen-test, vulnerability assess. etc.)?	
	4. Maintains incident response procedures?	
	5. Has a policy to protect client information against unauthorized access; whether stored, printed, spoken or transmitted?	
	6. Has a policy that prohibits sharing of individual accounts and passwords?	
	7. Has a policy that implements the following Information Security concepts: need to know, least privilege and checks and balances?	
	8. Requires system administrators to be educated and qualified?	
	9. Implements AAA (Authentication, Authorization, and Accounting) for all users?	
	10. Performs background checks for individuals handling confidential information?	
	11. Has termination or job transfer procedures that immediately protect unauthorized access to information?	
	12. Provides customer support w\ escalation procedures?	
	13. Has documented change control processes?	
	14. Requires contractors, subcontractors, vendors, outsourcing ventures, or other external third-party contracts to comply with policies and customer agreements?	
	15. Has a policy that implements federal and state regulatory requirements?	
	16. Maintains a routine user Information Security awareness program?	
	17. Has a formal routine Information Security risk management program for risk assessments and risk management?	
	Total Policy, Standards and Procedure Controls	

Answer: 0 = Not Applicable, based on service provided; 1 = Yes; 2 = Partially; 3 = No
Comments: are optional, but may be used to explain answers.

C. Architecture. The vendor:

Answer (0, 1, 2, or 3)	Question:	Comment:
	1. Will provide a network topology diagram/design?	
	2. Implements network firewall protection?	
	3. Implements web application firewall protection?	
	4. Implements host firewall protection?	
	5. Maintains routers and ACLs?	
	6. Provides network redundancy?	
	7. Has IDS/IPS technology implemented?	
	8. Uses DMZ architecture for Internet systems?	
	9. Adheres to the practice that web applications, which "face the Internet", are on a server different from the one that contains the database?	
	10. Uses enterprise virus protection on all systems?	
	11. Follows a program of enterprise patch management?	
	12. Provides dedicated customer servers to segregate JJC data from other customer data. If not then how is this accomplished in a secure virtual or segmented configuration?	
	13. Implements controls to restrict access to JJC data from other customers?	
	14. Ensures that remote access is only possible over secure connections?	
	15. Uses separate physical and logical development, test and production environments and databases?	
	16. Secures development and test environments using, at a minimum, equivalent security controls as the production environment?	
	17. Will provide the architectural software solution design with security controls?	
	18. Has managed, secure access points on its wireless network?	
	Total Architecture Controls	

Answer: 0 = Not Applicable, based on service provided; 1 = Yes; 2 = Partially; 3 = No
Comments: are optional, but may be used to explain answers.

D. Configurations. The vendor:

Answer (0, 1, 2, or 3)	Question:	Comment:
	1. Implements encryption for confidential information being transmitted on external or Internet connections with a strength of at least AES 256 bit or uses TLS 1.0, preferably TLS 1.1.	
	2. Implements encryption for confidential information at rest with a strength of at least AES 256 bit.	
	3. Has password-protected screen savers that activate automatically to prevent unauthorized access when idle, for computers used by system's support users.	
	4. Removes all unnecessary services from computers.	
	5. Uses file integrity monitoring software on servers (such as tripwire, etc.).	
	6. Changes or disables all vendor-supplied default passwords or similar "published" access codes for all installed operating systems, database management systems, network devices, application packages, and any other commercially produced IT products.	
	7. Uses passwords that are a min. of 8 characters, expire at least annually and have complexity requirements.	
	8. Ensures that passwords are never stored in clear text or are easily decipherable.	
	9. Checks all systems and software to determine whether appropriate security settings are enabled.	
	10. Manages file and directory permissions following least privilege and need-to-know practices.	
	11. Implements redundancy or high availability for critical functions.	
	12. Authenticates all user access with either a password, token or biometrics.	
	13. Formally approves, tests and logs all system changes.	
	14. Sets the account lockout feature for successive failed logon attempts on all system's support computers.	
	15. Prohibits split tunneling when connecting to customer networks.	
	Total Configuration Controls	

Answer: 0 = Not Applicable, based on service provided; 1 = Yes; 2 = Partially; 3 = No
Comments: are optional, but may be used to explain answers.

E. Product Design. The vendor:

Answer (0, 1, 2, or 3)	Question:	Comment:
	1. Ensures that if the product integrates with portable devices, confidential information is encrypted when stored on these portable devices and requires password access.	
	2. Ensures that access to confidential information, across a public connection, is encrypted with a secured connection and requires user authentication.	
	3. Implements protections for Common Vulnerabilities and Exposures (CVEs) in a timely manner to protect from exploits.	
	4. Audits the application against the OWASP Top 10 Application Security Risks.	
	5. Ensures that application server and database software technologies are kept up-to-date with the latest security patches.	
	6. Uses threat modeling in their software development lifecycle (SDLC).	
	7. Performs security code reviews as part of their SDLC.	
	8. Conducts OWASP code reviews for the Top 9 source code flaw categories as part of their SDLC.	
	Total Product Design Controls	

Answer: 0 = Not Applicable, based on service provided; 1 = Yes; 2 = Partially; 3 = No
Comments: are optional, but may be used to explain answers.

F. Compliance. The vendor:

Answer (0, 1, 2, or 3)	Question:	Comment:
	1. Will provide relevant certificates of applicable ISO 27001 certification?	
	2. Can provide documentation that its product is HIPAA compliant, if the vendor manages any PHI on behalf of JJC?	
	3. Can provide documentation of its PCI-DSS compliance if the vendor manages any payment card information?	
	4. Uses industry standard best practices for application security (e.g. OWASP)?	
	Total Compliance Controls	

Answer: 0 = Not Applicable, based on service provided; 1 = Yes; 2 = Partially; 3 = No
Comments: are optional, but may be used to explain answers.

G. Access Control. The vendor:

Answer (0, 1, 2, or 3)	Question:	Comment:
	1. Immediately removes, or modifies access, when personnel terminate, transfer, or change job functions.	
	2. Achieves individual accountability by assigning unique IDs and prohibiting password sharing.	
	3. Ensures that critical data, or systems, are accessible by at least two trusted and authorized individuals, in order to limit having a single point of service failure.	
	4. Ensures that users have the authority to only read or modify those programs, or data, which are needed to perform their duties.	
	Total Access Controls	

Answer: 0 = Not Applicable, based on service provided; 1 = Yes; 2 = Partially; 3 = No
Comments: are optional, but may be used to explain answers.

H. Monitoring. The vendor:

Answer (0, 1, 2, or 3)	Question:	Comment:
	1. Reviews access permissions monthly for all server files, databases, applications, etc.	
	2. Implements system event logging on all servers and records at a minimum who, what, and when for all transactions.	
	3. Reviews and analyzes after hours system accesses, at least monthly.	
	4. Reviews system logs for failed logins, or failed access attempts monthly.	
	5. Reviews and removes dormant accounts on systems at least monthly.	
	6. Reviews web server logs weekly for possible intrusion attempts and daily for significant changes in log file size as an indicator of compromise.	
	7. Reviews network and firewall logs at least monthly.	
	8. Reviews wireless access logs at least monthly.	
	9. Performs scanning for rogue access points at least quarterly.	
	10. Actively manages IDS/IPS systems and alert notifications have been implemented.	

	11. Performs vulnerability scanning at least yearly?	
	12. Performs penetration testing at least annually, if the vendor manages any PHI on behalf of JJC.	
	13. Checks routinely that password complexity is adhered to.	
	Total Monitoring Controls	

Answer: 0 = Not Applicable, based on service provided; 1 = Yes; 2 = Partially; 3 = No
Comments: are optional, but may be used to explain answers.

I. Physical Security. The vendor:

Answer (0, 1, 2, or 3)	Question:	Comment:
	1. Controls access to secure areas. e.g., key distribution management (both physical and electronic), paper/electronic logs, monitoring of facility doors, etc.	
	2. Controls access to server rooms and follows least privilege and need-to-know practices for those facilities.	
	3. Has special safeguards in place for computer rooms. e.g., cipher locks, restricted access, room access log, card swipe access control, etc.	
	4. Shreds or incinerates printed confidential information.	
	5. Prohibits or encrypts confidential information on laptops & mobile devices.	
	6. Positions desktops, which display confidential information, in order to protect from unauthorized viewing.	
	7. Escorts all visitors in computer rooms or server areas.	
	8. Implements appropriate environmental controls, where possible, to manage equipment risks, e.g., fire safety, temperature, humidity, battery backup, etc.	
	9. Has no external signage indicating the content or value of the server room or any room containing confidential customer information.	
	10. Provides an export copy of all of the customer's data in a mutually agreed upon format at the end of the contract.	
	11. Follows forensically secure data destruction processes for confidential data on hard drives, tapes & removable media when it's no longer needed and at the end of the contract term.	
	Total Physical Security Controls	

Answer: 0 = Not Applicable, based on service provided; 1 = Yes; 2 = Partially; 3 = No
Comments: are optional, but may be used to explain answers.

J. Contingency. The vendor:

Answer (0, 1, 2, or 3)	Question:	Comment:
	1. Has a written contingency plan for mission critical computing operations?	
	2. Has emergency procedures and responsibilities documented and stored securely at multiple sites?	
	3. Reviews and updates the contingency plan at least annually?	
	4. Has identified computing services that must be provided within specified critical timeframes, in case of a disaster?	
	5. Has identified cross-functional dependencies, so as to determine how the failure in one system may negatively impact another one?	
	6. Has written backup procedures and processes?	
	7. Tests the integrity of backup media quarterly?	
	8. Stores backup media in a secure manner and controls access?	
	9. Maintains a documented and tested disaster recovery plan?	
	10. Uses off-site storage and has documented retrieval procedures for backups.	
	11. Password protects and encrypts all backups.	
	12. Provides rapid access to backup data.	
	13. Labels backup media appropriately, to avoid errors or data exposure.	
	Total Contingency Controls	

Answer: 0 = Not Applicable, based on service provided; 1 = Yes; 2 = Partially; 3 = No
Comments: are optional, but may be used to explain answers.

K. Vendor's Business Associates. The vendor:

Answer (0, 1, 2, or 3)	Question:	Comment:
	1. Has confidentiality agreements that have been signed before proprietary and/or confidential information is disclosed to the vendor's business associates?	
	2. Has vendor's business associate contracts, or agreements, that are in place and contain appropriate risk coverage for customer requirements?	
	3. Has made vendor's business associates aware of customer security policies and what is required of them?	
	4. Has vendor's business associate agreements that document the agreed transfer of customer's data when the relationship terminates?	

	Total Business Relationships Controls	

Answer: 0 = Not Applicable, based on service provided; 1 = Yes; 2 = Partially; 3 = No
Comments: are optional, but may be used to explain answers.

Third-Party Controls

_____ A. Company Information Controls

_____ B. Policy, Standards and Procedure Controls

_____ C. Architecture Controls

_____ D. Configuration Controls

_____ E. Product Design Controls

_____ F. Compliance Controls

_____ G. Access Controls

_____ H. Monitoring Controls

_____ I. Physical Security Controls

_____ J. Contingency Controls

_____ K. Business Relationships Controls

_____ TOTAL THIRD-PARTY CONTROLS