CASTLETON UNIVERSITY
COMMUNITY COLLEGE OF VERMONT
JOHNSON STATE COLLEGE
LYNDON STATE COLLEGE
VERMONT TECHNICAL COLLEGE

VERMONT
STATE COLLEGES SYSTEM

OFFICE OF THE CHANCELLOR
PO BOX 7
MONTPELIER, VT 05601
P (802) 224-3000
F (802) 224-3035

Vermont State Colleges System
Request for Proposals
Human Capital Management System
March 5, 2018

Proposals due:
April 13, 2018
12:00pm ET

1.0 Organizational History

1.1 General Information

The Vermont State Colleges (VSCS) is Vermont's system of public higher education. The colleges are located throughout Vermont and include five institutions:

- Castleton University
- Community College of Vermont
- Vermont Technical College
- Northern Vermont University (The unification of Johnson and Lyndon State Colleges)

Together the colleges enroll more than 12,000 students of all ages and backgrounds; students come from Vermont, the U.S., and around the world. The colleges offer more than 125 academic programs at the associate, baccalaureate, and master levels. All offer small classes and individualized attention for students. As of November 2017, VSCS has combined employment count of 979 Full-Time employees and 1147 Part-Time employees.

1.2 Mission Statement

For the benefit of Vermont, the Vermont State Colleges System provides affordable, high quality, student-centered and accessible education, fully integrating professional, liberal, and career study.

This integrated education, in conjunction with applied learning experiences, assures that graduates of VSCS programs will:

1. Demonstrate competence in communication, research and critical thinking;
2. Practice creative problem-solving both individually and collaboratively;
3. Be engaged, effective, and responsible citizens;
4. Bring to the workplace appropriate skills and an appreciation of work quality and ethics;
5. Embrace the necessity and joy of lifelong learning.

The Vermont State Colleges system provides continuing educational opportunities for individuals to meet their specific goals.

2.0 Introduction

This Request for Proposal (RFP) is issued by Vermont State Colleges System (VSCS) to gather and obtain proposals and cost estimates for replacing the current ERP/Payroll system, a module in Colleague, to an online cloud-based solution, adding modular components to better automate and manage HR/Payroll processes throughout the system. The expectation is to be transformative to a modern, secure, innovative and efficient HCM system.

In addition to providing the software functionality identified in section 3.1, VSCS is expecting the vendor's proposal to provide professional services to ensure a successful implementation. The professional services should include at a minimum the following:

- Project Management
- Software Installation and Configuration
- Implementation Consulting
- Business Process Review and Redesign
- Data Conversion
- Training
- Documentation
- Change Management Consulting

3.0 Requirements

The following is a listing of the key functional requirements for the Human Capital Management System. VSCS will measure individual submissions against these.

3.1 General requirements

3.1.1 Solution must be SaaS, meeting all of the hosting requirements in section 3.2.

3.1.2 **Payroll** features should include but are not limited to: Direct deposit, W2 processing, Tax Filings, Tax Calculations for employees living/working in different states, Online Paystub, Mobile app, and ACA Tracking, Reporting and Filing.

3.1.3 Overtime calculations. System must be programmable with various overtime calculation rules dependent upon Collective Bargaining Agreements, Location and days worked.

3.1.4 Exempt vs. Non-Exempt. Must be able to appropriately track exempt and non-exempt employees (hourly & salary).

3.1.5 Varying methods of calculating and attributing contribution schedules based upon salary, allowing for mid-year adjustments or changes in salary. The contribution schedule can be made available for configuration.

3.1.6 System must allow deduction codes to have a cap/maximum deduction amounts (ex: retirement plans).

3.1.7 Federal & Vermont State tax tables must be available for auto upload into the system, not manual. Additional state tax tables will be needed as well including but not limited to: Arizona, Colorado, Florida, Indiana, Massachusetts, Nebraska, New York, Oregon, Pennsylvania, and Texas.

3.1.8 Vermont Healthcare Assessment form tracking – an included field indicating an employee is covered or uncovered. Also the ability to calculate the amount due and pay in addition to the VT unemployment taxes

3.1.9 Multi-level access. This payroll system must have access for each college payroll professional, only allowing them access to their employees. However, all information must be accessible from the main Chancellor's Office payroll dept. for final payroll run.

3.1.10 System must be able to track hire date based on various factors. Example: Hire date for student worker, then additional hire date if hired as faculty later. System needs to track and display various types of hire (and re-hire) dates.

3.1.11 Termination dates. System must be able to terminate an employee from employment and still keep the employee in the payroll system for 3 months after termination. Tracking of actual employment term date as well as final system term date must be available within system.

3.1.12 System must be able to produce reporting on new hire information for upload to VT DOL, as well as garnishment management, leave management and tax services.

3.1.13 FMLA tracking within the payroll system. Ability to adjust to various state leave statutes such as Vermont Parental and Family Leave (VPFL).

3.1.14 System must be set up on a 7 day work week

3.1.15 System should be capable of allowing exempt employee's to have a standardized work schedule and if there's a need to track actual hours worked without impeding ability to run payroll.

3.1.16 **HRIS** features should include but are not limited to: Job Status/History, Salary Tracking/History, OSHA Tracking, New Hire/On-boarding, Configurable Workflows, Custom Fields, Org Charts, Multiple Manager and Location Security Level access, Employee Self-Service (ESS), and Manager Self Service (MSS)

3.1.17 New Hire/On-boarding: system must be customizable for various Union and Non-Union employee on-boarding processes. If available, customizable on-boarding checklists would be preferable.

3.1.18 I-9 and W-4 upload feature – available for ESS

3.1.19 Retiree Benefit Tracking: system must be able to account for active retirees and any retiree benefit costs to be tracked within the general ledger.

3.1.20 Capable of sending notices and announcements to employees, bulk and individual.

3.1.21 Library with required web-based videos on how to use various ESS functions and systems

3.1.22 Customizable fields for tracking such items as Tuition Waiver Approval

3.1.23 Time & Attendance: ESS for requesting time-off and entering hours worked, including self-attested authorized breaks. MSS for approving time-off requests, approving time/pay, and submission to payroll.

3.1.24 **Recruitment** module features should include but not be limited to: online position posting, online application, applicant tracking, automated data transfer to HRIS/ Employee management system upon hire, stored job descriptions, resume importing, applicant stages/status, and mobile app.

3.1.25 Option to announce/post new job postings across the VSCS campuses.

3.1.26 Option to send job opening announcements and job descriptions to defined contacts

3.1.27 VSCS-wide access to job descriptions by job code/title

3.1.28 Centralized reporting for all campus openings, such as how many open positions across a period of time, which positions are turning over most frequently, etc.

3.1.29 Clear instructions on how the applicant is to apply for vacancies.

3.1.30 Automated notifications to search committee members if an applicant's status changes (interview, pass, hire, etc.)

3.1.31 Auto populate an appointment letter template

3.1.32 Data transfer from applicant files to employee record at time of hire, including demographic data.

3.1.33 **Talent management** features should include but are not limited to: performance review management & tracking, configurable evaluation forms, goal tracking, skill codes/descriptions, core competencies, succession planning, track hours/dates for training, certifications and licenses, online training enrollment, ability to track training costs, course library and mobile app.

3.1.34 **Benefits Administration** features should include but are not limited to: online enrollment, employee education, direct feeds to payroll/HRIS and benefit carriers and vendors, ESS, MSS, and mobile access and functionality.

3.1.35 Income Sensitive Contribution Tables

3.1.36 Customizable benefit class eligibility rules

3.1.37 ESS for new hire enrollment, annual open enrollment, and mid-year life event changes.

3.1.38 System able to capture Healthcare Declaration Form & E-signature for each employee during Open Enrollment, as well as tracking integrated with HRIS system.

3.1.39 Employee education videos, documents, and if needed in the future, plan selection assistance.

3.1.40 Multi-format access: Computer, tablet and mobile devices.

3.1.41 **Data analytics** – the system must be capable of producing a broad range of standard and customizable reports, in all functional areas, including but not limited to payroll, benefits administration, HRIS, recruitment and talent management.

3.2 Hosting requirements - The data center must:

3.2.1 Be a state-of-the-art data center offering secure, redundant facilities;

3.2.2 Have direct access to multiple tier 1 providers;

3.2.3 Have documented high availability uptime;

3.2.4 Have redundant core network, including firewall and load balancers;

3.2.5 Have on-site engineers to provide premier support 24 hours a day, 365 days a year;

3.2.6 Use secure facilities with redundant utilities and electronic security system restricting access and providing high level physical security.

3.2.7 Have a scalable infrastructure; customer pays according to resources required/used.

3.2.8 Offer the flexibility to customize data, storage and access to client requirements based on Customer needs.

3.2.9 Include active monitoring and application support.

3.2.10 Employ industry standard data protection measures.

3.2.11 Be compliant with current information technology audit requirements.

3.2.12 Have scheduled backup operations conforming to customer needs and frequencies;

3.2.13 Provide customer-required data retention and access;

3.2.14 Have data storage capacity to grow as Customer's data and storage needs expand;

3.2.15 Provide service and support 24x7x365 available to via telephone, email, fax, remote access.

3.2.16 Guarantee problem resolution response and follow-up time thresholds must be in agreement with Customer response needs, to be determined after award.

4.0 Scope of Work

Please include in your response an outline of your proposed statement of work and provide an example of a detailed project work plan from a project of similar size and complexity completed by your company. Identify any VSCS resources that you will require to perform tasks (project management, staff support, etc.).

You must respond to all of the questions listed below, along with detailing how your proposal will meet the requirements of §3. If you are submitting answers electronically in a separate file, please reference the specific numerical section of this list in your answer.

4.1 General

4.1.1 Please provide a brief statement demonstrating your understanding of the work to be performed as part of this RFP, and identify the contact person responsible for communicating on your behalf and who will have authority to execute the contract that will result from the RFP.

4.1.2 Please provide general company background including financial stability, number of employees, number and location of sites (domestic and international), years in business and number of clients.

4.1.3 Please detail your qualifications – why is your company qualified to provide us with this service or product? (in 100 words or less)

4.1.4 Does your company have a specialty within your industry? (in 50 words or less)

4.1.5 Does your company provide other products or services in addition to the proposed solution?

4.2 Solution Components

4.2.1 What components are required for your solution? Please provide a complete and detailed technical and functional description of the services proposed. Include in this section a general description of the product architecture and a detailed explanation of the product as designed and configured for the VSCS.

4.2.2 Please provide a diagram of the product that identifies and illustrates each component to be installed and a complete listing of components.

4.2.3 Please highlight any third party or subcontractor services.

4.3 Implementation

4.3.1 Please provide the resume of the proposed Project Manager and implementation consultant, including references. Implementation consultants should be experienced in higher education application processing. (See note about Project Management below.)

4.3.2 Please provide an implementation task list and timeline including time estimates for your proposed implementation.

4.3.3 Please provide a summary of all implementation services available. What additional implementation services are available with the purchase of your solution?

4.3.4 If the VSCS purchases your product, what is the earliest date we could begin testing the implementation?

4.3.5 Please outline the support you will be offering during the cutover or transition process.

4.4 Training

4.4.1 Please provide a summary of training services available, including costs.
4.4.2 What training services are available with the purchase of your solution? Does the vendor offer on-site training both before "go-live" and ongoing during the length of use? Is there web-based training available?

4.5 Maintenance and Support Services

4.5.1 Please include details on how you will maintain the product, including number and location of staff.
4.5.2 Please outline how you will provide product performance monitoring.
4.5.3 Please outline how you will provide real-time and historical reporting functions that demonstrate conformance to Service Level Agreements that will be negotiated.
4.5.4 Please outline how you will provide alerting capabilities to notify technical staff and others of outages.
4.5.5 What support services are included in your maintenance agreement?
4.5.6 Please provide a summary of optional support services, including costs, for your solution.
4.5.7 Please include a copy of your Service Level Agreements (SLA).
4.5.8 Please include a copy of your support and escalation policies.

4.6 Compliance

4.6.1 The VSCS require that all purchases be compliant with Sections 504 and 508 of the Rehabilitation Act of 1973, as amended, and the Americans with Disabilities Act of 1990, as amended.
4.6.2 Please describe how you will ensure that all interfaces (both for administrators and end users) are fully-accessible and compliant with Section 508 and/or WCAG 2.0 AA.
4.6.3 Please describe how you will comply with the standard Data Security Requirements.

5.0 Qualifications, References and Pricing

5.1 Qualifications and References

Provide a description of the qualifications and experience of your company. Include responses to the specific required items listed below:

Bidder Profile and Qualifications

- Name, mailing address, email address and telephone numbers of company.
- Federal tax identification number.
- Number of years in business. The company must have a minimum of five years of experience in providing the proposed solution.
- Number of employees in Vermont and nationally.
- Number of colleges and universities in which the product is installed and maintained by the bidder, identifying those institutions of similar size and complexity to the VSCS.
- Location of your data center.
- Number of technicians at the data center trained and certified to maintain/install the proposed components.
- List all certifications you hold for the proposed solution.

- Copy of your most recent audited financial statement, annual report, bank references, and all other relevant documentation used by your company to indicate financial stability.
- Describe any functions that you currently outsource as part of your solution delivery and the length of the relationship, including any related-party relationship. The related-party relationship is defined as you (or your principals or officers) having a direct or indirect ownership interest of greater than or equal to three percent of the related party organization.
- Briefly describe your customer service operations including number of customer call instances handled daily, monthly and annually, the average resolution time, average call pick-up time, and any other relevant data that would be helpful in our evaluation of your customer service.

Bidder References

You must demonstrate experience and capability in installation and maintenance of the proposed solution by providing evidence of successfully completing projects of similar size and scope. Please provide a list of customer references, with the following information:

- Customer name and location
- Contact person(s): name, title and telephone number
- Your project manager for the engagement
- Product installation date
- Number of years you have maintained the system
- Any special features or functionality implemented or proposed

You shall provide at least three such references. By submitting your proposal, you understand and agree that the VSCS may make any investigations it deems necessary to determine your ability to perform the work, and you agree to furnish the VSCS all such additional information and data for this purpose as the VSCS may request.

Project Management and Installation Team

In your proposal, you must identify and appoint a competent and experienced Project Manager to act as representative, and to supervise your employees and partners/subcontractors/third party providers during the installation, cutover, and final testing of the product. You are fully responsible for project management, timely delivery and communication with the VSCS of any subcontractors engaged to deliver your solution. The VSCS requires that the Project Manager be on site or available on a regular basis to manage the installation of the solution. VSCS should be given the opportunity to review and approve the proposed project manager, and if the project manager changes during the contract term, VSCS will be given the same opportunity to review and approve the next assigned Project Manager.

You must also identify additional key personnel who shall support the designated Project Manager, and be available to the VSCS in the absence of the designated Project Manager. You must clearly describe escalation procedures available to the VSCS and provide 24/7/365 contact information for all members of the escalation chain, including corporate officers residing outside of Vermont. Once the key project team members have been assigned and accepted, the VSCS will reserve the right to approve any proposed substitutions.

VSCS staff participation is expected to include providing access to facilities as appropriate, providing documentation, attendance at project meetings, and coordination among the VSCS departments and colleges. Your proposal must clearly identify any VSCS resources required.

The VSCS values project management and installation teams with demonstrated experience in all aspects of project management – requirements gathering, system design and configuration, training, testing, quality control, risk assessment, and completing projects on budget and on schedule – in large multi-site, multi-service installations with complex business requirements.

5.2 Pricing

Your proposal should include all of the charges, and it should clearly state the pricing structure along with the types of products and/or services accompanying each price. The VSCS expects fully bundled pricing for each service offered and any tiered pricing or volume purchasing discounts/rebates that maybe available due to purchasing loads.

Please provide all pricing noting any non-reoccurring (NRC) or initial costs, as well as Monthly Reoccurring Costs (MRC). Please break down any components of the NRC or MRC in addition to summarizing them.

5.3 Taxes/Fees

5.3.1 Please note any and all proposed taxes, fees, or charges.

5.3.2 The VSCS is exempt from sales and use taxes. Submitted proposals shall not include these taxes. The College's tax exempt number will be provided to the selected bidder. Please clearly note these exemptions in your proposal.

5.4 Terms

5.4.1 Please provide 36 & 60 month term options on all pricing, unless otherwise noted.

5.4.2 Your proposal—and any resulting agreement—must include VSCS's absolute right to cancel specific services after 60 days written notice without payment of cancellation or termination charges.

5.4.3 Your proposal—and any resulting agreement—must include VSCS's right to add additional locations under existing contract rates without penalties.

6.0 RFP Instructions, Requirements and Information

This section provides information on how to contact the VSCS for questions, deadlines, the selection process, legal and insurance requirements, and other general business matters.

6.1 Questions about this RFP

Please submit your questions to the VSCS on or before Friday, March 23, 2018, at 12:00 noon Eastern Time. All questions will be posted on the VSCS website, www.vsc.edu, and made available to all bidders. The contact information for questions to:

Name	Kevin Conroy
Title	Chief Information Officer, *VSCS*
Telephone number	(802) 224-3016
E-mail address	HRPayRFP@vsc.edu

6.2 Deadline and Delivery

The deadline for submitting responses is 12:00 noon Eastern Time, April 13, 2018. Provide an electronic copy **only, via email,** to:

Name	Kevin Conroy
Title	Chief Information Officer, *VSCS*
Telephone number	(802) 224-3016
E-mail address	HRPayRFP@vsc.edu

6.3 Selection Process

Method of Award

VSCS will base the evaluation of each proposal to this RFP will be based on its demonstrated competence, compliance, format, cost, and enterprise applicability. This includes, but is not limited to, product availability, quality, prices, service availability, timing and delivery. The purpose of this RFP is to identify those vendors having the interest, capability, and financial strength to supply the VSCS with an Integrated Library System. If the VSCS does not identify a suitable bidder within the RFP process, the VSCS is not obligated to award the project to any bidder.

The VSCS, in its best interests, reserves the option to accept or reject any or all proposals, to accept or reject any item or combination of items therein, to waive any irregularities or informalities in any proposal or items therein, and/or to negotiate with particular bidders following the evaluation of proposals without right of recourse by other bidders. A top proposal would be that assessed in the judgment of VSCS as best complying with all considerations set forth in this RFP. When VSCS has tentatively selected a successful proposal, VSCS may engage in discussions with the bidder to formulate plans in greater detail, to clarify unclear items for either party, and to otherwise complete negotiations prior to formal selection.

Evaluation Criteria (no weighting is implied by order of listing):

1. The extent to which the bidder's solution matches the requirements of the VSCS.
2. Engagement methodology.
3. Bidder's qualifications and references.
4. Cost and length of contract.

6.4 Bid Process

Date	Milestone
3/5/18	RFP issue date
3/23/18	Questions due to VSCS
4/6/18	Responses to questions returned
4/13/18	Bidder written proposal due date
4/30/18	Finalists notified
Week of 5/7 through 5/18	Finalist presentations to VSCS
6/8/18	Bidder(s) selected
**TBD	Contract(s) made

** The VSCS will make its best effort to meet these dates but will take the time necessary to make a well-informed decision and negotiate a good contract. Bidders participating in this RFP should expect this date to change. The VSCS will be under no obligation to inform bidders of a change in this date. The VSCS will inform bidders of a change in all other dates that are part of the bid process.

6.5 Intent to Respond

VSCS intends to respond to all candidates submitting an RFP response either by phone or e-mail. A response, whether positive or negative, will be given for each bidder as the selection process eliminates candidates in each round.

6.6 Confidentiality

The Vermont State Colleges comply with the Vermont Public Records Act, 1 VSA § 315 *et seq*. which requires public agencies to allow any person to inspect or copy any public record upon request. Accordingly, bidders are hereby advised that any communications, data or other information received by the Vermont State Colleges during the RFP process could be subject to a public records request. However, certain public records are exempt from public inspection and copying, as set forth in 1 VSA § 317(c), including, for example, those portions of a record which meet the statutory definition of a trade secret. Accordingly, bidders should submit a second copy of their proposal, from which any portion of the proposal that the bidder reasonably believes to be exempt from disclosure under the Public Records Act has been redacted.

By submitting a proposal, you indicate that you understand the requirements of this subsection (6.6) and the potential applicability of Vermont's Public Records Act to your proposal.

6.7 Indemnification

The bidder shall indemnify and hold VSCS, its officers, agents and employees free and harmless from any and all claims, liabilities, losses, actions, proceedings, suits, damages and expenses, including out-of-pocket litigation costs and reasonable legal fees, arising from or relating to the bidder's performance in response to this RFP and under any contract entered into with the successful bidder.

By submitting a proposal, and in exchange for VSCS's consideration of same, you agree on behalf of yourself, your shareholders and your officers to be bound by the indemnification provisions of this subsection (6.7).

6.8 Rights of the VSCS

VSCS reserves the right, at its discretion, to pursue actions that include but are not limited to the following:

- Request additional information
- Request clarification of any sections or questions in the bidder's response to this RFP
- Reject, for any reason, any or all of the proposals submitted to VSCS
- Issue subsequent RFP or RFP invitations to bid as a result of changes and/or refinements to the proposed project

This RFP does not obligate the VSCS to accept any proposal, negotiate with any bidder, award a contract or proceed with the project as it is outlined in this RFP.

6.9 Assignment

The bidder may not assign or transfer its rights or obligations under this RFP without the prior written consent of VSCS, which consent shall not be unreasonably withheld. Any assignment of the RFP agreement by the bidder without the prior written consent of VSCS shall void the RFP response from the bidder.

6.10 Insurance

You shall provide with your proposal, proof of insurance as stated below. In the event you do not carry the maximums requested, you must provide written proof that you will be able to provide the maximums if awarded the contract. You shall secure, pay for and maintain in effect the following insurance during the contract period:

- Commercial General Liability Insurance: Including Bodily Injury and Property Damage Liability, Independent Contractor's Liability, Contractual Liability, Product Liability and Completed Operations Liability in an amount not less than $1,000,000 combined single limit, per occurrence, and $3,000,000 annual aggregate.
- Workers Compensation and Employers Liability Insurance: For any bidders with employees, standard workers' compensation as required by Vermont State statute and employer's liability insurance in an amount not less than $100,000 per accident, $500,000 annual aggregate.
- Automobile Liability: For bidders who will drive on VSCS's premises, Automobile Liability in an amount not less than $1,000,000 per occurrence for bodily injury and property damage, including owned, hired, and non-owned vehicle coverage.
- Professional Liability: $1,000,000 each claim, when applicable.

If selected as the successful bidder, you agree to name the VSCS as additional insured on your liability policies and shall provide a 30-day notice of cancellation or non-renewal of coverage to the VSCS. The VSCS does not need to be named as an additional insured on the workers compensation policy.

If selected as the successful bidder, you agree to submit a copy of the Certificate of Insurance verifying the above coverage levels to the VSCS twenty (20) days prior to selling or distributing products and services at VSCS or otherwise performing under the contract. Any liability coverage on a "claims made" basis shall be designated as such on the certificate.

Failure of the bidder to take out and/or maintain any required insurance shall not relieve the bidder from any liability under the contract, nor shall the insurance requirements be construed to conflict with or otherwise limit the obligation of the bidder concerning indemnification. The bidder's policies shall be considered primary insurance and exclusive of any insurance carried by VSCS.

6.11 Intent to Bid

The undersigned ("You") agrees to all provisions required in the VSCS Human Capital Management RFP dated March 5, 2018 and all applicable addenda, with the exception of those listed below. Any exemptions listed may affect the viability of your proposal.

In addition, the undersigned ("You") agrees to provide all equipment, material and personnel associated with these services as described in the VSCS Human Capital Management RFP dated March 5, 2018, and all applicable addenda.

Exceptions:

Section Reference Number	Reason for exception

Company Name

_____

Signature of Authorized Representative

_____

Print Name of Authorized Representative

_____

Print Title of Authorized Representative

7.0 Appendices

Appendix A – Third Party Data Security Requirements

THIRD PARTY DATA SECURITY REQUIREMENTS

Introduction

The VSC engages in business in which data are being collected, transmitted or stored under contracted third party arrangements. In many of these situations, a web-based system is developed by a third party to collect data on behalf of a VSC operation. The VSC may also send data collected by the VSC for further processing or storage by a contracted third party.

"Third party" is defined as any vendor or entity doing business with or collecting, transmitting or storing data on behalf of the VSC or any of its member colleges. Data can be in electronic or paper formats.

A checklist has been created to assist in risk management, contract review and ongoing third party management, with a goal of minimizing the risk to VSC data.

Section I: Does this security review apply to my giving data to a third party?

If you answer YES to any of the following questions, your project needs security review.

1. Are you transferring private data currently residing on a computer owned by the VSC to a third party?
2. Are you contracting with a third party who will create a website on behalf of the VSC to collect and store private data?
3. Will a contracted third party collect private data that will later be transmitted for use by the VSC?
4. Will a third party process payments on behalf of the VSC?
5. Will a third party have logon access to VSC private data?
6. Are you renewing a contract with a third party that involves data sharing described in items 1-5?

To initiate a third party security review, contact VSC Information Technology Services. Over the course of contracting with any third party, additional security reviews may be required by IT, general counsel, or as part of an audit.

Section II: System Review

The VSC reviews the data security policies and practices of third parties in the context of existing VSC data security policies and practices. This review will be completed by OCIT for system-wide contracts, and by the appropriate college IT department in the case of a product used by only that college. In general, the VSC seeks third party agreements in which data security policies and standards are in alignment with those of the VSC. Third party systems used for the handling, processing or storage of data must be reviewed prior to contractual agreement and prior to contract renewal. Contract review is the responsibility of the VSC general counsel.

The individual or office seeking to provide data to a third party must document data elements to be collected, transmitted or stored (e.g., names, addresses, social security numbers, credit card processing, student data, alumni data, etc.).

IT will review VSC security requirements with the technology staff of any new third parties, using the Third Party Review checklist. This review will be completed by OCIT for enterprise contracts, and by the appropriate college IT department in the case of a product used by only that college.

Section III: Contract Development

Any contract with a third party to collect, transmit or store data shall address the following questions and requirements. Please refer to the sample contract (Data Security Terms for a Contract with an Outside Party) from Catholic University that reflects recent changes to FERPA at http://counsel.cua.edu/ferpa/resources/.

1. **Who will have access to the data?**
   - Data access on the part of the third party will be limited to those with a legitimate need to know and controlled by specific individuals. The third party will have procedures in place to prevent unauthorized access, and the procedures will be documented and available for the VSC to review on request. Those allowed to send data and receive data to and from the third party must be identified.
   - The third party will notify the VSC within four business hours of any incident that threatens the security, confidentiality, integrity, or availability of VSC information. In the event of a security incident, the third party will communicate with the VSC prior to notifying any individuals whose data may have been exposed.
   - Physical access to facilities where data are stored will be limited and controlled. Any damage or any attempted or successful unauthorized access to data storage facilities will be reported to the VSC within four hours of occurrence.
   - Standard non-disclosure language must be included, with guarantees to keep information and data private and confidential, except as may otherwise be provided for in the contract. Data shall not be shared with or sold to other parties without specific authorization by the VSC.

2. **Where will data be stored and how will it be destroyed?**
   - All computers used in the storage, processing, transmittal and display of data will have operating systems that are current in release, with unneeded services disabled, with default administrator access shut off, and with all security patches updated in a timely fashion soon after the release of the patch.
   - Any destruction of data will comply with the VSC Records Retention Policy and applicable state and federal law.

3. What security standards will be implemented?

- All computers and systems on which third parties maintain VSC data will be protected by acceptable industry practices for antivirus, firewalls, and network and system intrusion detection systems.
- Routine event monitoring will be performed by the third party; the VSC expects that the third party will routinely and immediately identify events related to unauthorized activity and unauthorized access.
- The third party will provide documentation of regular security audits and timely correction or mitigation of identified vulnerabilities.
- Websites that gather personal information must utilize Secure Socket Layer (SSL) with a certificate from an independent authority.
- File transmissions must be done using Secure File Transfer Protocol, or another VSC-approved method.

4. What are the disaster recovery and business continuity plans?

- Adequate backups of systems, files and data will be performed so that any restoration of the system will not result in more than 24 hours of data loss.
- The third party shall document that a disaster recovery plan exists, including off-site storage of data in a secure location. The VSC retains the right to reject the location for security reasons.

5. What is the quality of the data?

- The third party must meet VSC expectations for data integrity and accuracy, as set forth in the contract. No data exchanges will occur until the VSC has agreed that data are meeting the VSC standards for data quality, as determined by the VSC. The VSC retains the right to approve the quality of data displayed on websites; data not meeting the VSC standards will not be displayed.
- Processes that gather, edit, modify, calculate or otherwise manipulate the data must meet the VSC standards for data quality, as determined by the VSC.

6. How well do the data security policies and practices of the third party align with the data security policies and practices of the VSC?

- The maintenance and retention by the third party of all data must comply with the VSC Records Retention Policy.
- Social Security numbers will be encrypted when stored and transmitted, and masked on display so that only the last four digits will appear on any display; any public reporting will not include Social Security numbers. The retention period for storage of Social Security numbers must be approved in advance by the VSC.
- If credit cards are processed on a website, the third party must supply documentation of compliance to Merchant Security Review standards, including Visa's Cardholder Information Security Program and MasterCard's Security Data Program. Credit card numbers will not be stored unless a retention period for storage has been approved in advance by the VSC. If stored, credit card numbers will be encrypted when stored and transmitted, and masked on display so that only the last four digits will appear on any display, including reports.
- The third party agrees to comply with all related state and federal privacy and security laws.

7. Contract termination

- The VSC retains the right to terminate the contract for any reason related to the security items listed in the contract.
- The VSC aggressively protects copyrighted material, and all VSC logos, emblems, images, and .gif files must be used only with VSC approval, and must be destroyed at the end of the contract.

8. Insurance

- The third party will present evidence of liability insurance as appropriate.

Section IV: Third-Party Review Checklist

Individual or office seeking to transfer data: statement of work/ need:

__ Document data elements to be collected, transmitted or stored under contracted third party arrangements
__ Conduct third party reference check
__ Consult with BAC as necessary to review third party compliance with internal policies and external mandates related to processing electronic payments

IT review/ discussion with third party:

__ Review data security policies and practices of third party in relation to VSC security policies and practices
__ Discuss results of third party's most recent security audit
__ Review third party disaster recovery procedures
__ Review related firewall, anti-virus and patch management protections
__ Confirm that third party websites have been implemented utilizing Secure Socket Layer (SSL) with a certificate from an independent authority
__ Confirm that file transmissions will be done using Secure File Transfer Protocol
__ Identify and document any gaps or areas of concern relative to VSC security policies and practices

Contract development:

__ Confirm that items 1-8 in Section III of this policy are included in the contract

General Counsel review of contract:

__ Review of non-disclosure contract language
__ Review of systems administration and maintenance guarantees in contract language
__ Review provisions for data retention and data return to the VSC upon contract termination
__ Confirm assurances of compliance with federal and state laws
__ Confirm acceptable contract termination language if security provisions are not met

Section V: References

VSC policies:

VSC Policy 312: Federal Educational Rights and Privacy Act (FERPA)
VSC Policy 414: Computing and Telecommunications Conditions of Use

VSC internal information technology security policies:

VSC Information Sensitivity Policy
VSC Incident Response Policy
VSC IT Computer Hardware Security Policy
VSC IT Server Hardening Policy

Related Vermont laws:

9 V.S.A. §2430 (Definitions)
9 V.S.A. §2435 (Notification of Breach)
9 V.S.A. §2440 (Social Security Number Protection)
9 V.S.A. §2445 (Safe Destruction of Documents Containing Personal Information)

Related federal laws:

Gramm-Leach-Bliley Act - http://www.ftc.gov/privacy/glbact/
Health Insurance Portability and Accountability Act - http://www.cms.hhs.gov/hipaa/

Cardholder Security Programs:

http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html
https://sdp.mastercardintl.com/

Student and Exchange Visitor Information System - http://www.ice.gov/graphics/sevis/

Sample Checklist:

Oakland University – University Technology Services – Security – Outsourcing or Hosting Services Checklist – 6/10/2005

Contract reference:

The Catholic University of America, The Office of General Counsel - Data Security Terms for inclusion in Contracts with Service Providers - http://counsel.cua.edu/ferpa/

Approved by/on: Council of Presidents, June 3, 2009
Amended:
Reviewed: