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: