Risk Management Services

Security Checklist for Hosted IT Services

Background

The University of Texas at Austin (UT Austin) is engaging in business where university data are collected, transmitted, or processed under contracted third-party arrangements. In many of these situations, a network-accessible service is developed by a Vendor to collect, transmit, or process data on behalf of a UT Austin department. The university may also send data collected by the university for further processing or storage by a contracted third-party Vendor. The UT Austin Information Security Office (ISO) has created this checklist to assist purchasing project sponsor(s) in addressing risk management, contract review, and ongoing Vendor management, with the goal of minimizing the risk to university data.

The ISO expects the purchasing project sponsor(s) to have determined whether or not existing university services can be utilized to ensure coherence, consistency, and elimination of redundancy prior to pursuing third-party services. If no existing solutions are available on campus, the purchasing project sponsor(s) should also determine if it is cost effective to consider having the service built and/or maintained in-house (for example, by the local department or by Information Technology Services).

Determining the Need for a Security Assessment

A security assessment or review is required to be conducted if any of the following apply to the project:

1. The project involves transferring any university data classified as Category-I, or otherwise sensitive, from a university-owned device to a third-party contracted device
2. The project involves contracting with a Vendor who will create a network-accessible service on behalf of UT Austin to collect, transmit, or process any university data classified as Category-I, or otherwise sensitive
3. The project requires that a contracted third party collect or process any university data classified as Category-I, or otherwise sensitive, that will later be transmitted for use by UT Austin.
4. The project requires that a third party process payment card information on behalf of UT Austin.

The purchasing project sponsor(s) can elect to have their department conduct the security assessment themselves or can submit a request for assistance to the Information Security Office, security@utexas.edu. At a minimum, the security assessment should consider all applicable provisions of the UT Austin Information Resources Use and Security Policy and the UT Austin Minimum Security Standards.

Assess Compliance with University Policies

The purchasing project sponsor(s) shall review the University of Texas Information Resources Use and Security Policy. The following supplemental university security standards and guidelines should also be reviewed, as needed:

- Data Classification Standard
- Minimum Security Standards for Systems
- Minimum Security Standards for Data Stewardship
- Minimum Security Standards for Application Development and Administration
- Minimum Security Standards for Merchant Payment Card Processing
- Data Encryption Guidelines

The purchasing project sponsor(s) should note that certain types of data require the university to comply with external mandates. Such mandates include, but are not limited to:

- Federal Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Standards Supporting Documents (PCI)

Data management plans must conform to all applicable mandates. If there are any questions regarding policy interpretation or compliance, please contact the Information Security Office at security@utexas.edu.

System Security Assessment

The systems used to process, transmit, or store data must be reviewed prior to formalizing the agreement. References from other clients should be obtained prior to formalizing the agreement. The purchasing project sponsor(s) is responsible for ensuring that a system security assessment is conducted. The Information Security Office is available to assist in performing a security assessment based on priority and availability. In general, the university seeks to hold Vendors to the required university Minimum Security Standards (Section 25 of the UT Austin Information Resources Use and Security Policy).

Review of Contract Details

The Information Security Office can assist in the review of contract details upon request and based on priority and availability. The Purchasing Office, Office of Legal Affairs, or Internal Audit may require an assessment, and may require specific language in a contract. In general, the following items must be assessed.

1. Who will have access to the data?	
1.1	Data access shall be limited to those with a "need to know" and controlled by specific individual(s). The Vendor must have procedures and solutions implemented to prevent unauthorized access, and the procedures will be documented and available for UT Austin to review upon request. All of the Vendor's employees with access to university data must be identified and names provided to the university upon request.
1.2	Unauthorized exposures of university data shall result in the Vendor notifying UT Austin within twenty-four hours of discovery, and no notification shall be made to those affected by the unauthorized exposure of the university's data until the Vendor has consulted with UT Austin officials.
1.3	Physical access to facilities where data are stored must be limited and controlled. Any damage or unauthorized access to facilities must be reported to the university within 24 hours of its discovery. If any unauthorized access to university data occurred, the Vendor must consult with UT Austin officials before notifying those affected by the unauthorized access to this data.
1.4	Standard non-disclosure language must be included, with protection to keep information private and confidential, except as specifically provided for in the contract. Data shall not be shared with or sold to third parties.

2. What security standards will be implemented and where will data be stored?	
2.1	All the Vendor's systems handling university data must comply with the Minimum Security Standards for Systems with Category-I data.
2.2	All systems and applications shall regularly undergo vulnerability assessments, such as testing patch level, password security, and application security.
2.3	Routine event monitoring will be performed by the Vendor; the university expects that the Vendor will routinely and immediately identify events related to unauthorized activity and unauthorized access.
2.4	The Vendor should undergo regular security audits, preferably by certified third parties, occurring at least annually, and any identified issues must be resolved or mitigated within 90 days of the audit report. The university may demand written proof of this audit at any time during the duration of the contract.
2.5	All services that gather Category-I or otherwise sensitive information must utilize secure communications methods, such as SSl, and use a certificate from an approved independent authority, for example, VeriSign, if certificates are required.
2.6	All file transmissions involving Category-I or otherwise sensitive data must utilize secure communication methods; for example, SSL, SCP, SSH, SFTP.

3. Have both disaster recovery and business continuity plans been developed and are there plans to regularly test and review them?	
3.1	The purchasing project sponsor(s) shall detail the specific backup requirements for systems, files, and data. The Vendor must agree to the required time periods and processes. For example, if a department determines that no more than the previous 24 hours of data may be lost, the Vendor must be able to comply with that requirement.
3.2	The Vendor must have a disaster recovery plan.
3.3	The Vendor must have a secure secondary off-site storage location for university data. The university must approve the location of the off-site storage, and the university retains the rights to reject the location for security or availability reasons and to recommend another location.
3.4	The purchasing project sponsor(s) shall detail the specific system uptime requirements for the service and the Vendor will agree to the availability requirements. An example of availability requirements might be expressed as, "Guaranteed to 99.9 percent each year or no more than 8 hours and 45 minutes of downtime every year."

4. Does Vendor-managed data meet all integrity and accuracy requirements identified by the university?	
4.1	The Vendor must be able to maintain the integrity and accuracy of the data it manages for the university. No data exchanges will occur until the university has agreed that the data meets any specified university requirements for accuracy and integrity. The university retains the right to approve or reject the data displayed on Web sites; the display of data not meeting university standards will not be allowed.
4.2	Processes that gather, edit, modify, or otherwise manipulate data must meet university standards for data quality.

5. Does the Vendor comply with data retention and protection regulations and policies?	
5.1	The maintenance and retention of all data must comply with the university data retention schedule.
5.2	UT Austin officials, such as the Information Security Office or Office of Legal Affairs, must explicitly authorize the disclosure of Social Security numbers to any vendor. UT Austin officials must approve the retention period for the storage of Social Security numbers in advance.
5.3	Social Security numbers shall be encrypted when stored and transmitted, and masked on displays and reports.
5.4	If credit cards are processed via a network-based service, the Vendor must supply evidence of PCI compliance. Credit card numbers shall not be stored unless the university has approved a retention period for storage in advance.
5.5	Credit card numbers will be encrypted when stored and transmitted, and masked on displays and reports.
5.6	If financial records are processed, the Vendor must supply documentation of compliance to GLBA prior to the contract being accepted by the university, and annually thereafter.
5.7	All payment processing must comply with university cash management policy.
5.8	If medical record or medical insurance data is included, the data must be encrypted, and the Vendor must supply documentation of compliance to HIPAA prior to the contract being accepted by the university, and annually thereafter.
5.9	If student record data is included, the Vendor must supply documentation of compliance to FERPA prior to the contract being accepted by the university, and annually thereafter.
5.10	The Vendor must supply documentation of compliance with all other legislation as dictated by applicable laws and university policies.
5.11	All data will be retained for periods approved by the university and will be destroyed or returned to the university upon termination of the contract. The method of data destruction must be approved by the university and must be compliant with UT Austin Information Resources Use and Security Policy.
5.12	Vendor agrees to comply with all state of Texas and federal legislation within 60 days of enactment.

6. Contract termination	
6.1	The university retains the right to terminate the contract with 30 days notice for any reason related to the security items listed in the contract.
6.2	The university aggressively protects copyrighted material, and all university trademarks, logos, emblems, images, and graphics files must be used only with university approval, and must be destroyed at the end of the contract.

7. Insurance	
7.1	When the project presents significant risk, the Vendor will present evidence of $1 million or more in liability insurance, and preferably cyber risk insurance.
7.2	Review applicability of contractual cyber insurance requirements.

If you have any comments or suggestions, please contact the Information Security Office at security@utexas.edu.