Third Party Service Provider Information Security Reviews

Version: 2.0
Effective Date: 3/29/2016

Policy Summary:
Arrangements with third parties to provide hosted Information Technology & Security related services on behalf of university departments need to be evaluated prior to entering into contracts with them, to ensure that potential risks are identified and contracts incorporate data protection language that protects university interests.

Applicability/Eligibility:
Staff and Faculty, and third parties performing duties on behalf of The University of Tampa

Exceptions:
None

Policy Administration:

Mandating Authority: (Check all that apply)
☐ Federal Law ☐ State Law or Regulation
☒ University President ☐ Accrediting Body
☐ Other: (specify)

Responsible Office/Dept/Committee(s):

Name	Campus Address	Phone Number
Information Technology & Security	East Walker Hall, Rm 133	813-257-3950

Responsible Executive(s):

Name	Title	Phone Number
Tammy Clark	Chief Information Officer	813-257-7522

Policy Management:

Policy History:

Date	Version	Reason for Change
4/2/2015	1.0	Initial policy draft
3/10/2016	2.0	Organizational Changes and Policy Link Modifications

Policy Approvals and Reviews:

Date	Organizational Group
3/29/16	President
3/29/16	Senior Staff

Web Links:
Policy Link: Third Party Service Provider Information Security Reviews

Associated Links:

Acceptable Use Policy
Information Classification and Protection Policy

Full Policy Text:

Prior to signing or agreeing to execute third party hosting contracts with the university (including 'click through agreements'), contracts meeting the specifications outlined below in the Definitions section should be reviewed by The Office of Information Security to ensure that

- Service or solutions provider(s) include 'breach notification' language which requires them to contact infosec@ut.edu in the event an information security incident occurs (within 24 hours)
- Data protection language is included that ensures The University of Tampa won't be liable for damages in the event the third party service provider suffers a data breach
- The use of encryption to protect confidential information (SSN's, financial data, electronic health data) is directly specified
- The service provider's responsibilities to manage and protect university information and hosted/outsourced services (ex. Websites, databases, internet portals) from unauthorized access and intrusions are clearly outlined

1) If service providers either refuse or are unable to meet the above requirements, the Office of Information Security will meet with the appropriate Senior Staff member to determine the best course of action in favor of the university.
2) Once contracts are modified to provide acceptable protection for university systems and information, the UT requestor and Senior Staff member will be notified and asked to have the VP Administration and Finance execute the contract on behalf of the university.
3) When contracts are up for renewal, they will need to be reviewed to ensure that no material changes have occurred.

Contact information should be provided to allow *Information Security* to conduct a security review with all third party service providers university departments are considering or currently using (using the below definitions as a guideline) to ensure that

their information handling methods and/or service offerings do not pose unreasonable information security risks that can't be addressed or reduced appropriately by the service provider.

4) Security reviews of third party service providers will be performed by *Information Security* on an annual basis and/or when material changes in their services are made that can impact information security.

To initiate contract and/or security reviews, UT departments should submit a help desk work order or call the Help Desk directly.

Definitions:
Third Party Hosting Arrangements

Third party hosting arrangements can include any or all of the following services:

- A portal that staff, faculty and/or students authenticate with to enter or utilize information that is stored by the third party and accessed through a software client or internet browser
- A software package that integrates with the university's Active Directory account services (LDAP or SLDAP) or ERP system, that allows the third party to use university accounts or information in providing services to staff, faculty and/or students
- A hosted service that involves a third party providing technology services to UT department clients or customers, such as websites, data storage, or databases
- An outsourced service that involves a third party managing IT services on behalf of the university, such as outsourced staffing, Software as a Service (SaaS), Hardware as a Service (HaaS), or Infrastructure as a Service (IaaS)
- Technology related service offerings that are provided by a third party and don't require assistance or services from UT's internal service providers (IT, Information Security, Educational Technology, and/or Media Services)

Additional Information and Resources: *Information Security Guidelines for Data Owners*