Third Party Technology Service Provider Reviews

Version: 3.1
Effective Date: 12/09/2024

Policy Summary:
Prior to entering into contracts with third parties, Information Technology and Security (ITS) will initiate security reviews, to ensure that potential risks are identified, and contracts incorporate data protection language that protects university interests. Annual reviews will be conducted by ITS to highlight information security, business continuity, and customer service metrics to be displayed on an internal vendor scorecard and shared with the appropriate functional leadership.

Applicability/Eligibility:
Staff, Faculty, and external third parties performing technology services 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: (GLBA, Technology Project Request)

Responsible Office/Dept/Committee(s):

Name	Title	Phone Number
Information Technology & Security	TECH Building, UTCIO@ut.edu	813-253-6293

Responsible Executive(s):

Name	Title	Phone Number
Tammy Loper	VP, Information Technology & Security	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
2/21/2024	3.0	Changed Office of Information Security to ITS Information Security
12/09/2024	3.1	Updated title and description to add business continuity and customer service, updated references to Cabinet, changed from University President to Other (GLBA recommendations)

Policy Approvals and Reviews:

Date	Organizational Group
3/29/16	President
3/29/16	Senior Staff
12/09/2024	President's Cabinet

Web Links:

Policy Link: Third Party Technology Service Provider Reviews

Associated Links:

Acceptable Use Policy

Information Classification and Protection Policy

Full Policy Text:

Prior to signing or agreeing to execute third party technology solution contracts with the university (including 'click through agreements'), contracts meeting the specifications outlined below in the definitions section should be reviewed by ITS and UTampa Risk Management 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 48 hours)
- The service provider has clearly outlined responsibilities to manage and protect university information and hosted/outsourced services (ex. Websites, databases, internet portals) from unauthorized access and intrusions, and
- A thorough review of relevant terms and conditions is conducted.

1) If service providers either refuse or are unable to meet the above requirements, ITS will meet with the appropriate Cabinet member, or delegate, 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 UTampa requestor and Cabinet member, or delegate, will be notified and have the appropriate university official 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 *ITS* 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) Third party technology service provider reviews will be performed by *ITS* on an annual basis and/or when material changes in their services are made that can impact information security, business continuity, customer service, accessibility, etc.

To initiate technology contract and/or third party technology service provider reviews, UTampa departments should submit a Service Desk request or call the Service Desk directly.

Definitions:

Third party technology service arrangements can include any or all of the following:

- 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 single sign on (SSO) application, MyUTampa (powered by Okta), 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 UTampa 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 Services (HaaS), or Infrastructure as a Service (IaaS).
- Technology related service offerings that are provided by a third party and do not require assistance or services from UTampa's internal service providers.