**Intake Form for Third-Party Information Security Assessment**

This form is to be initiated by the UT System Administration department making or coordinating the purchase of products or services from vendors or other third-parties who will create, store, process, or access UT System Data. For detailed instructions see page 4 of this form.

|  |  |
| --- | --- |
| **Submission Date:** Select Date | **Requested Deadline:** Select Date |
| **Department:** Other | **Department Contact:** First and Last Name |
| **1. Contract Information**[ ]  New Contract[ ]  Amendment to Existing Contract[ ]  Renewal[ ]  Other: **Anticipated Value:** [ ]  < $15,000[ ]  $15,000 - $50,000[ ]  $50,000 - $1M[ ]  > $1M**Estimated Period of Contract:**[ ]  < 6 months[ ]  6 months – 1 year[ ]  1 – 2 years[ ]  2 – 5 years[ ]  > 5 years  | **Scope of Purchase:** [ ]  System Administration (internal use only) [ ]  Systemwide [ ] Faculty [ ] Staff [ ] Students [ ]  Other: If other, please describe**Procurement Method:**[ ]  Informal Bid[ ]  RFP[ ]  GPO/State Contract[ ]  UT System Institution Contract[ ]  Exclusive Acquisition [ ]  Other: If other, please describe |
| **2. Vendor Information – (Provide current and verifiable contact information)**Vendor Name:Vendor or Third-Party NameWebsite: Vendor websitePoint of Contact Name: Name of Vendor ContactEmail: EmailPhone Number: Phone Number |
| **3. Description of Service/Product and how it will be used:** |
| **4. Description of University Data[[1]](#footnote-1) that vendor/third-party product or service will create, store, process, or access:**  |
| **5. Will the vendor/third-party product or service create, store, process, or access Controlled or Confidential Data?**[ ]  Yes (please select all that apply) [ ]  Student Record Data (FERPA) [ ]  Social Security Numbers [ ]  Protected Health Information (HIPAA) [ ]  Personally Identifiable Information (PII) [ ]  Credit Card Numbers (PCI) [ ]  Donor Records [ ]  Research Data [ ]  Non-Confidential Information Exempt from TPIA Requests [ ]  Other: ­­­­­­­­­­­­­­­­­­­­Click here to enter text.[ ]  No[ ]  Unknown |
| **6. Does the vendor use a separate third-party cloud storage location? (e.g. any location outside of UT System such as Box, Dropbox, Google Drive, Azure and not on the UT System Cloud Storage approved list found here:** <https://community.utsystem.edu/sites/infosec/SitePages/cloudstorage.aspx>[ ] Yes\*[ ] No\*If yes, please complete the Cloud Storage Exception Request form which can be found here: <https://community.utsystem.edu/sites/infosec/SitePages/cloudstorage.aspx>  |
| **7. Is this either a full cloud-based vendor or a combination of a local application and a 3rd party website which is often referred to as *hybrid*? (Please contact ISO for questions)**[ ] Yes[ ] No |
|  |
| **8. Will this application/tool include using a mobile application for access to application?**[ ] Yes[ ] No |
| **9. Will this application or tool include accessing or authenticating to a third-party website (e.g. http://salesforce.com, www.utlivingwell.com)?**[ ] Yes[ ] No |

**Instructions:**

**When should this form be completed?**

There are several scenarios where this form may be required. The most common is when a department is in the process of purchasing resources or services that will require a vendor to interact with (create, access, process, or store) UT System data, regardless of the total purchase amount.

Other possible scenarios include:

when a department is purchasing a software or tool (either on premise or cloud-based) for departmental or system-wide use;

when renewing an agreement with an existing vendor;

when there is a change in the scope of services or resources being provided; or

when a vendor notifies you of a change in their third-party providers.

**What happens after I submit the form?**

The Office of Information Security will contact you to let you know who has been assigned to complete this request and request any additional documentation they need to complete the assessment.

The assessor will determine the level of security risk for using this service, tool, or application. Security risk ratings include:

***Low*** or ***Medium*** risk: Estimated time to complete is 7 business days.

***High*** risk: Estimated time to complete is 10-15 business days. Generally, a review is considered High risk if it will process, store, or handle UT System Confidential data. These require a more in depth assessment and the vendor will be asked to complete a security questionnaire. NOTE: Ensure you provide current contact information on this form.

Once the assessment is complete, your reviewer will send an email or document that explains the risk level and includes recommendations for implementing, options to include in the purchase, and general security best practices for this service, tool, or application.

**Definitions:**

**University Data** - All Data or Information held on behalf of U. T. System and its Institutions created as a result of and/or in support of U. T. System business, or residing on U. T. System Information Resources, including paper records.

**Controlled Data** - The “Controlled” classification applies to information/data that is not generally created for or made available for public consumption, but that is subject to release to the public through request via the Texas Public Information Act or similar State or Federal law.

**Confidential Data** - data that is exempt from disclosure under applicable State law, including the Texas Public Information Act, and Federal laws.  Data or information meeting these criteria are designated with the classification of “Confidential” within the U. T. System Data Classification Standard.

For examples and more information on UT System Data Classification see [UTS 165, Standard 9.](http://www.utsystem.edu/offices/board-regents/uts165-standards#s9)

**Questions? Please email** **iso3pra@utsystem.edu** **or call 512-499-4389**

|  |
| --- |
| ***FOR ISO OFFICE USE ONLY*** |
| Reviewer: |
|

|  |
| --- |
|  |
|  |
|  |

Rank the following as High, Medium, or Low using the UT System Categorization Guidelines:**Confidentiality** - Impact if the data is viewed by unauthorized persons.**Integrity** - Impact if data were to be accidentally changed.**Availability** - Impact if data were not available for extended periods. |
| Has the vendor been previously assessed by UT System or an institution? | [ ]  Yes: Institution Name[ ]  No |
| If yes, what was the date of the most recent assessment? |  |
| Is this a SaaS or cloud-based application? | [ ]  Yes[ ]  No |
| Overall Risk Rating: | [ ]  Low[ ]  Medium[ ]  High |
| Exception(s) granted? |  [ ]  Cloud Storage[ ]  Encryption[ ]  Other: List additional ISO exceptions |
| Recommendations for implementation, options, or management: |  |
| Additional Comments: |

1. See Definitions of University Data, Controlled Data, and Classified Data on the following page. [↑](#footnote-ref-1)