TTS Information Security Review Document Request List[1]

1. Tell Us about your Project - Write up a Project Summary

To help with our review, we need you to provide some key information. This document is called your Project Summary.

Copy the questions below into a document or any email and answer them there.

Project Summary

Brief Name of Project to use for easy reference:

Date summary prepared:

Prepared by:

1. Tufts project owner information

- *Which department/manager will have ongoing responsibility for this app, tool or service?*
- *Who is the Tufts project manager (and contact info) that is overseeing the implementation?*

2. Describe the project, solution, or services

- *Describe the total solution, including the goals/deliverables/benefits. Why is this app/tool/service being purchased? What need will it fill?*
- *What is being purchased, installed, upgraded, and/or migrated? Provide the vendor name and website links. Include the names of the specific software modules, product names or services involved. Please cover all current and future plans.*
- *Describe who is expected to use the app/tool/service. Are they students, faculty for educational use, researchers, or staff?*
- *Roughly how many users will there be in a year?*
- *Will there be users outside of Tufts who need to access this solution? If so, describe who and for what purpose, that is, describe the use case.*
- *When is the desired go-live, i.e. ready-for-use, date?*
- *Is this a cloud service (Software as a Service) or will this be hosted and run within a Tufts data center?*

[1] This document is an extract from the TTS Guide for Reviews, V: 10.1.2021, found at https://tufts.box.com/s/2q7k4wkmfpbqmmx3ekavpiwxuw8430bk .

- *Will any of the users be outside the US? If yes, where (countries or region)?*

3. Describe the Information involved

- *Describe the information or data involved in the project. Consider everything that is collected, stored, used, push/pulled to the vendor or the software involved.*

- *Describe the specific types of information involved (for example: names, emails, contact info, addresses, student data, class/program information, date of birth, government IDs like SS#, passport, driver's license, financial or payment information such as bank info, credit cards, health data etc.).*
- *Is any of this data sensitive that would be harmful if leaked or hacked?*
- *Do you know if any of the data involved is regulated or covered under a data contract (i.e., funded research)? If so, which regulations apply? If there are data, research or other third-party contracts that specify IT requirements for the data involved, provide these contracts as a part of the review.*
- *Will the data include information that is associated with persons from outside the US? If yes, where (countries or region)?*

2. Email the Vendor to collect information for the Security and Privacy Review, the Accessibility Attestation Report on Compliance (AROC), and if applicable, the Credit Card and eCommerce Payment Review

The office or department that will be purchasing the app, tool or service needs to collect key information from the vendor. To do so, you can copy the draft email below and send it to your contact at the vendor. Please see the instructions below.

Instructions for the Information Request Email:

- Don't worry - you don't need to understand what a SOC 2 or other terms mean or even read the linked documents. The vendor IT folks will (hopefully) talk IT!
- #1 - #10 ask for information needed for the Security and Privacy Review and Accessibility. Always include these. The Accessibility Attestation Report on Compliance (AROC) mentioned in # 10 is also attached as an Appendix to this Guide.
- #11 Include if a *Credit Card and eCommerce Payment Review* will be needed. This review will be required whenever the app, tool or service *directly involves* the collection of credit or debit card information in order to make payments *to* Tufts or any receipt of funds *by* Tufts in connection with the use of the app, tool, or service. This doesn't include payments made by Tufts for the license for the app, tool or service. More information is provided under *Credit Card and eCommerce Payment Review*.

Use the text below for your email message to the vendor. Copy the text below, add in the name of the app/tool/service, and send to your contact at the vendor.

I am writing to collect some more information about [name of app/tool/service] we are considering purchasing. As part of Tufts' processes for contract approval and for app, tool and IT service implementations, Tufts Technology Services asks for specific information from each vendor. The list below will support TTS's reviews, especially its security and privacy review. Please provide this list to your IT staff. If they aren't able to provide any of the information on the list, they can note that as their response.

1. *Security program documentation.* Any materials you have prepared for customers that provide a description of your information security program and processes. This may include security program descriptions, policy documents, customer-facing security whitepapers, etc.
2. *At least one industry-standard completed security questionnaire*. Tufts prefers the Higher Education Community Vendor Assessment Toolkit (HECVAT) from Educause or something like a SIG from Shared Assessments, and/or CSA Star self-assessment from Cloud Security Alliance are also accepted.
3. *Third-party external security reviews and attestations*. A SOC 2/SOC 3 report is preferred, but other useful reports include ISO 27000 audits, pen tests, etc.
4. *Compliance with Regulations*. Confirm/list which (if any) of the following regulations or government standards the vendor solution is compliant with: FERPA, HIPAA, GDPR, MA and

other state data privacy laws, any US government security standards such FISMA/NIST 800-53/NIST 800-171, and any other security and privacy regulations.

5. *Related vendors.* A list of all other vendors/subcontractors that are part of the app, tool or service Tufts is considering.
6. *Data Integrations and Feeds from Tufts*. Provide a list and description of any data integrations or data feeds from Tufts (one time or continuous) that will be needed for the solution. If none are required, describe how the vendor will get needed data for initial set up and then how will Tufts data in the solution be kept current. Does any data need to flow back to Tufts systems and if so, how will this be done?
7. *Architecture diagrams* of the systems involved and that show the typical data integrations and data flows. It's especially helpful to have a diagram of the expected use at Tufts.
8. *Authentication.* If the app, tool or service will require Tufts to have "admins" that will set up and maintain the solution and/or if there will be individual Tufts users, does the vendor support using Tufts SSO authentication with 2FA (Duo) through ADFS/SAML for the Tufts admins and/or other Tufts users? Will some users need to self-register and create their own logins?
9. *Encryption.* Will all data communications be encrypted in transit? Will Tufts data be encrypted at rest inside the vendor solution? Specify what encryption and if applicable, the version.
10. *Accessibility.* If available, please review the Accessibility Attestation Report on Compliance (AROC) and if you are able to do so, complete, sign and return it. If not, please explain the accessibility compliance status for your app or tool.
11. *Credit Card and eCommerce Payments.* Is the solution PCI DSS compliant? Provide the latest PCI DSS Attestation of Compliance (AOC). If all or part of the solution will be located on Tufts premises: How do the systems connect to the Internet to do credit card processing? Such as using: Cellular? Through Tufts wired network? Through Tufts wireless network? Are the devices accepting the credit cards certified using P2PE? Are the devices PCI certified?

Thank you for providing this information. We're looking forward to learning more about [name of app/tool/service].

Tufts Accessibility Attestation Report on Compliance (AROC)

Vendor and Product Information	
Company Name:	
List all Product(s) and Modules Being Purchased by Tufts and In-Scope for this AROC:	

Accessibility Attestation Report on Compliance

The following have been reviewed for the specific products and modules named above that are being supplied to Tufts University: **(Check that all apply)**

- ☐ Products above comply with WCAG 2.0/2.1 level AA
- ☐ After running frequently used pages from your product through an automated accessibility checker, please attach a report here (please include a report from a page that adequately represents your site's content and user interactions).
- ☐ The main user tasks expected under the purpose of the product(s) have been completed successfully using only a keyboard (no mouse)
- ☐ The main user tasks expected under the purpose of the product(s) have been completed successfully using only a screen reader, without relying on visual cues from the screen itself on both a Mac and a PC

Notes**:**

(1) Some online testing options: https://wave.webaim.org/ and https://www.deque.com/axe/ (see "Install Free Chrome extension" button)
(2) Free screen reading testing tools:

PC Users: NVDA Screen Reader: https://dequeuniversity.com/screenreaders/voiceover-keyboard-shortcuts

For Mac users: VoiceOver: https://dequeuniversity.com/screenreaders/voiceover-keyboard-shortcuts

Chrome extension free screen reader: ChromeVox
https://chrome.google.com/webstore/detail/chromevox-classic-extensi/kgejglhpjiefppelpmljglcjbhoiplfn?hl=en-GB

Company Attestation

This *Accessibility Attestation Report on Compliance* is a declaration that the products and modules named above being supplied to Tufts University meet the digital accessibility standards stated above at both the time of delivery and for all ongoing maintenance.

Signature of Authorized Officer:	
Printed Name:	
Title:	
Date:	