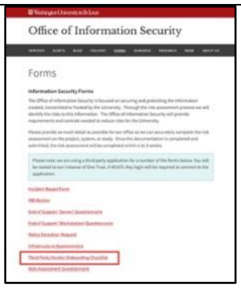
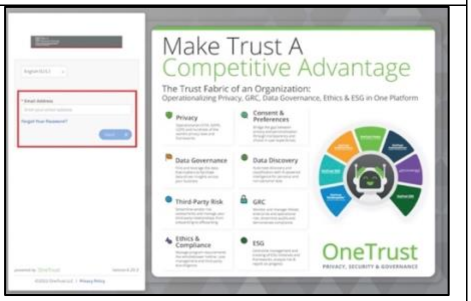
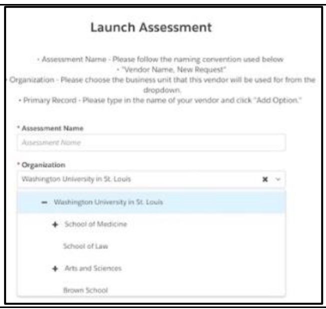
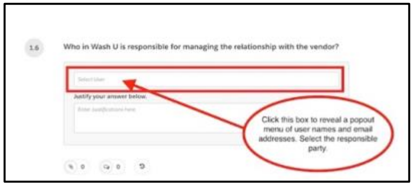
THIRD-PARTY VENDOR ONBOARDING GUIDANCE, ONETRUST

The Office of Information Security (OIS) supports our community's important work of administration, academia, and patient care by evaluating tools and services from an information security perspective. Our purpose is always to protect privacy and secure the work of our trailblazing knowledge seekers. The software platform, OneTrust, makes it easier for the OIS to work with users to identify, track, and mitigate security risks involved in the diverse projects underway at our institution. The vendor onboarding process allows our office to better understand the types of data involved in the project and the capacity of third-party service vendors to secure those data. This process empowers project owners to select vendors that make security a priority.

To onboard a vendor for evaluation, users need to complete two background questionnaires in the OneTrust portal. The process is described below.

INSTRUCTIONS	RELATED SCREENSHOTS
1 To onboard a vendor, first click on "Third Party Onboarding Checklist" on the OIS Forms page.	 Office of Information Security Forms Information Security Forms
2 Enter your WUSTL email address in the login page. If you aren't already logged in with DUO, you will be prompted to complete our WashU 2FA process	 Make Trust A Competitive Advantage The Trust Fabric of an Organization: Operationalizing Privacy, GRC, Data Governance, Ethics & ESG in One Platform Privacy Consent & Preferences Data Governance Data Discovery Third-Party Risk GRC Ethics & Compliance ESG OneTrust PRIVACY, SECURITY & GOVERNANCE
3 From the Self Service Assessment main page, click "Launch" under Vendor Onboarding.	
4 Name the assessment using the convention "Vendor Name, New Request." And select the business unit for which the vendor will be used.	 Launch Assessment • Assessment Name - Please follow the naming convention used below • "Vendor Name, New Request" • Organization - Please choose the business unit that this vendor will be used for from the dropdown. • Primary Record - Please type in the name of your vendor and click "Add Option." * Assessment Name Assessment Name * Organization Washington University in St. Louis − Washington University in St. Louis + School of Medicine School of Law + Arts and Sciences Brown School
5 You will need to complete two questionnaires for the onboarding process—the General Questionnaire, and Screening Questions. Click on "General" to get started with questions 1.1-1.7. Please have the following information ready to submit: 1.1 Vendor Name 1.2 Type of vendor (i.e., consulting, regulatory, technology, operations, strategic, unknown). 1.3 Expected procurement or purchase date 1.4 Products or services provided (select all that apply from pop-out menu) 1.5 Vendor processing activities (select all that apply from pop-out menu) 1.6 WashU responsible party (select name from pop-out menu) 1.7 Describe the University benefit/purpose or working with this vendor. 1.8 Primary Vendor Contact	 (1.6)  1.6 Who in Wash U is responsible for managing the relationship with the vendor? Justify your answer below. Click this box to reveal a popout menu of user names and email addresses. Select the responsible party.

6 Click the forward arrow at the bottom of the screen to continue or “Save and Exit” to come back later.

7 Complete the Screening Questionnaire. Please be prepared to answer the following questions:

2.1 Have you explored all WashU-U provided options that may be available to meet this need?

2.2 Will the vendor be storing ePHI?

2.3 Will the vendor be viewing, collecting, processing, and/or otherwise have access to protected and/or confidential data of the University’s consumers, employees, and/or third parties?

2.4 (if selected “yes” to question 2.3) What protected and/or confidential data will be shared with this Vendor? Select all that apply.

2.5 (if selected “yes” to question 2.3) Will any data be transferred outside of the United States?

2.6 Will the vendor be hosting any of the Company’s data off-site?

2.7 Does this implementation affect another project(s) at the University?

2.8 Will this implementation involve EPIC data?

2.9 Will our affiliated hospital system, BJC, be involved in the project implementation?

2.10 Will the vendor have remote access to the Company’s network?

2.11 Will the vendor have access to source code, repositories, or privileges to commit new code in the Company's network?

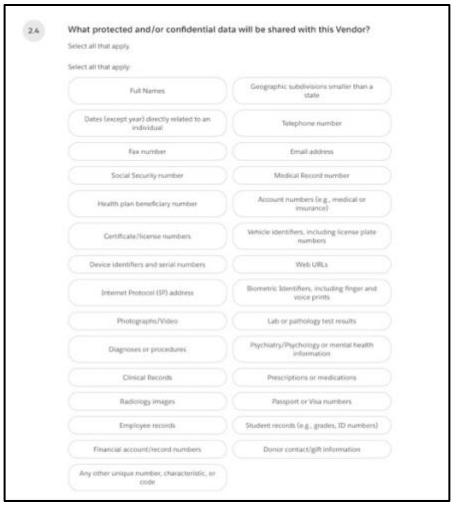
2.12 Will any proprietary or confidential business information (including customer data) be shared with the vendor?

2.13 Does the vendor serve critical business functions (i.e., those functions, which if corrupted or disabled, are likely to result in mission degradation or failure)?

2.14 How would you characterize the potential effect if this vendor were responsible for the unauthorized disclosure of, or access to, the information shared with them? (Select: limited adverse effect; severe adverse effect; severe or catastrophic effect).

2.15 Overall, how would you characterize the potential effect if this vendor were responsible for the unauthorized modification or destruction of the information shared with them? (Select: limited adverse effect; severe adverse effect; severe or catastrophic effect)

2.16 Overall, how would you characterize the effect the disruption of access to or use of information have on operations, assets or individuals? (Select: limited adverse effect; severe adverse effect; severe or catastrophic effect)



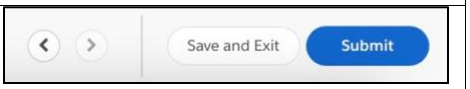
2.4 What protected and/or confidential data will be shared with this Vendor?

Select all that apply.

Select all that apply:

Full Names
Geographic subdivisions smaller than a state
Dates (except year) directly related to an individual
Telephone number
Fax number
Email address
Social Security number
Medical Record number
Health plan beneficiary number
Account numbers (e.g., medical or insurance)
Certificate/license numbers
Vehicle identifiers, including license plate numbers
Device identifiers and serial numbers
Web URLs
Internet Protocol (IP) address
Biometric Identifiers, including finger and voice prints
Photographs/Video
Lab or pathology test results
Diagnoses or procedures
Psychiatry/Psychology or mental health information
Clinical Records
Prescriptions or medications
Radiology images
Passport or Visa numbers
Employee records
Student records (e.g., grades, ID numbers)
Financial account/record numbers
Donor contact/gift information
Any other unique number, characteristic, or code

8 When you have completed all the required questions, the Submit button will become available. Click the button to submit your questionnaires.


Save and Exit
Submit