Vendor risk assessment [1]

University schools, departments and business units sometimes contract for data services with outside parties or service providers; of concern are those circumstances where service providers process or hold University data. While Duke University has taken steps to help ensure that its data is protected, service providers must also exercise appropriate controls to minimize the risk of exposing the data to potential unauthorized access and loss. (Note: Duke Health requires a separate review process. Please contact security@duke.edu [2] for more information.)

Duke provides a Service Provider Security Assessment to:

- Establish communications and promote constructive dialogue between Duke and the potential service provider
- Help identify business, technical, security, compliance, legal, and other control factors
- Determine the level of risk inherent to the processing of data beyond the University's physical controls

A security assessment is required in all instances where:

- University data is shared with a service provider
- A service provider captures data for subsequent use by the University

Performing an assessment

The school, department, or business unit provides the service provider with the links to the instructions for completing the security assessment (this page) and to the security assessment document. Service providers are encouraged to respond fully to the questions and return the completed assessment and any supporting materials to the Duke University IT Security Office for review and scoring. The results of the review are provided to the requesting school or business unit, the Office of General Counsel, and Procurement Services. **Please note this process can take up to two weeks.**

Protected data

Where the University's "Sensitive" and/or "Restricted" data is held or processed by a service provider, there is a potentially higher risk where unauthorized access or loss occurs, so additional weight is appropriately applied to those circumstances. For more information see: Duke's Data Classification Standard [3]

Required forms

As part of the risk assessment process, vendors must submit the following:

- **A security self-assessment.** To accommodate documentation a vendor may already have prepared, Duke will accept either of the following options:
    - A?HECVAT-Full [4]?(learn more about the?Higher Education Community Vendor Assessment Toolkit (HECVAT) [5]). The submitted HECVAT-Full should be version 2.04 or higher, and the Analyst Report worksheet must be present as part of the Excel spreadsheet submitted. No other file format will be accepted.
    - A?SOC 2 Type 2 report [6]?performed within the past two years for the vendor themselves (not a cloud service provider such as Amazon Web Services or Microsoft Azure),?plus?a?HECVAT-Lite [7]. The submitted HECVAT-Lite should be version 2.04 or higher, and the Analyst Report worksheet must be present as part of the Excel spreadsheet submitted. No other file format will be accepted.
- **Shibboleth Readiness Profile [8].** Duke requires SAML 2.0 authentication to securely integrate with Duke's Shibboleth authentication service for single sign-on. Vendors must complete this form to determine the level of effort required to integrate a vendor product with Duke's Shibboleth environment.

Instructions for the vendor

Please answer all questions fully.

- Read the HECVAT Instruction Worksheet first to understand the terminology used.
- In the HECVAT, make sure that the Additional Information entry fully answers what is noted as Guidance for each question.
- The HECVAT has several questions that request additional documentation, please make sure these items are returned with your completed HECVAT and the Shibboleth Readiness Profile.

Use of third-party cloud hosting

If the Service Provider uses a third party such as Amazon Web Services or Microsoft Azure, the Service Provider will need to work with that third party to answer questions specific to how and where Duke University data is accessed and/or stored. Answers of N/A are not appropriate for questions affected by such a hosting arrangement.

Please note: All forms and supporting documentation should be returned to the IT Security Office for processing. Duke University will carefully review the responses you provide. The University's decision regarding which providers to select is based, in part, on the information included in your response.

Accordingly, should our discussions proceed to the point of contract negotiation, Duke University will expect you to (i) warrant that the services you provide will be in substantial conformity with the information provided in the response to the Service Provider Security Assessment form; (ii) inform Duke promptly of any material variation in operations from that reflected in your response;

and (iii) agree that any material deficiency in operations from those as described in your response will be deemed a material breach.

Source URL: https://security.duke.edu/vendor-risk-assessment

Links
[1] https://security.duke.edu/vendor-risk-assessment
[2] mailto:security@duke.edu
[3] https://security.duke.edu/policies/data-classification-standard
[4] https://library.educause.edu/resources/2016/10/~/media/files/library/2019/11/HECVATFull211.xlsx
[5] https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit
[6] https://www.netgainit.com/soc-2-type-ii-certification-defined/
[7] https://library.educause.edu/resources/2016/10/~/media/files/library/2019/11/HECVATLite211.xlsx
[8] https://duke.box.com/v/shibbolethReadinessProfile