BYU HAWAII

Church Educational System
Security Operations Center

Vendor Security Risk Assessment Process

Last Updated: 6 August 2025
Document Custodian: John Payne
Chief Information Security Officer
801-422-9099
John_Payne@byu.edu

All vendor agreements that involve sharing BYU–Hawaii's Nonpublic Institutional Data should be cleared through a CES Security Operations Center (SOC) security risk assessment review (SOC Assessment). For existing agreements, the SOC Assessment should be performed as soon as possible. For new and upcoming agreements, the SOC Assessment should be performed prior to signing the agreement. The purpose of the SOC Assessment is to provide a reasonable assurance that BYU–Hawaii's third-party vendors are following good security practices that will keep BYU–Hawaii's data safe. While the SOC Assessment helps minimize the risk of cybersecurity incidents it does not provide a guarantee against such incidents to BYU–Hawaii or the vendor. To begin an assessment, please see https://byuh.teamdynamix.com/TDClient/1902/ithelp/Requests/ServiceDet?ID=49619

During the assessment, a number of questions will be addressed:

- Is the data classification for the shared data Public, Internal, Confidential, or Restricted; as determined by the Data Steward?
- Will PII be shared or included?
- Is the data or application subject to any laws or regulations?
- Does the solution allow for Single Sign On using BYU–Hawaii credentials and/or Multifactor Authentication?
- Does the vendor have a SOC 2 Type II report that can be shared?
- What is the vendor's URL?

A SOC Assessment typically takes one to two weeks, depending on how quickly the above information is provided to the SOC and whether additional controls need to be implemented to ensure the safety of the BYU–Hawaii data.

Note: A similar risk assessment can and should be performed for all BYU–Hawaii hosted systems that house, transmit, or share BYU–Hawaii's nonpublic institutional data. A similar process is followed, with the following additional questions that need to be answered:

- Do servers have a current operating system version and are they patched?
- Are applications being built (where applicable) with a current framework? Are they patched regularly?
- Are server logs being collected centrally and managed appropriately?
- Are data/servers being backed up? Are restores tested regularly?
- A listing of all server names and IP addresses will be needed.