AP 372_ Vendors Risk Management

Reference: ***Education Code Section 70902; Board Policies 3720, 4030; Title 5 Sections 58050, 58164, 58168, 58170, 58172; Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45; FTC Regulations 16 CFR 313.3(n), 16 CFR 314.1-5; Gramm-Leach Bliley Act Sections 501, 505(b)(2); U.S. Code 15 USC 6801(b), 6805(b)(2)***

Date Issued: October 16, 2023

Overview

The Grossmont-Cuyamaca Community College District relies upon a variety of third-party applications, hardware, services, and vendors (third-party systems) to support many of its core business functions. These systems often have direct access to institutional data, networks, and other information systems, thereby presenting an inherent risk to the District. The inclusion and consideration of information security controls is, therefore, an integral part of purchasing and maintaining new and existing third-party systems.

GCCCD has chosen to utilize the Educause's Higher Education Community Vendor Assessment Tool (HECVAT) when assessing risk to the district and its data. Vendor risk is a key element of GLBA compliance along with other state and federal regulations pertaining to personally identifiable information (PII). The HECVAT involves assessing the operations, IT and security controls employed at the vendor. This process assists the district in ensuring the security and privacy of data, especially where sensitive data and PII are involved.

Federal and State Compliance

California community colleges are subject to several federal and state information-security mandates. One such requirement of the Gramm-Leach-Bliley Act (GLBA) is to comply with the FTC Safeguards Rule (16 CFR §314.4[d]), which states that institutions shall:
Oversee service providers, by:

1. Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
2. Requiring your service providers by contract to implement and maintain such safeguards.

In support of this mandate, Project Owners (the individuals or business units endorsing a project) shall be responsible for gathering information for both the Acquisition Planning and Vendor Security Assessment phases of the process before any third-party system is procured, purchased, or otherwise adopted.

Vendor Risk Management Process

Acquisition Planning

During the planning phase, the Project Owner shall address several security-related considerations as part of the District's compliance efforts with GLBA.

1. Does the system integrate with the District's centrally managed authentication services?
2. Does the system support two-factor authentication?
3. Have you identified and classified the information to be provided, accessed, transmitted, or stored to determine appropriate data protection and handling?
4. Have you confirmed that the vendor or external party will not store or transmit protected data (identified above) outside of the U.S.?
5. If the application or system involves credit/debit card payment transactions, have you contacted the Purchasing department regarding payment card compliance?

In the event that a vendor cannot meet minimum information technology or security standards *and* a compensating control cannot be provided to address critical gaps, the Project Owner shall be required to find an alternative solution.

Failure to complete this process may adversely slow the purchasing process as these considerations must be addressed before a Requisition can be completed.

Vendor Security Assessments

Security assessments are a crucial part of managing and understanding risks associated with third-party systems. Vendors must be able to show that they have the proper administrative, physical, and technological safeguards in place to ensure the confidentiality, integrity, and availability of institutional data and related systems.

Project Owners shall be responsible for providing the vendor with a Higher Education Community Assessment Toolkit (HECVAT). Although originally created for cloud applications, the HECVAT has been widely adopted by higher education to assess any service that interfaces with institutional data, information systems, and/ or infrastructure. The completed HECVAT shall be attached to the requisition and approved by the IT team before a Purchase Order is created. The assessment will be reviewed to ensure that:

1. The vendor or system meets District standards and
2. In the event that any gaps are identified, necessary compensating controls are negotiated for and agreed upon.

For the most restricted and internal data, GCCCD requires the completion of the Full HECVAT. For lower risk data and engagements, GCCCD requires the completion of the HECVAT Lite.

In the event that a vendor cannot meet minimum information technology or security standards *and* a compensating control cannot be provided to address critical gaps, the Project Owner shall be required to find an alternative solution.

Existing vendors shall be required to submit an updated security assessment once every two years. Before renewal, if gaps were identified in the prior contract.