Third-Party Vendor Management Policy for IT Commodities

Accommodations for individuals with disabilities in accessing these policies are available upon request by emailing accessiblepolicy@wcupa.edu

Purpose and Scope

The Third-Party Vendor Management Policy for IT Commodities for West Chester University Information Services & Technology computing facilities, systems and resources applies to all members of the University community, including faculty, students, staff, contractors, and affiliates, and to authorized visitors, guests, and others for whom University technology resources and network access are made available by the University. This policy also applies to campus visitors who avail themselves of the University's temporary visitor wireless network access service or eduroam access, and to those who register their computers and other devices through Conference Services programs or through other offices, for use of the campus network.

Policy Statement

The purpose of this policy is to identify external companies, offering IT services, software, support, or physical assets, that potentially pose a risk to West Chester University through increased exposure or creating new avenues for cyber-attackers to utilize. Information Services & Technology will verify that appropriate controls are in place to minimize risk that could adversely affect the Confidentiality, Availability, and Integrity of University data and resources

through consistent evaluation and performing due diligence on each third-party vendor,

This policy applies to all prospective vendors entering into a purchase or service agreement with West Chester University for any IT services, software, support, or physical assets regardless of cost of acquisition and implementation and must undergo an IS&T (Information Services & Technology) risk review prior to the purchase and use of the product or service.

While West Chester University utilizes third-party products and services to support its mission and goals, it is imperative that each vendor be evaluated to ensure that the appropriate capabilities exist to properly protect University data and resources. Vendors, and the products offered, will be evaluated based on their security capabilities and documentation, classification of the data involved, the implementation or utilization of the products, and any other criteria that IS&T, Procurement or PASSHE (Pennsylvania State System of Higher Education) Legal find relevant to the information security impact of the product.

Policy Framework

All University departments engaging third party IT products or services are required to undergo a security risk review of the requested product or service. The third-party vendor must provide copies of relevant contracts, end user agreements, and/or public security and privacy documentation. Also, most vendors will be required to complete a security questionnaire, known as the Higher Education Community Vendor Assessment Tool (HECVAT) lite version

and/or provide a copy of their most recent independent security audit or certification reports (i.e., SOC (Service Organization Controls) 2 or ISO 2700x certification).

The Information Security Office will review the security documentation and determine whether the third-party vendor complies with the University security requirements. Factors that will be considered include but are not limited to the method of access and implementation, data classification of the information involved, and types of users that will utilize the product. If the third-party vendor is non-compliant, compensating controls will need to be implemented and reassessed. The implementation and use of the product or service is contingent on the successful implementation of compensating controls.

Subsequent reviews of third-party vendors will be required in advance of any renewal period of previously approved and implemented products. This will ensure that the continued compliance and adequate security posture of each offering is maintained.

Definitions

Availability: The principle of ensuring timely and reliable access to and use of Information based upon the concept of Least Privilege.

Confidentiality: The principle of preserving authorized restrictions on Information access and disclosure, including means for protecting personal privacy and proprietary information.

Data: Element(s) of information in the form of facts, such as numbers, words, names, or descriptions of things from which "understandable information" can be derived.

Integrity: Ensuring records and the Information contained therein are accurate and Authentic by guarding against improper modification or destruction.

Third-Party Vendor: Third party as an external entity, including, but not limited to, service providers, vendors, supply-side partners, demand-side partners, alliances, consortiums, and investors, with or without a contractual relationship to West Chester University or the PA State System of Higher Education Office of the Chancellor.

References

Acceptable Use Policy
http://www.wcupa.edu/policies/documents/Acceptable%20Uses%20of%20Electronic%20Signatures%20Policy.pdf

Information Technology Procurement Policy
http://www.wcupa.edu/policies/documents/Information%20Technology%20Procurement%20Policy.pdf

HECVAT - https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit

Reviewed by: Information Services & Technology

Policy Owner: **Stephen Safranek**

Chief Information Security Officer
Information Services & Technology

Office of Labor Relations Review: Review completed December 27, 2022

Approved by:

JT Singh
Senior Associate VP & CIO
Information Services & Technology
Date: October 13, 2023

Effective Date: **November 15, 2023**

Next Review Date: October 13, 2027

History:

Initial Draft: 11/1/2022

Initial Approval: 12/27/2022

Review Dates: 11/1/2022, 10/14/2023, 11/15/2023

Amended: 11/15/2023