



CHRISTOPHER NEWPORT

UNIVERSITY

Third Party Vendor Risk Management Standard

VERSION 1.1

June 2023
Department: Information Security

Proprietary Statement

This document was developed specifically for and by Christopher Newport University. The concepts and methodologies contained herein are proprietary to Christopher Newport University. Duplication, reproduction, or disclosure of information in this document without the express written consent of Christopher Newport University is prohibited.

All Trademarks, Registered Trademarks, Service Marks, and brand and product names used in this document are the property of their respective owners.

© Copyright 2022 Christopher Newport University. All rights reserved.

Third Party Vendor Risk Management Standard

Review and Revision History

Date	Version	Description of Change (Affected Sections)	Author
9/30/2022	1.0	Initial Release	Wendy L. Corrice
June 2023	1.1	Annual Review	Wendy Wilde

TABLE OF CONTENTS

Introduction	4
Purpose	5
Scope	5
Roles and Responsibilities	5
Standards Statement	6
Required Risk Assessment	6
Alternative Assessments	7
Third Party Management	7
a. Initial Screening	7
b. Comprehensive Security Assessment	7
c. Contracting Agreements	8
d. Subsequent Reviews	8
Enforcement	8
References	8
Definitions	9
APPENDIX A - DATA CLASSIFICATION MATRIX	11
APPENDIX B - VENDOR ASSESSMENT REQUEST FORM	11

Third Party Vendor Risk Management Standard

Introduction

The Vendor Risk Management Standard is an initiative to reduce the risk to Christopher Newport University data and computing resources from third party providers. The university's Information Security Office collaborates with the IT Services Project Management Office, the Business Office, and the Office of Procurement, to protect information technology resources and digital intellectual property of Christopher Newport University.

Purpose

The purpose of this standard is to establish minimum-security standards for the initial and ongoing review and implementation of third party systems. This standard shall be applied to all university third party vendors and service providers in order to maintain the confidentiality, integrity and availability of university data.

Scope

- a. This standard applies to all university operations involving all university data, including regulated data, for example; GLBA, PCI-DSS, FERPA, HIPPA, PHI and PII.
- b. This standard applies to all university faculty and staff.

Roles and Responsibilities

Role	Responsibilities
University Departments	<ul style="list-style-type: none">● Prior to engaging a vendor, consult with the IT Service Project Management Office to see if an existing solution exists.● Participate in the Technology Vetting Program prior to procurement.● Provide the information necessary to perform a Risk Assessment prior to procurement to the Information Security Office.● Perform a review of the Risk Assessment annually.● Provide the information to perform a Risk Assessment to Information Security to perform a full Risk Assessment every three years.
Information Security Office	<ul style="list-style-type: none">● Oversees the Third Party Vendor Management process.● Performs pre-procurement Risk Assessments.● Documents Risk Assessment results from Technology

Third Party Vendor Risk Management Standard

	Vetting requests.
Information Technology Services Project Management	<ul style="list-style-type: none"> ● Manage the Technology Vetting Program. ● Coordinate with requestor, Office of Procurement and Information Security during Technology Vetting.
Office of Procurement	<ul style="list-style-type: none"> ● Ensure all hosted systems/service providers meet all VITA approved contract language. ● Ensure contracts for all cloud hosted systems must include language stating that the supplier will comply with all applicable VITA security standards
Business Office (ARMICS)	<ul style="list-style-type: none"> ● Coordinate with university departments working with third party vendors subject to the PCI-DSS (Payment Card Industry Data Security Standard) on annual risk assessments. ● Coordinate with the Information Security Office on pre-procurement risk assessments for PCI-DSS third party hosted providers. ● Coordinate with PCI-DSS vendors on periodic/annual SOC2 or other security assessments.
Vendor/Supplier	<ul style="list-style-type: none"> ● Comply with the VITA Security Standards (SEC525). ● Provide annual audits, Service Organization Control Type II (SOC2) or equivalent audit reports. ● Notify Christopher Newport University of any security breach via contractually agreed upon procedures. ● Ensure that the University data, including all system components and services remain within the continental United States. ● The vendor shall be subject recurring Risk Assessments at least annually or immediately following an incident that is classified as significant, and provide security assessments upon request.
System Administrator	<ul style="list-style-type: none"> ● Responsible for managing the third party hosted application. ● Participate in the annual system risk analysis process with the data and system owners ● Ensure vendors provide vulnerability scan reports,

Third Party Vendor Risk Management Standard

	monthly activity logs and forward to the Information Security Team
--	--

Standards Statement

Required Risk Assessment

University departments engaging third party vendors who process, store, or transmit data classified as Class 1 or Class 2 according to the Data Classification Standard, must work with their vendor to collect the necessary security assessments. Assessment should be routed to the Information Security Office to complete a risk assessment and review, prior to procurement and as part of the Technology Vetting procedures. (See Appendix A for the Data Classification Matrix)

The vendor's SOC2 Type II report must cover a time period within 6-months of the request. If the SOC2 Type II report is not within six months of the date requested, then the vendor must provide a bridge letter (see definitions)

After receiving the report, the department must forward the security assessment to the Information Security Officer at iso@cnu.edu

Alternative Assessments

In cases where a SOC2 Type II report is unavailable from a vendor:

- a. The vendor may submit an external security assessment or alternative self assessment provided:
 - i. The controls in the assessment are representative of the vendor's current state.

Third Party Management

a. Initial Screening

- i. All university departments engaging third party IT products or services are required to participate in the Technology Vetting process. Technology Vetting helps to reduce risk, avoid redundancy and improve customer support for campus technology needs. The process provides a centralized and streamlined process to allow University employees to submit technology-related proposals with approval from the relevant area Vice President or the Provost. Additionally, this process will also ensure that the University maintains compliance with the Commonwealth of Virginia's information security and procurement requirements.
- ii. Based on the information provided during the Technology Vetting process, the Information Security Officer will determine the data classification if a vendor security assessment is required. (See APPENDIX B - Vendor Assessment Request Form)

Third Party Vendor Risk Management Standard

b. Comprehensive Security Assessment

- i. The Third Party vendor must provide either a SOC2 Type II or alternative security assessment such as a HECVAT.
- ii. The Information Security Team will review the security assessment and determine whether the Third Party vendor complies with university and VITA security requirements.
- iii. If the Third Party vendor is not compliant, the procurement may not proceed until compensating controls are assessed and implemented.
- iv. The Information Security Officer will perform a pre-procurement Risk Assessment based on the information submitted during the Technology Vetting process and provide the result to the Project Management Team based on the [Third Party Risk Management Procedures](#).

c. Contracting Agreements

- i. Procurement will confirm contractual language conforms to Christopher Newport University and Virginia Information Technology Agency (VITA) standards.
- ii. Procurement will verify that the vendor agrees to comply with all provisions of then-current Commonwealth of Virginia security procedures, published by the Virginia Information Technology Agency (VITA).

d. Subsequent Reviews

- i. Annual security reviews will be conducted on third party vendors will be performed
- ii. Monthly reviews of activity logs related to the operation of service will be performed by the CNU system administrators of the Third Party system and provide monthly reports to the Information Security Officer.
- iii. Third party vendors shall conduct and supply vulnerability scan reports to the system administrator at least once every 90-days.
- iv. System administrators should provide vulnerability scan reports and annual security assessments reports to isoreports@cnu.edu.
- v. Security assessments and related documents will be stored for the duration of the contract.

Enforcement

Non-compliant third party vendors may be considered to be in default (see definition below).

All procurements and contracts entered into by Christopher Newport University are governed in all respects by the laws of the Commonwealth of Virginia, without regard to its choice of laws provisions, and any litigation with respect thereto shall be brought in the circuit courts of the Commonwealth. The agency and the contractor are encouraged to resolve any issues in controversy arising from the award of the contract or any contractual dispute using Alternative

Third Party Vendor Risk Management Standard

Dispute Resolution (ADR) procedures ([Code of Virginia, § 2.2-4366](#)). ADR procedures are described in Chapter 9 of the Vendors Manual. The contractor shall comply with all applicable federal, state and local laws, rules and regulations.

References

[SEC525 Commonwealth of Virginia's Hosted Environment Information Security Standard](#)

[Code of Virginia 2.2-4366](#)

[Christopher Newport University Data Classification Standard](#)

[Information Security Vendor Assessment Request Form](#)

[Third Party Vendor Risk Management Procedures](#)

Next Review Date: June 2024

Third Party Vendor Risk Management Standard

Definitions

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

Bridge Letter: A bridge letter is a letter from a vendor that attests to the continued validity and accuracy of the provided external assessment (no significant changes in their environment or threat landscape) between the report end date and the current date.

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

Contractor: A person or a company that undertakes a contract to provide materials or labor to perform a service.

Data: Information collected, stored, transferred or reported for any purpose, whether electronically or via hard copy.

Default: A contractor may be considered in default if it fails to perform in accordance with the terms and conditions of the contract or purchase order. Any non-delivery or non-conformance to a contract is considered a breach to the contract. The University shall give the contractor and its surety ten (10) calendar days via a verbal or written notice, during which the contractor and/or his surety may rectify the deficiency. If a satisfactory resolution is not reached, the University will terminate the contract for default and it shall become effective at the end of the ten-day (10) notice period. In the alternative, the University may postpone the effective date of the termination notice, at the University's discretion, if the University should receive reassurances from the contractor and/or its surety that the causes for termination will be remedied in a time and manner which the University finds acceptable. If at any time more than ten (10) days after the notice, the University determines that contractor and/or its surety has not or is not likely to rectify the causes for termination in an acceptable manner or within the time allowed, then the University may immediately terminate the contract for cause by giving written notice to the contractor and its surety. In no event shall termination for default terminate the obligations of the contractor's surety on its payment and performance bonds. As an agency of the Commonwealth of Virginia, Christopher Newport University can terminate a contract for default and may hold the contractor liable for any excess costs.

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

Third Party Hosted Provider: External vendors who process, store, or transmit data classified as Class 1 or Class 2 according to the Data Classification Standard. Third party as an external entity, including, but not limited to, service providers, vendors, supply-side partners, and investors, with or without a contractual relationship to university.

SAAS: Software as a service is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted.

SOC 2: SOC 2 is a voluntary compliance standard for service organizations, developed by the American Institute of CPAs (AICPA), which specifies how organizations should manage customer data. The standard is based on the following Trust Services Criteria: security, availability, processing integrity, confidentiality, privacy.

Third Party Vendor Risk Management Standard

System Administrator: The System Administrator is an analyst, engineer, or consultant who implements, manages, and/or operates a system or systems at the direction of the System Owner, Data Owner, and/or Data Custodian. The System Administrator assists agency management in the day-to-day administration of agency IT systems, and implements security controls and other requirements of the agency information security program on IT systems for which the System Administrator has been assigned responsibility.

University Data: Information collected, manipulated, stored, reported or presented in any format, on any medium, by any unit of the University.

VITA: Virginia Information Technology Agency (VITA)

Third Party Vendor Risk Management Standard

APPENDIX A - DATA CLASSIFICATION MATRIX

CNU ITS will develop and work with Data Owners to create a department or application specific classification matrix. For example, the matrix below classifies data into the appropriate categories. The matrix also accounts for the risk or exposure the University may be subjected to in the event of a disclosure of data to unauthorized parties.

Classification	CLASS 1	CLASS 2	CLASS 3	CLASS 4
	Information that are restricted, with the highest Security\Privacy Requirements	Information that are confidential, with moderate security\privacy requirements	FERPA directory information and other confidential business information	Information that may have some minor sensitivity but are not regulated by laws and contracts; as well as public information
Examples	SSN Passport Driver's License Passport Health Insurance Gramm-Leach-Bliley Act (GLBA) Covered information (nonpublic personal information) Tuition payments and/or financial aid) containing personally identifiable information (PII) *Payment Card holder data (PCI-DSS) *Medical treatment/diagnoses and history (HIPPA/PHI) Presidential working papers	Grades and GPA Class schedule Class Roster Transcripts Student Conduct record	Internal business documents under NDA Internal intellectual property Some university financial data Business process documents FERPA Directory Information may include: *Name * Date of birth * Photograph * Major field of study * Participation in officially recognized activities * Weight and height of athletic team members * Dates of attendance * Degrees, honors, and awards received * The most recent educational institution attended * Date Admitted * Degree sought	Enrollment numbers ready to be published Public reports
Risk	HIGH	HIGH	MEDIUM	LOW
Access	Authorized individuals with approved access	Authorized individuals with approved access	CNU employees and non-employees with a business "need to know"	CNU affiliates and general public with a "need to know"


APPENDIX B - VENDOR ASSESSMENT REQUEST FORM

Third Party Vendor Risk Management Standard

Vendor Assessment Request Form Link - [HERE](#)

Vendor Assessment Request Form

The following information is being requested as part of the 3rd party vendor assessment process to ensure appropriate protections and safeguards of University information. Responses will be reviewed by the Information Security Officer to determine if additional steps, reviews or contract language is necessary to meet university or regulatory requirements. You will be notified if additional action on your part is required. Thank you.

 wendy.murray@cnu.edu (not shared) [Switch account](#) 

* Required

Requestor's Name: *

Your answer

Requestor's E-Mail Address: *

Your answer