Purpose

The purpose of this policy is to ensure that all systems procured by the University meet the required standards as outlined by both the Virginia Information Technology Agency (VITA) and are compliant with the National Institute of Standards and Technology (NIST) for third party, cloud-based systems. The policy includes the University's guidelines for evaluating third party and/or cloud services for both existing contracts and for future procurements.

Guiding Principles

The guiding principles for this policy is ensure that third party vendors that supply automated systems and/or computerized services to the University are compliant with NIST, VITA and University governance. Each vendor must supply an annual audit review in the form of a SOC 2 Report, which includes the vendor controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy.

Scope of Policy

This policy applies to all third party systems/services, whether hosted externally at a vendor site, cloud-hosted, or on-premises at the University

Responsibility and Duties

A. Agency Requirements

Technology Services will be responsible for the following:

a) Ensure that each vendor completes the VSU Vendor Checklist during the evaluation process within the Initiation Phase of the System Development Life Cycle (SDLC).

b) For cloud-hosting systems/services, once the initial evaluation is completed by VSU Technology Services, a pre-authorization must be completed and submitted to VITA. This pre-authorization is initiated by completing the *VITA Enterprise Cloud Hosting Form.*

c) Because the VITA approval is only valid for one year (unless otherwise noted), an annual evaluation of each vendor is required to ensure that the vendor is still compliant with Commonwealth of Virginia policy and NIST standards and policies.

d) For cloud-hosted systems/services, VSU will conduct periodic reviews to ensure continued adherence to University and VITA standards and policies.

e) Any exceptions will be logged and stored on file at the University for a period of one year. At the end of the one year period, an evaluation will be completed to ensure that the exception is still required. If the exception is still required, an additional exception will be filed or modifications to the vendor's contract will be requested to ensure compliance.

B. Agency Requirements

The Vendor/Supplier will be responsible for the following:

a) For "hosted" systems/service providers, the vendor/supplier is responsible for complying with *Hosted Environment Information Security Standard (SEC 525-02); Information Security Policy (Sec 501-09.1); IRS Publication 1075 and NIST Risk Management Framework*.
b) Ensuring that they are compliant with relevant and mandated-third party standards such as Health Insurance Portability and Accountability Act (HIPPA), Federal Tax Information (FTI) and Payment Card Industry Data Security Standard (PCI DSS) are to be detailed within the supplier's assessment response
c) Vendor shall supply annual audits, Service Organization Control Type 2 (SOC 2) or equivalent external audit report.
d) Notifying the University and VITA of any security breach via the contractually agreed to procedures.
e) The University shall at all times maintain control of University data. In the event of a breach of contract or default, the Vendor must provide the University its data in the agreed upon format per the original Statement of Work (SOW).
f) The Vendor shall ensure that the University data, including all system components and services, remain within the continental United States.
g) The Vendor shall be subject to recurring Risk Assessments at least annually, but immediately following an incident that is classified as significant (i.e. that could impact University data).

C. Procurement/Acquisitions:

For procurements/acquisitions:

a) For "hosted" systems/service providers, all contract language must meet VITA approval
b) For all cloud-hosted systems, contracts must include language stating the supplier will comply with all applicable, federal regulations, Commonwealth of Virginia laws, security requirements and industry standards and regulations. Appropriate language will be included in the contract to outline the Vendor's responsibilities to all applicable standards and regulations.

Acronyms:

Additional IT security definitions and terms can be found in the COV ITRM IT Glossary. It is referenced on the ITRM Policies, Standards, and Guidelines web page on www.vita.viminia.gov/library.

FTI	Federal Tax Information
HIPPA	Health Insurance Portability and Accountability Act
NIST	National Institute of Standards and Technology
PCI DSS	Payment Card Industry Data Security Standard
SOW	Statement of Work
VITA	Virginia Information Technologies Agency

Title: Vendor Management Policy Policy: 6820

Policy Review

This policy will be reviewed every two years on the anniversary of the policy effective date or more frequently as needs of the University warrants.

References

Virginia Information Technology Agency VITA):

Information Security Standard (SEC 501-09.1)
Hosted Environment Information Security Standard (SEC 525-02)

12-18-2017

Approval By: _____ **Date:** _____
President