Policy Title: Third-Party Security Assessment Policy	**Effective Date: 10/1/2025**
Policy Number: IT-PO-1505	**Date of Last Review: N/A**
Oversight Department: Information Technology Services	**Next Review Date: 10/1/2028**

1. PURPOSE

The *Third-Party Security Assessment Policy* for Radford University (University) outlines the information security assessment requirements for the acquisition or use of information technology products and services involving University data that is stored, processed, or transmitted by a Third-Party Provider.

2. APPLICABILITY

This policy applies to all systems, regardless of the technology, that store, process, or transmit University data by a Third-Party Provider. This policy also applies to all members of the University community.

3. DEFINITIONS

HECVAT - The Higher Education Community Vendor Assessment Toolkit™ is a comprehensive questionnaire that vendors can complete to provide a detailed picture of their cybersecurity, privacy, and compliance standards.

Highly Sensitive Data - University data which, because of its potential risk in the event of disclosure, alteration or destruction, is approved for use only on a very limited basis and with special security precautions. This includes personally identifiable information that can lead to identity theft exposure. The following data is defined as Highly Sensitive:

a. Social Security Number,
b. Driver's license number or state identification number issued in lieu of a driver's license number,
c. Passport or Visa information/number
d. Financial bank/account numbers, credit card or debit card numbers; or
e. Health information, that if exposed, can reveal an individual's health condition and/or history of health services use.

Information Security Incident - An adverse event or situation, whether intentional or accidental, that poses a threat to the integrity, availability, or confidentiality of an IT system.

Sensitive Systems – systems where confidentiality, integrity or availability are rated as High.

SOC 2 (System and Organization Controls 2) Report– a report issued by an independent auditor that evaluates how well a company's systems and processes protect customer data over time, specifically focusing on security, availability, processing integrity, confidentiality, and/or privacy.

System – An interconnected set of IT resources under the same direct management control.

Third-Party Provider – A company or individual that supplies IT systems, or services to the University and is not a Commonwealth of Virginia entity, whether they are paid or not.

Third-Party/Cloud-Hosted Systems - IT resources—such as software, applications, platforms, or infrastructure—which store, process, or transmit University data, but are controlled or managed by a Third-Party Provider.

University Community – For the purpose of this policy, all persons who are employees, students, contractors, volunteers, and visitors, including invited guests, of the University.

4. Policy

A. All Third-Party/Cloud-Hosted systems must have an information technology security assessment before being acquired or initially used to store, process, or transmit University data.

B. University community members must follow the procedures outlined herein to ensure that any Third-Party/Cloud-Hosted System that they wish to use to store, process, or transmit University data has had an information technology security assessment performed by, and the Third-Party/Cloud-Hosted system has been approved by the Information Security Office prior to being acquired or initially used.

C. The Information Security Office will determine the system classification of the Third-Party/Cloud-Hosted System and perform a security assessment based upon that classification.

D. The Information Security Office will approve or deny the acquisition or initial use of the Third-Party/Cloud-Hosted system.

5. PROCEDURES

A. Before the Acquisition or Initial Use of a Third-Party/Cloud-Hosted System:

a. The department or University community member wishing to acquire or initially use the system (Requestor) will fill out the System and Data Classification Questionnaire available online at: https://radford.qualtrics.com/jfe/form/SV_eVQUPebHySaK3Ot.

b. Results will be electronically submitted to the Senior IT Procurement Officer in Procurement and Contracts and to the Information Security Office to initiate the security assessment. This form will also be used by the Information Security Office to determine the sensitivity of the system and identify the system classification.

c. If the system is a **Third-Party or Cloud Hosted System**, the Requestor will obtain the appropriate documentation (Examples: SOC2, HECVAT) from the third-party vendor.
d. All purchases must follow Procurement and Contracts policies and procedures.

B. System Assessment and Results

1. Upon receipt of the third-party provider's documentation, the Information Security Office will assign a classification of Sensitive System or Non-Sensitive System and conduct the security assessment. The requirements that the system must meet are primarily based upon the assigned classification.
2. The system assessment will consist of an examination of the vendor's documentation, and should include evidence provided by an external assessment, such as a SOC2 Report and an internal assessment such as a HECVAT.
3. The Information Security Office will document the assessment findings and, upon completion of the assessment, provide a determination to Procurement and Contracts and the Requestor.
4. The following categories of determination will be used:
    a. Approved - no issues with assessment.
    b. Approved with compensating controls – *approved only if* the specified compensating controls are put in place to mitigate risks identified during the security assessment.
    c. Approved with an approved Exception Request - Exception Requests must be submitted, reviewed, and approved in accordance with exception procedures outlined in Section 1.5 of the Radford University Information Technology Security Standard 5003s-01.
    d. Failed – Vendor has failed the assessment, and the system cannot be utilized.

C. Other Required Security Assessments

1. In addition to the initial Security Assessment, the University requires other assessments to be performed. These requirements are based upon the system classification. Specifically,
2. Sensitive Systems
    a. Annual security assessments are required and are performed by the Information Security Office.
    b. Additional security assessments will be performed when 1) a significant system change, such as changing the type of data being stored (highly sensitive data) or the transfer of the system to a new Third-Party Provider or platform, or 2) when an Information Security Incident, such as a data breach, has occurred.
3. Non-Sensitive Systems
    a. Additional security assessments will be performed when 1) a significant system change, such as changing the type of data being stored (highly sensitive data) or the transfer of the system to a new Third-Party Provider or platform, or 2) when an Information Security Incident, such as a data breach, has occurred.
4. The Information Security Office will document the assessment findings and, upon completion of the assessment, provide the determination to Procurement and

Contracts and the Requestor, using the same determination categories as noted in 5.B.4. above.

D. Documentation of Security Assessments

1. The Information Security Office will maintain documentation of all security assessments and related supporting documentation in accordance with the retention requirements of the Library of Virginia.

6. EXCLUSIONS

None

7. APPENDICES

None

8. REFERENCES

Information Technology Security Standard IT-5003s-01
Information Technology Data and System Classification Standard IT-PO-5102s

9. INTERPRETATION

Information technology is managed under delegated operational authority granted to the University by the Virginia General Assembly, as set forth in the Restructured Higher Education Financial and Administrative Operations Act, § 23.1-1000 et seq. of the Code of Virginia, and Chapters 824 and 829, Acts of Assembly, 2008. The Board of Visitors (Board) approved the University to operate under this delegated authority in Board resolutions dated April 23, 2009, and May 4, 2012. Accordingly, the authority to interpret this policy rests with the President of the University and is generally delegated to the Vice President for Finance and Administration & Chief Financial Officer.

10. APPROVAL AND REVISIONS

The *Third-Party Security Assessment Policy* was initially approved by the President's Cabinet on September 22, 2025

For questions or guidance on a specific policy, contact the Oversight Department referenced in the policy.