Virginia Tech IT Vendor Risk Assessment Standard

1. Purpose and Scope

Virginia Tech is committed to protecting the privacy of its community as well as protecting the confidentiality, integrity, and availability of information important to the university's mission. The IT Vendor Risk Assessment Standard specifies the information security evaluation requirements for the acquisition and utilization of information technology products and services in which university data is stored, processed or transmitted by a commercial vendor, service provider, or any entity not under control of the university. Typically, this includes outsourced services, server hosting, Managed Service Providers (MSPs), Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Function as a Service (FaaS) and other related Cloud Computing services.

2. Standard

2.1 Vendor Software Security Risk Assessment

The Virginia Tech Risk Classification Standard shall be used to determine the appropriate classification for the vendor's software/service based on the classification of the university data being entrusted to the vendor. The general security evidence requirements for each classification are shown in *figure 1*.

Classification and Security Evidence Requirements		
HIGH	High-Risk Vendor Service	Required Security Evidence
	Vendor service handles "High-Risk" university data.	Higher Education Community Vendor Assessment Toolkit (HECVAT) - "Full" version. HECVAT "Lite" acceptable at discretion of ITSO. Service Organization Controls (SOC) 2 Type II report Copies of information security policies and procedures, application architecture/data flow diagrams, penetration tests/vulnerability scans, business continuity/disaster recovery (BC/DR) plans, etc.
MODERATE	Moderate-Risk Vendor Service	Required Security Evidence
	Vendor service handles "Moderate-Risk" university data, but no "High-Risk" university data.	HECVAT - "Full" or "Lite" at discretion of ITSO SOC 2 Type II, SOC 2 Type I or SOC 3 report optional based on availability. ISO 27001:2022 ISMS Certificate of Registration/Certification may also be considered a suitable alternative to SOC 2 Type I/SOC 3 report.
LOW	Low-Risk Vendor Service	Required Security Evidence
	Vendor service handles *only* "Low-Risk" university data (appropriate for public use).	None required, supplied evidence will be reviewed if provided.

Figure 1: Classification and Security Evidence Requirements

Note: SOC reports must cover a time period within 6-months of the request from VT. If the SOC report is not within six months of the date requested, then the vendor/service provider shall provide an accompanying bridge letter.

The IT Security Office (ITSO) shall review and evaluate the security evidence provided by the vendor/service provider to ascertain compliance with university policies and standards, relevant data protection addendum(s), vendor's privacy policy, and relevant laws and regulations; and to identify areas of weakness in security controls which could create a risk to the confidentiality, integrity, and/or availability of university data. The ITSO's evaluation will be conducted in the context of the use case for the software/service as documented by the requestor/service owner in the department procuring the service.

The ITSO will also review security evidence obtained using various "open-source intelligence (OSINT)" and/or "third-party risk management (TPRM)/vendor risk management (VRM)" tools and capabilities to identify potential security risks/vulnerabilities in the vendor/service provider's Internet-facing systems and to help formulate an understanding of the vendor's "cyber hygiene" as it relates to their observable use of current cybersecurity best practices. These activities are always entirely non-intrusive, utilize only information collected from the public domain, and are not considered activities that constitute penetration testing. As such, these review activities are not intended to inform all potential security risks nor are they intended to act as a preventive, detective, or corrective security control on their own, but rather serve to help inform risk-based decision-making processes. The extent of OSINT/TPRM activities performed in individual assessments will vary based on numerous factors.

Where potential deficiencies in security controls are discovered, or where gaps exist in the evidence that adversely impacts the ITSO's ability to ascertain the state of a security control, the ITSO will engage the vendor/service provider to validate the concerns/issues detected as they relate to the vendor's systems and services where university data is stored, processed or transmitted, and to determine appropriate remediation actions for the vendor, to include the application of compensating controls, where appropriate. If remediation of any identified security deficiencies is not possible and the application of compensating controls is not possible to mitigate risk, the ITSO will document the presence of residual risk. Residual risks shall be subject to further risk analysis, and ultimately risk treatment.

2.1 Risk Analysis

The Virginia Tech IT Risk Assessment Standard defines the risk model and risk analysis process used to determine the severity of information security risk based upon the combination of factors of "**Likelihood**" - the probability that a given threat is capable of exploiting a given vulnerability, and "**Impact**" - the magnitude of harm that can be expected to result from the consequences of the risk event occurring. The ITSO shall determine, in coordination with the vendor, contract administrator, and applicable data stewards when necessary, the appropriate likelihood and impact values to assign the risk based on the context of the use case for the software/service as documented by the requestor/contract administrator, and that combination shall determine the appropriate effective risk severity rating for the risk (see the Virginia Tech IT Risk Assessment Standard for details on risk severity ratings).

2.2 Reporting

The ITSO will issue an opinion based upon the evidence reviewed as to the suitability of the vendor/service provider's security controls relative to the documented business use case and risk classification and will provide details of the review to include any risks discovered and any adjustments made by the vendor during the review. Any residual risks listed in the report shall be assigned a risk severity rating based upon the outcome of the ITSO's risk analysis.

2.3 Risk Ownership, Risk Acceptance, and Risk Treatment

Figure 2 establishes the stakeholder responsibilities in ownership and acceptance of residual security risks based upon the assigned risk severity rating. Risk acceptance is a business decision to accept the potential risks and associated outcomes of a particular security threat rather than treating it further. Named data trustees and data stewards are listed in the Standard for Administrative Data Management. Risk acceptance documentation shall be maintained by the ITSO.

Risk Ownership and Risk Acceptance	
Negligible-Severity Risk	Negligible-Severity and Low-Severity risks are owned by the service owner in the department procuring the service. These risks can be accepted by the applicable department head with a written acknowledgement (e.g. email or response in ticket system).
Low-Severity Risk	
Moderate-Severity Risk	Moderate-Severity risks are owned by the service owner and/or any applicable data steward(s). These risks can be accepted by the department head OR relevant data steward(s) if applicable, with a written acknowledgement.
High-Severity Risk	High-Severity risks are owned by applicable data steward(s) in coordination with the data trustee(s), department head, and the ITSO. Risk acceptance shall be carefully considered amongst relevant stakeholders and documented as necessary.
Major-Severity Risk	Major-Severity are owned by the VT IT Risk Governance Committee. Major-Severity risks may potentially threaten the university's mission and cannot be accepted; these risks must be treated.

Figure 2: Risk Ownership and Risk Acceptance

Risk treatment efforts shall be undertaken to mitigate documented unaccepted risks, using appropriate administrative, technical and/or physical security controls. Valid risk treatment options are:

1. **Mitigation** – Apply controls to reduce the impact of the risk event's potential consequences and/or the likelihood that it will occur.
2. **Avoidance** – Eliminate the conditions that allow the risk to exist.
3. **Transference** – Transfer liability (partially or wholly) of the risk event's potential consequences to another party.

Risk treatment decisions, including all related corrective action plans, should take account of the legal-regulatory and private certificatory requirements; organizational objectives, operational requirements and constraints; and the costs associated with implementation and operation relative to the risk being reduced. All risk treatment decisions are subject to approval of the University IT Security Officer.

2.4 Related Requirements and Periodic Reassessment

- University business units engaging vendors/service providers to handle Virginia Tech data must comply with all Virginia Tech IT Procurement policies and procedures. Additionally, contract administrators/service owners are responsible for ensuring the appropriate security evidence is obtained from the service provider and made available to the ITSO for assessment and review.

- Business units engaging vendors/service providers to handle the Social Security Number and the Individual Taxpayer Identification Number (collectively abbreviated as "SSN") must comply with University Policy No. 1060 – "Policy on Social Security Numbers", and shall obtain and submit appropriate security evidence for ITSO assessment and review on an **annual basis**.

- Business units collecting nonpublic personal financial information from a customer seeking to obtain a financial product or service as described in the Gramm-Leach-Bliley Act (GLBA), must comply with all related responsibilities in University Policy No. 7025 – Safeguarding Nonpublic Customer Information, and shall obtain and submit appropriate security evidence for ITSO assessment and review on an **annual basis**.

> *This standard supports the GLBA "Safeguards Rule" [1] requirements related to risk assessment by ensuring that agreements with third-party contractors who have access to nonpublic personal financial information collected by or on behalf of the university contain safeguarding provisions and periodically assessing those service providers based on the risk they present and the continued adequacy of their safeguards.*

- Business units engaging vendors/service providers to, either directly, or indirectly via a subservice provider, process, store, or transmit credit card information (a.k.a. "PCI data" or "cardholder data (CHD)") must comply with University Policy No. 3610 – "Accepting and Handling Payment Card Transactions" and appropriate PCI-DSS Attestation of Compliance (AoC) must be provided for review and approval by the designated University Payment Card Coordinator in the Bursar's Office.
- Business units engaging vendors/service providers through ACH payments must comply with the Automatic Clearing House (ACH) Payment and Security procedure and shall obtain appropriate evidence that their payment provider complies with the NACHA Account Validation Rule described in the procedure. Documentation from the provider confirming their compliance should be kept on file in the department for audit purposes.
- Business units engaging vendors/service providers to handle research data subject to United States export regulations including International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR), Export and Import of Nuclear Equipment and Materials Regulations (EINEMR), Assistance to Foreign Atomic Energy Activities Regulations (AFAEAR), Foreign Assets Control Regulations (FACR), National Industrial Security Program Operating Manual (NISPOM) and/or other applicable export control, sanction, or security related laws, regulations, or orders must comply with University Policy No. 13045 – "Export Control, Sanctions, and Research Security Compliance Policy".

2.5 Exceptions

- Vendors/service providers being engaged for use cases where the only student academic record information being handled is data designated as "directory information" (see https://www.registrar.vt.edu/FERPA.html) are not required to have a documented acceptance of risk based solely on the absence of a SOC 2 Type II report as long as the service can integrate with Virginia Tech's single sign-on (SSO) service.

3. Maintenance and Enforcement of Standard

As cybersecurity is a rapidly evolving field that continuously presents us with new challenges, this standard will be revised and updated accordingly by the Information Technology Security Office. Any exception to this standard must be approved by the University IT Security Officer. Questions may be directed to itso@vt.edu.

4. References

1. FTC Safeguards Rule implementing sections 501 and 505(b)(2) of the Gramm Leach-Bliley Act: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

5. Revisions

Version 1, published August, 2024