DOMINICAN UNIVERSITY
Information Technology

General Information		
Title Vendor Risk Management and Data Classification		**Category**
Responsible Department Information Technology	**Responsible Officer** Chief Information Officer	**Effective Date** July 01, 2023

I. Scope

The following categories of the University community should be familiar with this policy:

- ❑ Entire University Community
- ❑ Presidential Cabinet
- ❑ Dean's Team
- ❑ Full-time Staff
- ❑ Part-time Staff
- ❑ Full-time Faculty
- ❑ Part-time Faculty
- ❑ Student Employees
- ❑ Students
- ❑ Contractors

II. Policy Summary

This policy establishes accountability, procedures, and standards for the selection and management of technology-related vendors. By following a set protocol, Dominican University shows commitment to protecting community members from intentional and unintentional damaging acts related to data and/or systems.

III. Policy History

This policy was approved by the President's Cabinet on July 01, 2023.

IV. Policy

Dominican University Information Technology (DU-IT) is committed to supporting community members in finding ideal solutions to meet strategic goals. When the solution involves a technology vendor partnership (i.e. – purchasing a system, utilizing institutional data sets for analysis, integrating systems, providing university datasets to external vendors, etc.), the following policy applies. Failure to adhere to this policy will result in immediate action, including but not limited to: cessation of DU-IT resources, requests to remove DU data from third-party systems, or other corrective actions to mitigate overall risk and exposure.

Vendor/Solution Selection Process

Prior to executing any contract or agreement that involves a technology vendor partnership, multiple approvals must be obtained from DU-IT depending on the nature of the system or service. Community members with a strategic need which may involve a technology vendor partnership are urged to reach out to DU-IT as early as practical for consultation. In doing so, DU-IT will be able to best assist

in applying best practices to selecting an appropriate technology vendor partner. Where practical, DU-IT recommends reviewing a minimum of three (3) possible technology vendor partners against a list of solution requirements.

Risk Assignment

Once an appropriate vendor is selected for the strategic need, but prior to executing a contract, DU-IT must assign a risk to the solution. The assignment of the inherent risk of any vendor is based on several considerations, and the primary concern is the type of data to which the vendor will have access. However, other factors including legal, regulatory, compliance, and others such as the availability and uniqueness of services provided must be also considered.

All technology vendor partnerships will be assigned an inherent risk ranking by DU-IT per the guidelines below:

- **Minimal Risk:** These vendors 1) would have no access to any type of information, and extremely little to no opportunity to access sensitive information when conducting services, 2) services are not unique or special in the marketplace, 3) have multiple competitors available that can offer replacement services with no disruption to business functions, 4) do not pose any other type of risk per the above.

  Low Risk: These vendors 1) would have no access to any type of sensitive information and little opportunity to access sensitive information when conducting services, 2) services are not unique or special in the marketplace, 3) have multiple competitors available that can offer replacement services with very little to no disruption to business functions, 4) do not pose any other type of risk per the above. If assigned a low risk ranking, the vendor must complete a Data Security Addendum (DSA) before Dominican University will engage in a contract.

- **Moderate Risk:** These vendors 1) would have access to a limited amount of sensitive information and/or some opportunity to access sensitive information when conducting services, 2) services are not unique or special in the marketplace, 3) may have some competitors available that can offer replacement services with some disruption to business functions, 4) may pose some other type of risk per the above. Examples include: bulk email marketing distribution vendor who maintains list of email addresses and names of employees or alumni or students or donors, compensation analysis vendor who would have access to anonymized or aggregated compensation data for employees of the university. If assigned a moderate risk ranking, the vendor must complete a Data Security Addendum (DSA) and a Vendor Risk Assessment (VRA) before Dominican University will engage in a contract.

- **High Risk:** These vendors 1) May be considered critical to Dominican University's mission or business operations. Security events or disruptions related to these vendors would have Enterprise wide or large departmental impacts. These vendors may be accessing, or processing data classified as restricted or internal. They may also be storing data classified as internal., 2) services may be unique or special in the marketplace, 3) may have some competitors available that can offer replacement services, however, significant planning and preparation would be required to avoid any disruption to critical operational or educational functions, 4) may pose some other type of risk per the above. Examples include:

Outsourced HR or payroll vendor, 403(b) provider, financial auditors, student medical record aggregator, etc. If assigned a high-risk ranking, the vendor must complete a Data Security Addendum (DSA) and a Vendor Risk Assessment (VRA) before Dominican University will engage in a contract.

- **Critical Risk:** These vendors are similar to High-Risk vendors with regard to their access to sensitive information but may also be storing data classified as "Restricted". They may also include another element(s) that increases the potential risk to the institution or the services provided are critical to the operations of the institution, or may pose particular harm to the reputation of the institution. Examples include: Whistle-blower reporting, etc. If assigned a critical risk ranking, the vendor must complete a Data Security Addendum (DSA) and a Vendor Risk Assessment (VRA) before Dominican University will engage in a contract

Vendor Risk Assessments (VRA) and Data Security Addendums (DSA):

Once a risk ranking is assigned to the vendor, further analysis or actions may be required such as utilizing a Vendor Risk Assessment (VRA) and/or executing a Data Security Addendum (DSA). The VRA process involves a thorough review of various documentation to gain a full understanding of the cybersecurity controls and risk involved in partnering with a vendor. This review is performed by the Chief Information Officer (or their delegate) and takes approximately thirty (30) days to complete. At the conclusion of the VRA, DU-IT will inform the vendor and community sponsor of what, if any, risks and/or controls must be addressed prior to entering into a contract. This may include, but not be limited to: amending portions of the contract, requesting risk mitigating actions, or terminating the technology vendor partnership.

If necessary, the DSA requires vendor agreement to a comprehensive list of risk controls and measures to safeguard university data. The vendor may exclude parts of the DSA that do not apply to the proposed partnership, but the document must be signed and returned prior to contract execution. DSA's are retained in DU-IT and must be renewed at the conclusion of each contract or at the request of DU-IT.

Vendor Inventory:

DU-IT will maintain an inventory of vendors, documenting the following:

1. Risk rating: Impact to operations if the service or product were suddenly not available and/or excessive liability to the DU would be incurred.

2. Community sponsor: The primary Dominican University contact with the vendor. The business sponsor manages the overall vendor relationship.

3. Business purpose: A brief description of the types of goods or services being provided by the vendor.

4. Vendor contact information: Name, address, and email address for the primary vendor contact.

5. Contract/DSA: If applicable, a contract or DSA executed by the vendor will be on file.

6. VRA score: If applicable, the VRA score will be on file.

7. Date of last review: Date when the last VRA was completed. Depending on the risk rating applied, DU-IT will determine the frequency by which a VRA will need to be performed (i.e. – annually, biannually, etc.).

Updated VRA's and/or DSA's

DU-IT retains the right to request an updated VRA and/or DSA at any time. If required, DU-IT will coordinate with the business sponsor to complete the additional requirements. Updated VRA's and/or DSA's will also be required if the vendor updates any contract/agreement terms and conditions.

V. Procedures

The following procedures apply to this policy:

1. As early as possible, community sponsors must notify DU-IT of the strategic goal(s) and possible need for a vendor technology solution by submitting a business case to supportcenter@dom.edu.

2. Once received, DU-IT will consult with the community sponsor to review the strategic goal(s), requirements, and possible vendor technology solutions. This consultation will typically occur within five to ten (5-10) business days of form submission.

3. If the strategic goals will be accomplished by a vendor, DU-IT will review all components of the solution and apply a risk assignment. Although certain factors may impact the review timeline, most risk assignments are applied within five to ten (5-10) business days. The risk assignment will then be reviewed with the community sponsor.

4. If applicable, a VRA will be conducted by DU-IT. The technology vendor solution will be scored according to the VRA rubric (rubric to be added) and findings will be communicated with the vendor and the community sponsor. This timing of this step varies widely depending on vendor cooperation, but is typically completed within thirty (30) days.

5. If applicable, DU-IT will ask the vendor to sign the University Data Security Addendum. Depending on the cooperation of the vendor, the time to completion may vary widely. However, DSA's are typically executed within thirty (30) days.

6. When all required milestones are completed, DU-IT will notify the community sponsor to proceed with executing the contract or agreement. If implementation services are required, DU-IT will also assist at this time.

VI. Division Collaborations

N/A

VII. Contact Information

Information Technology
supportcenter@dom.edu
(708) 524-6888

VIII. Appendices