



Vendor Risk Management and Data Classification		
Information Technology	Chief Information Officer	July 01, 2023



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

- | | |
|--|--|
| <ul style="list-style-type: none"> Entire University Community Presidential Cabinet 8YUbjg'HYUa Full-time Staff Part-time Staff | <ul style="list-style-type: none"> Full-time Faculty Part-time Faculty Student Employees Students Contractors |
|--|--|



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.



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



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 dataET00.000003(ere)-2()H iof vs swq(e tle tle

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.

- These vendors are similar to High-Risk vendors with regard to their access to information. These vendors may 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. The DSA 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.).

I dXUHYX'J F 5.g'UbX#cf'8G5.g

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. I dXUHYX'J F 5.g'UbX#cf'8G5.g'k]''Ugc'VY'fYei]fYX'ZH\Y'j YbXcf'i dXUHY'g'UbmVcbfUW#U[fYYa YbhYfa g'UbX'WcbX]h'cbg''





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

