Third-Party Risk Management

Category: Operations
Responsible Department: Finance
Responsible Officer: Executive Vice President
Effective Date: 6/26/2025

Policy Summary

This policy summarizes the university's program and procedures for use of third parties to provide products or services in support of business operations. Such outsourced relationships may benefit the university by reducing costs, improving performance, staff augmentation, increasing business competitiveness, access to specific expertise, and establishing distribution channels. However, the reliance on third-party relationships presents risks that must be identified, assessed, and managed. Failure to manage these risks can expose the university to financial loss, litigation, damages, and significant operational impairment.

Scope

This policy affects the following groups of the University:

- Executive Officers
- Full-Time Staff
- Part-Time Staff
- Full-Time Faculty
- Part-Time Faculty
- Budget Managers

Policy

A. Program

Relationships with third parties are fundamental to the university's ability to maintain its operations. However, the university's use of third parties does not diminish its responsibility to ensure that the activities are performed in compliance with applicable laws, regulatory guidelines, university policies and procedures. The Third-Party Risk Management policy (hereinafter referred to as the policy) is established to formally define the framework, tools, roles, responsibilities, scope, and components

needed for a fully functioning Third-Party Risk Management program ("Program"). Accordingly, this policy sets forth the requirements for the effective identification, assessment, and management of these risks.

B. Scope of the Program

This policy, along with other applicable university policies and procedures related to standards and guidance relating to the university's management of its third-party relationships and the associated inherent and residual risks presented by those third-party relationships, constitutes the Program. Such other policies include, but are not limited to:

- Access to and Responsible Use of Data
- Contract Requirements and Procedures
- DePaul University Computing Policy
- Prohibited and Special Purchasing Processes
- Purchasing & Bidding Requirements

The Program applies to all business relationships between a third party and the university, whether by contract or otherwise, where the third party has access to DePaul University data that is classified as *Highly Sensitive*, *Sensitive*, or *Internal Restricted*, as defined by the Access to and Responsible Use of Data policy. Such data includes, but is not limited to, Social Security numbers, credit card numbers, personal health information, student financial aid information, and personnel files. All university employees, independent contractors, and consultants are subject to this Policy.

The following university third-party relationships have been excluded from this Policy.

- Relationships with students
- Relationships with public utility providers
- Relationships with emergency services such as police or fire departments
- Relationships with government agencies, taxing authorities, and regulatory bodies
- Relationships with donors and benefactors

C. Elements of the Program

1. Third-Party Risk Management Oversight

The elements of this policy are managed by the university's Procurement department and the department entering into a contract (the "Contracting Department"). The university's Procurement department is the designated department responsible for overseeing, implementing, and enforcing the Program, including Risk Assessment and Due Diligence of third parties. In accordance with the referenced policies, the Contracting Department, as defined by the Contracting Requirements and Procedures policy is responsible for Planning, Contracting, and Monitoring third party relationships, as well as knowing when a contract is going to terminate and whether it should be renewed. Additional information on Contracting Department responsibilities is available in the Contract Requirements and Procedures policy.

2. Risk Management Overview

The university's Third-Party Risk Management process is comprised of the following elements:

- **Planning**
- **Risk Assessment & Due Diligence**
- **Contracting**
- **Monitoring**
- **Termination**

These elements apply to all third-party activities; however, the extent and scope required for any third party are dependent on multiple factors. The university's risk identification and management process contemplate the nature of the third-party relationship, the complexity, and magnitude of the activity provided, and the identified risks related to the third-party relationship. Risk identification, assessment, and monitoring are appropriately scaled and commensurate with the risk.

3. Planning

Before entering into a third-party relationship, the Contracting Department should ensure alignment with the university's strategic goals and objectives and identify how it might impact strategic initiatives. Budget managers, including university officers, have the fiduciary responsibility to ensure funds are properly spent, including:

• Ensuring purchases are based on genuine need, avoiding the acquisition of unnecessary or duplicate items.

• Conducting price analyses to determine market rates, where appropriate, and to conduct purchasing transactions in a manner that maximizes competition.

The proposed relationship is evaluated by weighing its overall benefits against estimated costs. This assessment also considers other relevant factors, including the arrangement's complexity, technology requirements, potential foreign third-party involvement, and possible impacts on the organization's employees.

The Program requires the use of requisition and procurement intake and review as described in the Purchasing & Bidding Requirements policy which outlines the requirements and responsibilities associated with making university purchases including competitive bidding, master agreements/contracts, purchase orders, vendor selection and vendor solicitations.

The Prohibited and Special Purchasing Processes policy outlines the types of purchases that are either not allowed or have a specific process that must be followed.

The Access to and Responsible Use of Data policy outlines procedures for data access and use (including security) to ensure that relevant data are accessible for the effective management and legitimate educational and business purposes of the university, while protecting data integrity, providing appropriate data confidentiality, and safeguarding individual privacy.

The DePaul University Computing Policy outlines general principles, guidelines and security requirements for all computing environments.

4. Risk Assessment & Due Diligence

For each prospective third-party relationship and subsequent engagement, Procurement, in collaboration with Information Services, will assess the inherent risk posed to the university based on the data classification as defined by the Access to and Responsible Use of Data policy. The inherent risk assessment assesses distinct categories of risk and the total risk of the relationship. Specific risk areas examined may include:

- **Business Continuity Risk** – The possibility of an event that could stop or disrupt operations or increase the potential for ceasing operations/becoming inactive.
- **Financial Risk** – The possibility of financial loss due to various factors including creditworthiness and financial health.
- **Cyber Risk** – The possibility of damage or loss due to cyberattacks, data breaches, or other cyber-related incidents including insecure applications, endpoints, network settings, system configurations, etc.

Risk Assessment:

To assess risk accurately, the methodologies below are utilized:

- **Information Security Risk:** DPU Information Services Third-Party Management outlines Information Services' process to assess third- party security risk assessment based on data classification and access controls. Additional information related to cybersecurity third-party onboarding can be found in the Information Services Knowledgebase article on Cloud Services Responsibilities, Requirements, and Procedures.
- **All Other Risks:** third-party risk management tool that scans public domain and other databases for risks related to legal, financial, business continuity, bankruptcies, etc.

As each third-party is risk-rated, the distinct and separate classification of risk serves to identify the most essential and highest-risk business activities provided by third parties to the university in service of its operations. Third parties deemed "High Risk" are subject to additional monitoring, risk management and reporting.

Due Diligence:

Comprehensive, risk-based due diligence processes are appropriately scaled to ensure that contracted engagements meet strategic and financial objectives, data security and privacy standards, and support operational and contractual requirements. For third parties deemed "High Risk" Procurement will conduct due diligence ensuring it is completed and formally documented before the university and third party enter a contract. Procurement will continue to conduct due diligence periodically during the relationship and will notify the Contracting Department if that due diligence calls into question the suitability of the vendor to continue business with DePaul. Before renewing contracts, reference checks are conducted by the Contracting Department or Procurement, in accordance with the Purchasing and Bidding Requirements policy**.**

5. Contracting

In accordance with the procedures outlined in the university policy entitled Contract Requirements and Procedures, third-party relationships shall be documented by written agreements that

appropriately and adequately consider the contemplated relationship and provide the university with appropriate protections and controls, consistent with prudent business practices. This policy collectively refers to all legal agreements as "contracts." The term "contract" refers to all written legal agreements facilitating the use of products or services to university, including statements of work, purchase orders, licensing, servicing, marketing agreements, and other similar written agreements. This policy details, among other things, when a written contract is required; who has the authority to sign and negotiate contracts on behalf of DePaul; when a contract must be reviewed by the Office of General Counsel (OGC); and the procedures for obtaining OGC approval.

6. Monitoring

Procurement and the Contracting Department jointly monitor the third-party's operations to verify that they are consistent with the written agreement terms.

The Contracting Department will:

- Perform ongoing performance evaluations of the third-party against contractual requirements and performance standards, including both service level agreements and quality standards, with appropriate follow-up as needed.
- Evaluate the third-party relationship's overall effectiveness and the relationship's consistency with the university's strategic goals.
- Monitor day-to-day operational aspects of the relationship.
- Report incidents, service failures, or compliance issues to relevant stakeholders.
- Monitor for compliance with university policies and applicable regulations.
- Maintain records of all monitoring activities and communications with the third-party.

Procurement will:

- Confirm that the third party is meeting its financial obligations to others.
- Monitor third-party financial stability and risk indicators.
- Ensure adherence to university-wide Procurement policies.
- Monitor for any changes in third-party ownership or organizational structure.
- Track contract expiration dates and initiate renewal discussions.
- Serve as escalation point for significant issues identified by Contracting Departments

At a minimum, Procurement will perform a periodic risk assessment within one calendar year of completing initial due diligence or previous assessment for High-Risk third parties. If results of such risk assessment call into question the suitability of the vendor to continue business with DePaul, they are escalated to Senior Management for review.

7. Termination

Prior to termination of a third-party relationship, the Contracting Department will inform Information Services (IS) and Procurement that the third-party relationship is being terminated.

The Contracting Department must develop a comprehensive transition plan to ensure:

- Continuity of critical services
- Minimal disruption to university operations

- Smooth transfer of responsibilities
- Termination of access to university data

The Contracting Department will ensure the third party's access to sensitive DePaul data is sufficiently removed, including the return or destruction of all organizational data in compliance with university data protection standards.

Additionally, the Contracting Department will perform a thorough financial reconciliation, ensuring all outstanding invoices have been processed, paid or disputed as appropriate, and that all payment obligations on both sides have been fulfilled. The Contracting Department should calculate and process any applicable prorated refunds.

Procurement will update vendor management files as necessary.

8. **System of Record & Inventory**

Procurement will ensure the system of record preserves third-party agreements for ongoing tracking and monitoring based on risk and criticality. Software tools may be used for tracking third-party risk management activity. The use of software tools to manage third-party documentation provides multiple control and notification layers to assist in and ensure the proper control over document collection, storage, and timelines.

Procedures

University-wide procedures related to the Program are specified in the various policies and procedure documents referenced throughout this policy. Additional, non-conflicting, departmental procedures regarding Third Party Risk Management may be developed by the individual university business and academic units.

Divisional Collaborations

Procurement
Information Services
Office of the General Counsel
Office of Risk Management

Contact Information

AVP, Finance
Kevin Achettu
kachettu@depaul.edu

AVP, Risk Management
Eric Hoberg
choberg@depaul.edu

Appendices

None.

History/Revisions

Origination Date: 6/26/2025
Last Amended Date: N/A
Next Review Date: