University of Portland

VENDOR MANAGEMENT POLICY

1. **PURPOSE:** Due to the specialized expertise needed to design, implement and service new technologies, vendors may be needed to provide resources that the university is unable to provide on its own. This could include consulting services, Software-as-a-Service (SaaS), new application implementations or existing application upgrades.

2. **SCOPE:** This policy applies to all vendor engagements including, but not limited to any software purchase that is accompanied by a contract or agreement.

3. **POLICY:** No software or service contract may be entered into by a university employee without prior approval/review by the Chief Information Officer (CIO), the Vice President for University Operations and Vice President and General Counsel. All new vendors with Software-as-a-Service (SaaS) must conform to the requirements in the Cloud Application and Infrastructure Policy.

4. **GUIDANCE:**

   a. **Statement of Work (SOW):**

   - Must clearly state the security requirements for the vendors to ensure that their work is consistent with the University policies.
   - Must include a clear description of the scope of services provided under the contract.
   - Must clearly identify all types of sensitive data to be exchanged and managed by the vendor.
   - Must contain a documented System Security Plan which describes all existing and planned security controls.
   - Depending on the type of work being performed Information Services (IS) may require the vendor to submit a Higher Education Cloud Vendor Assessment Tool – Lite (HECVAT-Lite). A copy of this form can be obtained from IS
   - If this is an online tool an Accessibility Conformance Report needs to be submitted to ensure ADA compliance is present.

   b. **Agreements and Contracts:**

   - Must contain a documented System Security Plan which describes all existing and planned security controls.
   - Contracts that include exchange of sensitive data must University confidentiality agreements to be executed by the vendor, must identify applicable University policies and procedures to which the vendor is subjected, and must identify security incident reporting requirements.
   - Contracts must clearly identify security reporting requirements that stipulate that the vendor is responsible for maintaining the security of sensitive data, regardless of ownership.
   - Contracts must include formal sanctions or penalties for failure to meet the security requirements in the contract or purchase document.
   - Information Services shall provide the appropriate security reporting contact information to each vendor upon contract initiation.
   - Upon termination of vendor services, contracts must require the return or destruction of all University of Portland data. Information Services is to immediately ensure termination of all access to University information systems and, if applicable, facilities housing these systems.

c. **Reporting Requirements:**

- In the event of a breach of the security of the sensitive data, the vendor is responsible for immediately notifying and working with IS regarding notification, recovery and remediation.
- Security reporting requirements in the contract must also require the vendor to report all suspected loss or compromise of sensitive data exchanged pursuant to the contract within 24 hours of the suspected loss or compromise.
- The vendor is responsible for notifying all persons whose sensitive data may have been compromised because of the breach as required by law.
- All contracts shall require the vendor to produce regular reports focusing on four primary potential risk areas:
  - Unauthorized Systems Access
  - Compromised Data
  - Loss of Data Integrity
  - Inability to Transmit or Process Data
  - Exception Reporting

Any exceptions from normal activity are to be noted in the reports, reviewed, and the appropriate responses determined.

d. **Security and Data Risk Assessment:** In general, contracts for software and other services delivered from cloud vendors are reviewed by Information Services for security and accessibility compliance. New vendors are required to fill out a Higher Education Cloud Vendor Assessment Tool – Lite (HECVAT-Lite) and a Voluntary Product Accessibility Template (VPAT) supplied by Information Services. For more details, please reference the *'Technology Purchasing Policy'*, the *'Cloud Application & Infrastructure Policy'*, and the '*Data Risk Classification Guidelines'* found on the Information Services Policies website at https://www.up.edu/is/is-policies.

5. **EXCEPTIONS:** There are no other exceptions for this policy.

6. **SANCTIONS:** Accounts and network access may be administratively suspended by the University with or without notice when, in the University's judgment, continued use of the University's resources may interfere with the work of others, place the University or others at risk, or violate University policy. Any violation of this policy by a student may lead to disciplinary charges under the appropriate student disciplinary policy, which may include expulsion or suspension of student status. Faculty and staff violations will be addressed by their respective disciplinary policies and procedures. All known and/or suspected violations will be reported to the Vice President for University Operations. Users of University of Portland computing facilities are subject not only to University Policies, but also to applicable local, state and federal laws.