UTICA
UNIVERSITY

Integrated Information Technology Services

POLICIES AND PROCEDURES

Vendor Management Policy

POLICY:

Utica University is committed to ensuring the security, confidentiality, and integrity of institutional data when engaging with vendors and third-party service providers. This Vendor Management Policy establishes guidelines for evaluating, onboarding, and monitoring vendors to mitigate risks associated with third-party relationships and ensure compliance with applicable regulations and institutional policies.

SCOPE:

This policy applies to all data created, collected, stored, or processed by Utica University. This policy applies to employees, students, retirees, alumni, volunteers, vendors, third parties, and all others who create, modify, transmit, and store Utica University data, including, but not limited to, academic partners and auxiliary staff members.

REASON FOR POLICY:

Vendors and third-party service providers play a critical role in supporting Utica University's operations. However, these relationships introduce potential risks, including unauthorized access, data breaches, and non-compliance with regulations. The purpose of this policy is to:

- Establish a standardized process for assessing and managing vendor risks.
- Ensure that vendors comply with the university's data protection and security standards.

- Protect institutional data from unauthorized modification, destruction, or disclosure.
- Support compliance with applicable laws and regulations governing data security and privacy.

DEFINITIONS:

- **Vendor:** Any third-party entity providing goods, services, or software to Utica University.
- **Institutional Data:** All data created, collected, stored, or processed by Utica University, including sensitive or confidential information.
- **Vendor Risk Assessment:** A process for evaluating the potential risks associated with engaging a vendor.
- **Data Processing Agreement (DPA):** A contractual document ensuring vendors adhere to Utica University's data security and privacy standards.

PROCEDURE:

1. **Vendor Evaluation:**
    - Before engaging with a vendor, the responsible department must perform a risk assessment, considering the type of data accessed, vendor security practices, and compliance with relevant laws and regulations.
    - Obtain and review vendor certifications, security policies, and audit reports.
2. **Contractual Safeguards:**
    - All vendor contracts must include provisions addressing data security, confidentiality, and breach notification requirements.
    - Ensure a DPA is executed for vendors handling institutional data.
3. **Onboarding:**
    - Vendors must undergo an onboarding process, including verifying their compliance with Utica University's security standards.
    - Provide vendors with relevant university policies and guidelines.
4. **Ongoing Monitoring:**
    - Periodically review vendor performance and compliance with contractual obligations.
    - Conduct security reviews and audits as necessary.
5. **Termination of Vendor Relationships:**
    - Ensure secure data transfer or deletion when a vendor relationship ends.
    - Review and update access controls to revoke vendor access.

RESPONSIBILITY:

- **Information Security Officer (ISO):** Oversees vendor risk assessments, provides guidance on security requirements, and ensures compliance with data protection standards.
- **Departments and Divisions:** Responsible for conducting initial vendor evaluations, ensuring compliance with this policy, and monitoring vendor performance.
- **Legal Affairs:** Reviews and approves vendor contracts, ensuring they include appropriate data security provisions.
- **Data Owners:** Ensure that vendor access to institutional data aligns with business needs and security standards.
- **Users:** Are responsible for protecting the confidentiality and privacy of individuals whose records they access, observing ethical restrictions that apply to the information they access, and abiding by applicable laws and policies concerning accessing, using, or disclosing information.

ENFORCEMENT:

Enforcement of Utica University policies is the responsibility of the office or offices listed in the "Resources/Questions" section of each policy. The responsible office will contact the appropriate authority regarding employees, students, vendors, or visitors who violate policies.

Utica University acknowledges that University policies may not anticipate every possible issue that may arise. The University, therefore, reserves the right to make reasonable and relevant decisions regarding the enforcement of this policy. All such decisions must be approved by an officer of the University (i.e., President, Provost and Senior Vice President for Academic Affairs, Vice President for Financial Affairs, Senior Vice President for Student Life and Enrollment Management, or Vice President for Legal Affairs and General Counsel).

RESOURCES/QUESTIONS:

For more information, contact the Utica University IITS Help Desk, which can be reached via telephone at (315) 792-3115. See also the Responsible Use of University Computing Resources policy.

Please note that other Utica University policies may apply or be related to this policy. To search for related policies, use the Keyword Search function of the online policy manual.

____

Todd Pfannestiel, President Date

Effective Date:
Promulgated:

Last Revised:
Promulgated: