07.400.01 Information Technology Vendor Risk Management Policy

Authority: Vice Chancellor for Business Affairs

History: Adopted October 18, 2022

Sources of Authority: UNC System adoption of ISO/IEC 27002
ISO/IEC 27002:2013 8.2 Classification of Information
UNC System Policies 1400 Series on Information Technology

Related Links: UNCW 01.250 Data Governance and Management Policy
UNCW Data Classification Matrix
Information Technology Vendor Risk Management Standard

Responsible Office: Information Technology Services

I. Purpose

The purpose of this policy is to define the Information Technology Vendor Risk Management Program at the University of North Carolina Wilmington (UNCW). This program is established to meet requirements for a formal information technology (IT) vendor risk management program and to ensure the protection of university data in accordance with university, state, and federal information security and compliance standards and regulations.

II. Scope

This policy shall apply to the following:

A. Information technology solutions as outlined in section III.C. of this policy, whether hosted externally by a vendor, cloud-hosted, or on-premises at the university; and
B. All university units and individuals procuring, accessing, utilizing, or managing these solutions in relation to university business.

All users of university information technology solutions and data must be familiar with and comply with this policy and related standards, guidelines, and procedures issued by the university or responsible office in support of this policy.

III. Definitions

A. Data Classification: Data classification refers to the categorization of data and the consistent application of security standards based on such categorization. University data will be classified according to the UNCW 01.250 Data Governance and Management Policy.
B. Regulated Data: Regulated data means Personally Identifiable Information (PII) and any other data that is protected or regulated by local, state, or federal laws or regulations.
C. Information Technology Solutions: Information technology solutions include but are not limited to software, systems, services, or other related solutions used to electronically store, process, transmit, or utilize university data regardless of form, location, or origin.
D. University: University refers to the University of North Carolina Wilmington, its divisions, colleges, schools, and affiliates.

E. **Vendor**: A vendor is any company, organization, or entity providing or supplying an information technology solution sought out by the university, whether free or paid.
F. **Terms and Conditions**: Terms and conditions are legally binding contractual language agreed to by both authorized university officials and vendors of information technology solutions.
G. **Competitive Procurement Process:** The competitive procurement process includes but is not limited to request for proposals, invitation for bids, requests for quotes, and other procurement processes utilized by the university.

IV. Roles

A. **Data Trustees**: Data Trustees (University Vice Chancellors or senior members of the Chancellor's Cabinet) are appointed by the Chancellor and are the highest-ranking divisional leaders with responsibility for ensuring that data are properly managed and appropriate compliance is practiced as related to university functions for their units.
B. **Data Stewards**: Data Stewards are designated by and accountable to the Data Trustees for the accuracy, privacy, and security of the institutional data under their responsibility. During the Information Technology Services (ITS) Vendor Risk Assessment Process Data Stewards will approve the use of university data with information technology solutions in accordance with section V.C. below.
C. **Chief Information Officer (CIO)**: The Associate Vice Chancellor for Information Technology Services and CIO will be consulted if discrepancies or concerns are identified through the ITS Vendor Risk Assessment Process. When necessary, the CIO will confer with the respective Data Trustee(s) concerning the recommendation offered by ITS through the risk assessment process.
D. **Information Technology Services**: The ITS Department will be responsible for leading the IT Vendor Risk Management Program and ITS Vendor Risk Assessment Process for information technology solutions.
E. **Purchasing Services**: University Purchasing Services will ensure that university and state public procurement requirements are satisfied throughout the acquisition process for information technology solutions.
F. **Office of the General Counsel**: The Office of the General Counsel, on an as-needed-basis, will advise on matters pertaining to legal requirements associated with contracts, revisions, and the incorporation of the UNCW ITS terms and conditions into any formal agreement.
G. **Data Governance Committee:** The Data Governance Committee will aid in communicating this policy within each committee member's unit to ensure awareness and compliance are properly emphasized.
H. **IT Risk Assessment Partner (RAP):** Risk Assessment Partners may be identified and appointed from university units to liaise between ITS, vendors, and their respective unit(s) or sub-unit(s) thereof. They will be relied upon to communicate status updates to their assigned unit(s) and, when necessary, interface with vendors regarding ITS risk assessment requirements.

V. Policy

A. All information technology solutions within the scope of this policy shall be reviewed and assessed by UNCW ITS prior to purchase or installation on university owned devices. Information technology solutions acquired prior to the formalization of the ITS Vendor Risk Assessment Process that are within the scope of this policy shall be reviewed and assessed prior to any subsequent renewals, updates, license transfers, system integrations, or re-installations on university owned devices.

B. University units seeking to purchase any information technology solution(s) through the competitive procurement process shall engage with ITS as outlined in the IT Vendor Risk Management Standard.

C. ITS staff reviewing information technology solutions for acquisition, whether paid or free, will determine if a formal ITS Vendor Risk Assessment will be required. An assessment *may* be required for the use of certain regulated university data or for resources integrating with university systems, at the discretion of the respective Data Steward(s) or ITS. An ITS risk assessment *will* be completed for information technology solutions storing, processing, transmitting, or otherwise utilizing any university data elements classified as highly sensitive or ultra-sensitive in accordance with the UNCW 01.250 Data Governance and Management Policy, unless an exception is granted in accordance with section V.F. of this policy.

D. RAPs may serve as the main point of contact between ITS and university units, once appointed, throughout the ITS Risk Assessment Process. These partners may initiate the request for documentation, information, and/or artifacts from vendors for ITS to include in the assessment process. Additional information regarding the appointment, training, and responsibilities of RAPs may be found in the IT Vendor Risk Management Standard.

E. Vendors of information technology solutions will be required to undergo periodic ITS risk assessments throughout the duration of any agreement, contract, or service engagement with the university.

F. Exceptions to the ITS Vendor Risk Assessment Process may be granted as contingency-based approvals for the renewal of information technology solutions only, and only in circumstances where an ITS risk assessment cannot be completed prior to renewal. These approvals will be offered after the CIO has consulted with and received authorization from the respective Data Steward(s) and Data Trustee(s). New acquisitions will be reviewed in accordance with section V.C. of this policy.

G. In the event a vendor does not meet established assessment criteria during the acquisition of a new information technology solution, the CIO will issue a recommendation memorandum outlining the ITS risk assessment, including:

i. Risk associated with any information security, compliance, or regulatory concerns;
ii. Commercially available alternative information technology solution(s); and
iii. Possible financial responsibility associated with any future information security incident(s) and/or other regulatory non-compliance(s).

This memorandum shall be addressed to the respective Data Trustee(s) with a copy provided to the requesting university unit. Only appointed Data Trustees may assume presented risk and financial responsibility. Financial responsibility may be delegated to the requesting university unit.

H. After authorization from the respective Data Steward(s) and/or Data Trustee(s) for the renewal or new acquisition of an information technology solution in accordance with sections V.F. and V.G. of this policy, the CIO will notify the Enterprise Risk Management Steering Committee of the authorized exception and provide a copy of the applicable recommendation memorandum and any other applicable documentation.

VI. Enforcement and Addressing Concerns

A. All users of university information technology solutions and data must be familiar with and comply with this policy and related standards, guidelines, and procedures issued by the university or responsible office in support of this policy. Failure to comply with the requirements of this policy and related documents may result in harm to individuals, organizations, or the university. Use of non-approved information technology solutions introduces great risk and security threats to the university and its information resources.

B. Failure to comply with the requirements of this policy may result in university discipline, revocation of administrative privileges to university-owned devices, termination of volunteer service, or a determination that the user has materially breached an agreement.

C. Questions about this policy, the university's IT Vendor Risk Management Program, the ITS Vendor Risk Assessment Process, or any related standards, guidelines, and procedures issued by the university or responsible office in support of this policy should be addressed to: Information Technology Services, Chief Information Officer.