TECHNOLOGY VENDOR SECURITY AND COMPLIANCE MANAGEMENT

POLICY NUMBER: ADM-TECHVENDORSECURITY
RESPONSIBLE OFFICIAL TITLE: VICE PRESIDENT ADMIN. & FINANCE
RESPONSIBLE OFFICE: INFORMATION & TECHNOLOGY (IT)/CHIEF INFORMATION OFFICER
EFFECTIVE DATE: 10/14/2024
NEXT REVIEW DATE: PRESIDENTIAL APPROVAL PLUS FOUR (4) YEARS – 10/14/2028
SUPERSEDES POLICY DATED: N/A – NEW POLICY
BOARD OF REGENTS REPORTING: PRESIDENTIAL REPORT

I. POLICY STATEMENT

PREAMBLE

This policy outlines the requirements that external service providers of technology products and services must follow in order to maintain appropriate information security and data privacy controls for Northern Kentucky University (NKU) engagements.

Third Party Technology Vendors (also referred to as third party tech vendors, technology vendors, IT vendors, or IT suppliers) of information technology (IT) products, on-premises services ("on-prem"), and off-premises services ("cloud") are a vital part of NKU's technical operations. As such, Third Party Technology Vendors must provide security and privacy controls for any products or services provided to NKU that meet or exceed the level of controls that internal NKU IT uses to protect the information security and privacy of students, faculty, staff, and alumni.

BUSINESS ENGAGEMENT REQUIREMENTS

Third Party Technology Vendors must abide by NKU and Commonwealth of Kentucky procurement procedures, including contractual, relationship, and termination requirements. All contractual engagements are subject to review and management by the NKU Procurement/Finance, Information Technology, Legal, and Records Retention teams. All formal contract change requests must be made in writing to the NKU Procurement team. All contractual or legal documentation is subject to review and approval by NKU Legal. All contractual or legal documentation regarding an engagement must seek approval and meet the requirements set forth by the Commonwealth of Kentucky Legislative Research Committee (LRC) in order to establish any formal working relationship between NKU and a third party.

Any and all contracts for technology services with Northern Kentucky University (NKU) are subject to compliance with Kentucky Revised Statutes and the ***NKU Security and Privacy Terms and Conditions Agreement***, described below under "VI. Procedures".

CONTRACTUAL DOCUMENTATION REQUIREMENTS FOR UNIVERSITY BUSINESS RELATIONSHIPS

External suppliers of IT products or services must include all operational, security, privacy, and legal requirements and practices in written form, usually in the form of a contract. This written documentation may also be known as terms of services, master services agreement, or master terms and conditions. A Statement of Work (SOW) or an acceptable equivalent is required as part of the contractual

documentation. SOWs should clearly define the work being performed, timeframes for expected completion, and expected outcomes. Changes to SOWs or requirements must be made in writing, typically as a change order. All documents are subject to review and approval before commencement or execution of work. Appropriate signatures are required for all SOW changes.

If two or more external suppliers of IT products or services will be partnering in a business agreement to provide products or service to NKU, the contractual or agreement documentation must clearly define each supplier's role in the relationship. One party in the joint relationship must be named as the primary contract owner of the multi-supplier relationship, and all contractual documentation should accurately reflect such ownership.

All suppliers of IT products or services are required to provide documentation that appropriate security controls are in place to protect the supply chain that services NKU. In all cases, the Third Party Technology Vendor of products or services must conform to NKU and Commonwealth of Kentucky procurement process and approval requirements.

Technology Vendor contracts or supplementary contractual documentation must include service level agreement (SLA) information for the delivery of services provided.

OPERATIONS MANAGEMENT AND REPORTING REQUIREMENTS

Third Party Technology Vendors should provide relevant operational and managerial reports to NKU throughout the term of the engagement. These reports should include reasonable details for line-item financial accounting.

END-OF-CONTRACT OR RELATIONSHIP CLOSURE REQUIREMENTS

During the expected or unexpected end of a contract or formal engagement between NKU and a Third Party Technology Vendor, the following must occur:

- Formal, written response of the closure of the contractual agreement must be provided by the requesting party.
- Automatic renewal of contract (without express written approval from NKU) is prohibited, per Kentucky Revised Statutes.
- Return or verified proof of destruction for all NKU data and/or system data stored or processed with the Third Party Technology Vendor must be provided. This includes any backups of NKU data or system data. At the end of the engagement, the Third Party Technology Vendor shall not retain any copies of any NKU data or system data, unless formally approved by NKU Legal the end of the engagement.

II. ENTITIES AFFECTED

This policy applies to all Third Party Technology Vendors (individuals or organizations) that supply products or services and provide paid or unpaid technology products or services to NKU to directly or indirectly access, process, manage, or control NKU data, information, or other NKU technology resources.

III. AUTHORITY

U.S. Department of Education Family Educational Rights and Privacy Act (FERPA) guidelines

U.S. Department of Health and Human Services Health Insurance Portability and Accountability Act (HIPAA) regulations

U.S. Copyright Law

European Union General Data Protection Regulation (GDPR) laws

IV. DEFINITIONS

Appropriate Security and Privacy Controls are subject to the data, product, or service being serviced. The general requirements are detailed in the ***NKU Security and Privacy Terms and Conditions Agreement*** (see "VI. Procedures" below); however, NKU Information Security may adjust these requirements based on need or other factors.

Off-Premises Services ("Cloud") provided to NKU users or systems are those that reside remotely from an NKU campus or NKU-owned facility. Such services are usually hosted and operated by a non-NKU entity and provide NKU users and systems access to services used to support the University's academic or business functions.

On-Premises products or services reside and operate onsite at an NKU campus or an NKU-owned facility.

NKU Data are electronic or written records created by NKU users or records created on behalf of NKU users.

NKU System Data are data produced by NKU or on behalf of NKU related to security and operational data of electronic or computer systems for the purpose of system functionality, utility, or management. These types of records are generally not created directly by a user, but are generated by the system in a form of a log, token, API call or other similar data types.

University Business includes all business, operational, and academic related work, transactions, or support conducted on behalf of NKU, its constituents, and those parties that represent NKU.

V. RESPONSIBILITIES

NKU faculty, staff, or anyone in an official capacity representing NKU in an engagement for Third Party Technology Vendor products or services must engage NKU IT for technical interfaces, support, security requirements, and implementation when evaluating Third Party Technology Vendor products or services,.

NKU IT is responsible for evaluating technical requirements, system interfaces, and determining suitability for operations and support within the NKU technical architecture.

NKU Information Security is responsible for evaluating service provide or vendor product security profile, requirements, alignment to the ***NKU Security and Privacy Terms and Conditions Agreement*** and determining suitability for operations and support within the NKU technical architecture.

All Third Party Technology Vendors are responsible for providing accurate, timely, and truthful information and data regarding their products, products, and services. They are also responsible for addressing operational, security, and compliance requirements determined by NKU IT and NKU Information Security on an ongoing basis during the active tenure of their engagement with NKU. They

are responsible for timely notification of service changes, outages, and security or privacy issues or breaches. In the case of security or privacy issues or breaches that affect NKU user data or system data, the vendor must be familiarized and notify NKU in accordance with local, state, and federal laws that dictate timely notification.

VI. PROCEDURES

NKU departments who engage in relationships with Third Party Technology Vendors or the NKU Procurement/Contracts Department must consult with NKU IT/Information Security so that an assessment of the vendor's information security and data privacy practices for compliance.

Third Party Technology Vendors must provide continuous adherence to the ***NKU Security and Privacy Terms and Conditions Agreement*** throughout the term of the agreement or contract.

- If a Third Party Technology Vendor determines parts of the Security and Privacy Terms and Conditions to be unnecessary due to the nature of the service or the data being stored/transmitted/processed, language approved by NKU and the Third Party Technology Vendor must be included in the agreement or contract.
- Third Party Technology Vendors may be asked at any time, for any reason, to provide proof of selective or comprehensive adherence to the ***NKU Security and Privacy Terms and Conditions Agreement*.**
    - Proof must be provided in writing to NKU within 72 hours in working days.
    - The ***NKU Security and Privacy Terms and Conditions Agreement*** is maintained in the Information Security department within the Office of Information Technology.
    - The ***NKU Security and Privacy Terms and Conditions Agreement*** is subject to change, based on NKU's needs, legal, or regulatory requirements. NKU Information Security will work with Third Party Technology Vendors when such changes arise to address compliance. Third Party Technology Vendors should actively work with NKU Information Security for the current ***NKU Security and Privacy Terms and Conditions Agreement*** and compliance requirements.

VII. REFERENCES AND RELATED PRODUCTS

REFERENCES & FORMS

NKU Security and Privacy Terms and Conditions Agreement

RELATED POLICIES

Vulnerability and Patch Management

Information Security

REVISION TYPE	MONTH/YEAR APPROVED
New Policy	October 14, 2024

TECHNOLOGY VENDOR SECURITY AND COMPLIANCE MANAGEMENT

PRESIDENTIAL APPROVAL

PRESIDENT

Signature Cady Short-Thompson *Date* 10/14/24

Cady Short-Thompson

BOARD OF REGENTS APPROVAL

BOARD OF REGENTS (IF FORWARDED BY PRESIDENT)

☐ This policy was forwarded to the Board of Regents on the ***Presidential Report (information only)***.
Date of Board of Regents meeting at which this policy was reported: _____/_____/_____.

☐ This policy was forwarded to the Board of Regents as a ***Presidential Recommendation (consent agenda/voting item)***.

- ☐ The Board of Regents approved this policy on _____/_____/_____.
  (Attach a copy of Board of Regents meeting minutes showing approval of policy.)
- ☐ The Board of Regents rejected this policy on _____/_____/_____.
  (Attach a copy of Board of Regents meeting minutes showing rejection of policy.)

SECRETARY TO THE BOARD OF REGENTS

Signature *Date*

Tammy Knochelmann