DATA GOVERNANCE & SECURITY

POLICY NUMBER: ADM-DATAGOVERNANCE
POLICY TYPE: ADMINISTRATIVE
RESPONSIBLE OFFICIAL TITLE: VICE PRESIDENT – ADMINISTRATION & FINANCE
RESPONSIBLE OFFICE: INFO. TECHOLOGY (IT) / CHIEF INFORMATION OFFICER (CFO)
EFFECTIVE DATE: UPON BOARD APPROVAL – 7/2/2016
NEXT REVIEW DATE: PREVIOUS REVIEW PLUS FOUR (4) YEARS – 7/25/2027
BOARD OF REGENTS REPORTING (CHECK ONE):
☒ PRESIDENTIAL RECOMMENDATION (CONSENT AGENDA/VOTING ITEM)
☐ PRESIDENTIAL REPORT (INFORMATION ONLY)

I. POLICY STATEMENT

Northern Kentucky University's (NKU) institutional data is a valuable asset and resource and must be maintained and protected as such. Although individuals, offices, departments, programs, or colleges may have responsibilities for creating and maintaining portions of university information and records, NKU itself retains ownership of, and responsibility for, the information.

The purpose of this policy is to protect NKU's information resources from accidental or intentional unauthorized access, modification, or damage, while also preserving the open information sharing requirements of its academic culture.

Permission to access institutional data should be granted to all University employees for all legitimate University purposes.

II. ENTITIES AFFECTED

This policy applies to all Northern Kentucky University community members who have access to University institutional data as well as all University colleges, units, divisions and their agents and contractors. It also applies, to the extent possible, to any person or organization, whether affiliated with the University or not, in possession of University institutional data.

III. SCOPE AND APPLICABILITY

This policy applies regardless of the environment, media or device where the data resides or is used and regardless of how the data is transmitted or stored.

IV. DEFINITIONS

Data Classification: Classification of data provides a basis for understanding and managing institutional data based on the level of criticality and required confidentiality of data; for NKU's data classifications, see the data classification table.

Data Communities: Data communities are stewards/data custodians who are responsible for ownership of common data elements used across the University. Data community members work together to provide a formal communication to NKU data producers/consumers when common data elements require a change.

Data Custodians: Data custodians are individuals appointed by and accountable to the data stewards. Data custodians are responsible for the operation and management of systems and servers that collect, manage, store, and/or provide access to institutional data.

Data Producers/Consumers: Data producers/consumers include all NKU employees who produce and/or have access to institutional data in order to perform assigned duties or in fulfillment of assigned roles or functions within the University; this access is granted solely for the conduct of University business. Data producers/consumers are responsible for knowing and following University policies and procedures on data governance.

Data Stewards: Data stewards are institutional officers who are appointed by the President or Provost and have authority over policies and procedures for one or more types of institutional data and the access and usage of that data within their delegations of authority. Each data steward appoints data custodians for their specific functional area of responsibility.

Data Quality: Data quality refers to the management, process, and measurement of information's fitness to serve its purpose in a given context. Aspects of data quality encompass the following characteristics:

- Accuracy
- Completeness
- Consistency across the University
- Relevancy
- Unduplicated
- Traceability
- Interpretability
- Timeliness
- Accessibility

Institutional Data: Institutional data include data elements that are created, received, maintained, and/or transmitted by NKU administrative information systems. Information is a collection of institutional data representing quantitative/qualitative measurements and facts related to the business of the University. Click the following link for types of NKU institutional data: https://inside.nku.edu/datagovernance/data.html

V. RESPONSIBILITIES

All University community members who work with or use institutional data in any way must comply with all federal, state and other applicable laws; University policies, procedures and guidelines; and applicable contracts and licenses. Examples include, but are not limited to:

- Family Education Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Kentucky Open Records laws
- Kentucky Revised Statutes

- Kentucky Statutes regarding personal information security and breach investigations (KRS 61.931 to 61.934)
- Payment Card Industry Data Security Standards (PCI-DSS)
- European Union General Data Protection Regulation (GDPR)
- Other NKU information and security policies

NKU employees and their supervisors are responsible for understanding and complying with all laws, rules, policies, standards, guidelines, contracts, and licenses that are applicable to their own and their subordinates' specific uses of institutional data.

Employees are expected to do the following:

- Access confidential data only for the purpose of conducting university business
- Access only the confidential data required to perform their job
- Respect and protect the confidentiality and privacy of the individuals whose confidential records they have access to
- Abide by all applicable laws or policies with respect to access, use, or disclosure of confidential information
- Ensure adequate security measures are in place so that confidential data is protected to the extent required by law or policy when sensitive data is transferred from a well-secured system, such as SAP, to a user's destination computer
- Ensure controls for labeling and handling (storage, transmission, distribution, and disposal) of data are followed; examples of controls include encryption, secure disposal (shredding or wiping), and document labeling

Employees should not do the following:

- Disclose confidential data to others except as required by their job responsibilities
- Use confidential data for their own or others' personal gain or profit
- Access confidential data to satisfy personal curiosity
- Forge, falsify, or alter (without authorization) documents, records, or university data in any form (including financial documents)

University community members who are acting in one or more specific roles when collecting, maintaining, accessing, or using institutional data must understand and fulfill the responsibilities associated with their roles. These roles are as follows (see definitions in Section IV):

- Data Custodians
- Data Producer/Consumers
- Data Stewards

For specific instructions on how to access institutional data via NKU administrative information systems, please contact the designated Data Custodian of that system.

VI. EUROPEAN UNION (EU) GENERAL DATA PROTECTION REGULATION (GDPR)

NKU is an institution of higher education involved in education, research, and community engagement. NKU has a lawful basis to collect, process, use, and maintain data about current and prospective students, current and prospective employees, research subjects, and others involved in its education, research, and community engagement. Examples of data that NKU may need to collect may include, but are not limited to, names, email addresses, IP addresses, mailing or physical addresses or other location identifiers, photos, and other personal data obtained with prior consent.

NKU takes seriously its duty to protect the personal data that it collects or processes. In addition to complying with NKU's overall data protection program and policies, NKU will comply with European Union (EU) General Data Protection Regulation (GDPR) legislation. Requirements contained in GDPR include, but are not limited to, the following:

- Transparency regarding personal data collected, processed and used by NKU
- Monitoring all use and disclosure of personal data
- Proper security of all personal data

NKU will protect personal and sensitive data that it collects. All personal and sensitive data that NKU collects or processes will be:

- Processed lawfully, fairly, and transparently;
- Collected for specific and legitimate purposes;
- Limited to what is necessary for those legitimate purposes;
- Accurate and kept up to date;
- Retained as long as necessary; and
- Secure.

Individual data subjects covered by the GDPR will have the following rights (as applicable), provided that NKU determines that the right(s) are permitted and/or required by the GDPR:

- The right to receive confirmation from NKU regarding whether the individual's personal data is being processed by NKU. If personal data is being processed by NKU, the individual has the right to access their personal data, as well as receive information regarding the categories of personal data collected and how such data is being used;
- The right to correct inaccurate personal data;
- The right to obtain erasure of personal data (to the extent allowed by applicable law);
- The right to restrict or object to the processing of personal data; and
- The right to request a copy of their personal data.

All data at NKU will be collected, processed, used, and maintained in compliance with applicable federal and state laws, including FERPA, University records and information management guidelines and policy, and Kentucky law.

Any individual who wishes to exercise their rights under the EU GDPR should visit http://dataquality.nku.edu/. Additional information may be requested in order to facilitate the request. All requests will be reviewed and processed in accordance with applicable federal and state laws.

VII. COMMITTEE

The Data Governance Committee was formed to recommend and oversee the implementation and management of a formal data governance program that functions across the University. A list of the members of the committee can be found on NKU's Data Governance website.

Data classifications are created and maintained by the Data Governance Committee.

VIII. VIOLATIONS

Any member of the University community found to have violated this policy is subject to discipline in accordance with applicable University policies and procedures, or, in the case of student violations processed under the Code of Students Rights and Responsibilities, expulsion.

IX. DATA QUALITY REPORTING REQUIREMENTS

You may submit an NKU data quality issue by signing in using your NKU user ID and password.

A flowchart depicting the data quality issue resolution process is available.

X. GDPR DATA BREACH OR DISCLOSURE REPORTING REQUIREMENTS

Any NKU unit, department, or college that is aware of or suspects that a data breach or disclosure of personal data has occurred must immediately refer to the Information Security Incident Response policy.

XI. REFERENCES AND RELATED MATERIALS

REFERENCES & FORMS

Data Governance website

Data Dictionary and Report Repository

European Union GDPR

RELATED POLICIES

Credit Card Processing and Security

Information Security

Information Security Incident Response:

Records Management

REVISION HISTORY

REVISION TYPE	MONTH/YEAR APPROVED
Review & Minor Editing/Formatting	July 25, 2023
Revision	May 8, 2019
Revision	January 10, 2018
Policy	July 2, 2016

DATA GOVERNANCE & SECURITY

PRESIDENTIAL APPROVAL

PRESIDENT

Signature A.Vaidya Date 4/12/19

Ashish K. Vaidya

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 5 / 8 / 19. (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.)

EXECUTIVE ASSISTANT TO THE PRESIDENT/SECRETARY TO THE BOARD OF REGENTS

Signature Wendy Peek Date 5/10/19

Print Name Wendy Peek