

DATA GOVERNANCE & SECURITY

POLICY NUMBER: ADM-DATAGOVERNANCE

POLICY TYPE: ADMINISTRATIVE

RESPONSIBLE OFFICIAL TITLE: CHIEF INFORMATION OFFICER

RESPONSIBLE OFFICE: OFFICE OF INFORMATION TECHNOLOGY

EFFECTIVE DATE: UPON BOARD APPROVAL – 1/10/2018

NEXT REVIEW DATE: BOARD APPROVAL PLUS FOUR YEARS – 1/10/2022

SUPERSEDES POLICY DATED: 7/2/2016

REQUIRES LEGAL/COMPLIANCE REVIEW:

(PER SECTION V. OF THE APPROVED POLICY REQUEST FORM) YES NO

REQUIRES I.T. POLICY COUNCIL REVIEW:

(PER SECTION V. OF THE APPROVED POLICY REQUEST FORM) YES NO

REQUIRES PROFESSIONAL CONCERNS COMMITTEE REVIEW:

(PER SECTION V. OF THE APPROVED POLICY REQUEST FORM) YES NO

REQUIRES FACULTY SENATE APPROVAL:

(PER SECTION V. OF THE APPROVED POLICY REQUEST FORM) YES NO

REQUIRES HUMAN RESOURCES REVIEW:

(PER SECTION V. OF THE APPROVED POLICY REQUEST FORM) YES NO

REQUIRES BOARD OF REGENTS APPROVAL:

(PER SECTION V. OF THE APPROVED POLICY REQUEST FORM) YES NO

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

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 to provide 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: <https://inside.nku.edu/content/dam/datagovernance/docs/Data%20Classification.pdf> .

Data Communities – Data 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 – 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 – 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 – 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 – The management, process, and measurement of information's fitness to serve its purpose in a given context. Aspects of data quality encompass:

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

Institutional Data - Data elements which 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 Standards ([PCI-DSS](#))
- 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

- 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
- To abide by all applicable laws or policies with respect to access, use, or disclosure of confidential information

Employees should not:

- 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 (see definitions in Section IV):

- Data Steward
- Data Custodian
- Data Producer/Consumer

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

VI. 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:

<https://inside.nku.edu/datagovernance/roles.html>.

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

VII. 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.

VIII. DATA QUALITY REPORTING REQUIREMENTS

To submit an NKU data quality issue, please follow this link: <https://dataquality.nku.edu/> . You will need to sign in using your NKU user ID and password.

To see a flowchart depicting the data quality issue resolution process, please click the following link:

<https://inside.nku.edu/content/dam/datagovernance/docs/DQ%20Issue%20Resolution.pdf>

IX. REFERENCES AND RELATED MATERIALS

Data Governance website: <https://inside.nku.edu/datagovernance.html>

Data Dictionary and Report Repository: <https://inside.nku.edu/datagovernance.html>

RELATED POLICIES

[Credit Card Processing](#)

[Information Security Policy](#)

[Records Management Policy](#)

REVISION HISTORY

REVISION TYPE	MONTH/YEAR APPROVED
Revision	January 10, 2018 (NKU Board of Regents meeting)
Policy	July 2, 2016
Choose an item.	

January 17, 2018

*May/Handel
Please
file*

Dr. Sue Hodges Moore
Senior Vice President for Administration & Finance
812 Lucas Administrative Center

Dear Dr. Hodges Moore:

The Northern Kentucky University Board of Regents, at its regularly scheduled meeting on January 10, 2018, approved the following policies.

Disclosure of Campus Security and Crime Statistics
Facilities and Administrative Expenses for Grants and Contracts
Graduate Course Reinstatement
Grade Appeals
Information Security Incident Response
Data Governance and Security

Sincerely,

Gerard St. Amand

Gerard St. Amand
Interim President