INFORMATION SECURITY

POLICY NUMBER: IT-INFOSECURITY
POLICY TYPE: ADMINISTRATIVE
RESPONSIBLE OFFICIAL TITLE: CHIEF INFORMATION OFFICER
RESPONSIBLE OFFICE: OFFICE OF INFORMATION TECHNOLOGY
EFFECTIVE DATE: UPON PRESIDENTIAL APPROVAL – 5/16/2018
NEXT REVIEW DATE: PREVIOUS REVIEW PLUS FOUR (4) YEARS – 5/11/2026
SUPERSEDES POLICIES: INFORMATION SECURITY – 7/2/2016; SECURITY; SOCIAL SECURITY NUMBER USAGE – 3/22/2006
BOARD OF REGENTS REPORTING (CHECK ONE):
☐ PRESIDENTIAL RECOMMENDATION (CONSENT AGENDA/VOTING ITEM):
☒ PRESIDENTIAL REPORT (INFORMATION ONLY)

I. POLICY STATEMENT

Northern Kentucky University (NKU) recognizes the obligation to protect confidentiality, maintain the integrity, and ensure appropriate availability of information regarding students, faculty, staff, alumni, and customers, and to provide proper administrative, technical, and physical safeguards to protect university information assets per NKU's data classification categories (see below).

This policy covers:

- information and data that are acquired, transmitted, processed, managed, transferred, stored, and/or maintained by NKU organizations;
- security of passwords, decryption, and encryption processes
- all data systems and equipment including departmental, divisional and other ancillary systems, as well as information residing on these systems and equipment;
- work/home/personal electronic and mobile devices of NKU faculty, staff, alumni, and administrators who access information technology information and data.

Each member of the NKU campus community should make a best effort towards the security and protection of NKU information and data resources and must adhere to the Acceptable Use policy. Resources to be protected include data stored on any laptops, desktops, mobile devices (e.g., iPads, tablets, cell phones), any data accessed, transferred, or stored, regardless of format (e.g., text, graphic, audio), passwords, decryption/encryption processes. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, inappropriate or unsafe transmission or storage of confidential data, inappropriate release of confidential or private information (whether accidental or intentional), or inadvertent compromise, such as theft or loss.

It is the policy of NKU to:

- safeguard personal and confidential information of NKU students, faculty, staff, alumni, and customers, regardless of format or medium;
- protect against anticipated threats or hazards to the physical security or integrity of NKU information and data assets, including data files and hardware equipment;

- ensure campus compliance with federal and state laws, regulations, NKU policies, procedures, and standards regarding information security, privacy and prevention of threats, breaches, and intrusions;
- ensure employees, departments, and organizations operate in compliance with state and federal laws for access, usage, and transmission of electronic data (e.g., FERPA, HIPAA). Compliance with state law includes following the State University Model Records Retention Schedule and NKU Records Management Policy for the retention and disposal of electronic records
- ensure departments and organizations are held responsible for implementing appropriate managerial, operational, physical, and technical controls for access, usage, transmission, storage, and disposal of NKU data in compliance with this policy.

II. ENTITIES AFFECTED

This policy applies to all individuals who access, use, or control NKU information or data resources. Those individuals covered include, but are not limited to faculty, staff, students, contractors, alumni, and individuals authorized by affiliated institutions or organizations.

III. DEFINITIONS

Classification Definitions and Examples – The table on the next page clarifies the nature of each data category and provides criteria for determining which classification is appropriate for a particular set of data.

NKU Data Classification Categories

	Confidential Data (highest, most sensitive)	Private Data (moderate level of sensitivity)	Public Data (low level of sensitivity)
Legal Requirements	Protection of data is required by law (i.e. HIPAA, FERPA, GLBA, etc.)	NKU has a contractual obligation to protect the data	Governed by the Kentucky Open Records Act, K.R.S. §§ 61.870 to 61.884
Reputation Risk	High	Medium	Low
Other Institutional Risks	Information which provides access to resources, physical or virtual	Smaller subsets of protected data from a school or department	General university information
Access	Only those individuals designated with approved access, signed non- disclosure agreements, and a need-to-know	NKU employees and non-employees who have a business need-to-know	Unrestricted
Examples	• Student education records • Individuals' health records and information • Human subjects research data that identifies individuals • Prospective students • Personally Identifiable Financial Information • Campus Security Systems and Details • Credit card numbers • Certain management information • Social Security Numbers • Government restricted and/or classified Information • Financial transactions of students and employees • Personnel Records (Although certain records contained within employee personnel files may be "public records" subject to disclosure, personnel files should be maintained as confidential data and disclosure of "public records" shall only be made after a case-by-case determination.)	• Information resources with access to confidential data • Research data or results that are not confidential data • Information covered by non-disclosure agreements • Materials for performance of official duties • Proprietary information of NKU or others contained within proposals, contracts, or license agreements	• Campus maps • Directory information (e.g., contact information; Find It) • Departmental websites • Academic course descriptions • News • Information posted on University website • Budgets • Purchase Orders • All institutional data made available to the general public by the Kentucky Open Records Act

IV. RESPONSIBILITIES

All employees working with NKU data are responsible for properly protecting that data. The following protective measures should be used as a foundation for due diligence in keeping data secure:

- Understand NKU's data classification categories (see the table on the previous page):
- The NKU data classification categories will be used as reference in defining Confidential, Private, and Public data
- Confidential and Private data are to be protected from disclosure, breaches, unauthorized alteration, and data loss.
- For a more comprehensive list of examples and legal requirements, see NKU's Data Governance and Security policy.
- Follow FERPA guidelines: The Family Educational Rights and Privacy Act (FERPA) guidelines are maintained and must be adhered to for student rights and controlled disclosures of their records. For more information, see the information about FERPA on NKU's Registrar website.
- Use encryption for laptops (when available for the device): All NKU owned laptops will be encrypted if the device supports encryption. NKU IT personnel will assist in providing encryption services. NKU employees are not permitted to remove encryption from laptops, and exceptions will only be permitted with VP and CIO approval.
- Notify IT to update security access for employees when department transfer occurs; disable previous security roles in SAP and departmental drives.
- Store data within NKU networks: Data that is classified as Confidential or Private should be stored within the NKU file server network ("J" / "K" drives) or the Microsoft OneDrive service, or encrypted storage devices. Storing such data on unencrypted hard drives (e.g., laptops, desktops, tablets, or unencrypted mobile storage devices) can subject the data to breach by viruses, malware, hacking, physical loss of device, etc. IT can assist if a user requires storage quotas that exceeds currently allocated amounts.
- Use Virtual Private Network (VPN) to access data when not on campus (e.g., home, travel). NKU's VPN technology provides security when used from remote locations. See VPN information.
- Only access Confidential and/or Private data through encrypted or secure networks when on campus.
- Use a secured login when leaving your device unattended in an unsecured space. When leaving your computer unattended, lock your screen and require login to re-access.
- Dispose of non-permanent Confidential and Private data as soon as possible according to the State University Model Records Retention Schedule to reduce risk and potential liability.
- Report any breaches, inappropriate disclosures, abuses, data loss, or unauthorized alterations to abuse@nku.edu
- If a personally owned device is lost or stolen and has been used to access Confidential or Private information, it is the individual's responsibility to report this to abuse@nku.edu.
- Do not store Confidential or Private data within cloud-based and third party data services: The use of individual cloud-based storage services such as Google Docs, Dropbox, Amazon, iCloud,

or other external storage for NKU Confidential or Private data is prohibited. (Microsoft OneDrive, provided through NKU, is the only cloud-based storage service approved for storage of NKU Confidential or Private data.) Third-party contracts that require data collection, distribution, or interfaces with NKU systems will require Legal, IT, and Procurement approval.

- Do not store Confidential or Private data on unencrypted portable or mobile storage devices: "Flash" or "thumb" drives are prohibited when storing NKU Confidential or Private data, unless the device and/or data has been properly encrypted. For assistance with encryption of mobile and portable devices, please call the IT Help Desk.
- Do not share passwords: Sharing or using weak passwords may put NKU data at risk. Even in the safest environment, a password disclosure by unauthorized personnel or hackers could result in a data breach. Use strong passwords, and do not share with friends, co-workers, or family.
- When sending email messages, do not send Confidential or Private data through unencrypted email. Even internal email messages are vulnerable to possible attack.
- Do not mix NKU Confidential or Private data with individual personal records.

V. VIOLATIONS

Any university employee, student, or non-university individual who stores university data outside NKU networks and secure servers without proper permissions and protection measures is in violation of this policy and will be subject to appropriate disciplinary action, including possible dismissal and/or legal action.

Depending upon the nature and seriousness of the infraction, any faculty, staff, student, contractor, alumni, or other user within the university network found to have violated this policy may be:

- removed from the network
- subject to disciplinary action, up to and including termination of employment or expulsion
- held personally responsible for any fees, charges or other costs to recover from incidents, including fraud protection for breach of information if best practices for security were not followed
- subject to legal actions from internal and external agencies.

Such penalties shall be levied through ordinary disciplinary procedures set forth in other official university personnel policies, including the NKU Faculty Policies and Procedures Handbook (the "Faculty Handbook") and the Chase College of Law Faculty Policies and Procedures (the "Chase Faculty Handbook").

Please see NKU's Acceptable Use policy for additional details on IT usage and policy enforcement, and contact the IT Help Desk (x6911) for assistance with security needs.

VI. EXCEPTIONS

Exceptions are limited in regards to data and information protection measures. If an individual is required for a business need to store highly sensitive Confidential or Private data that are outside NKU managed networks, that individual must obtain permission from the Chief Information Officer and the area Vice President.

VII. REFERENCES AND RELATED MATERIALS

REFERENCES & FORMS

Family Educational Rights and Privacy Act (FERPA)

Health Insurance Portability and Accountability Act (HIPAA)

NKU Virtual Private Network (VPN) information

NKU Data Governance website

NKU Data Classification categories

RELATED POLICIES

NKU Acceptable Use policy

REVISION TYPE	MONTH/YEAR APPROVED
Minor Edits/Update Links & Formatting	May 11, 2022
Revision	May 16, 2018
New Policy	July 2, 2016
Replaces Security Policy; Social Security Number Usage	March 22, 2006

INFORMATION SECURITY

PRESIDENTIAL APPROVAL

PRESIDENT

Signature  Date 5/16/18

Gerard St. Amand

BOARD OF REGENTS APPROVAL

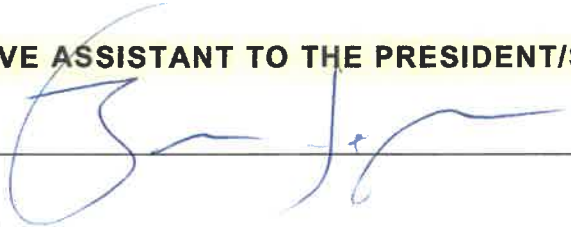
BOARD OF REGENTS (IF FORWARDED BY PRESIDENT)

☑ 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: 9 / 12 / 18.

☐ 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.)

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

Signature  Date 9.18.18

Benjamin Jager