1. POLICY STATEMENT

Northern Kentucky University 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).

The NKU Information Security 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 which access information technology information and data;

Each member of the NKU campus community is personally responsible for the security and protection of NKU information and data resources over which he or she has access, use, and/or control, and must adhere to the Acceptable Use Policy. Resources to be protected include data stored on any laptops, desktops, mobile devices (iPads, tablets, cell phones, etc.), any data which are accessed, transferred or stored, regardless of format (text, graphic, audio), passwords, decryption and 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 (FERPA, HIPAA, etc). 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.
<table>
<thead>
<tr>
<th>Confidential Data (highest, most sensitive)</th>
<th>Private Data (moderate level of sensitivity)</th>
<th>Public Data (low level of sensitivity)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Legal Requirements</strong></td>
<td>NKU has a contractual obligation to protect the data</td>
<td>Governed by the Kentucky Open Records Act, K.R.S. §§ 61.870 to 61.884</td>
</tr>
<tr>
<td><strong>Reputation Risk</strong></td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td><strong>Other Institutional Risks</strong></td>
<td>Smaller subsets of protected data from a school or department</td>
<td>General university information</td>
</tr>
<tr>
<td><strong>Access</strong></td>
<td>Only those individuals designated with approved access, signed non-disclosure agreements, and a need-to-know</td>
<td>NKU employees and non-employees who have a business need-to-know</td>
</tr>
<tr>
<td><strong>Examples</strong></td>
<td>• Student education records</td>
<td>• Information resources with access to confidential data</td>
</tr>
<tr>
<td></td>
<td>• Individual health records and information</td>
<td>• Research data or results that are not confidential data</td>
</tr>
<tr>
<td></td>
<td>• Human subjects research data that identifies individuals</td>
<td>• Information covered by non-disclosure agreements</td>
</tr>
<tr>
<td></td>
<td>• Prospective students</td>
<td>• Materials for performance of official duties</td>
</tr>
<tr>
<td></td>
<td>• Personally Identifiable Financial Information</td>
<td>• Proprietary information of NKU or others contained within proposals, contracts, or license agreements</td>
</tr>
<tr>
<td></td>
<td>• Campus Security Systems and Details</td>
<td>• Campus maps</td>
</tr>
<tr>
<td></td>
<td>• Credit card numbers</td>
<td>• Directory information (e.g. Contact Information, Find It)</td>
</tr>
<tr>
<td></td>
<td>• Certain management information</td>
<td>• Departmental Websites</td>
</tr>
<tr>
<td></td>
<td>• Social Security Numbers</td>
<td>• Academic course descriptions</td>
</tr>
<tr>
<td></td>
<td>• Government restricted and/or classified information</td>
<td>• News</td>
</tr>
<tr>
<td></td>
<td>• Financial transactions of students and employees</td>
<td>• Information posted on university website</td>
</tr>
<tr>
<td></td>
<td>• 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.)</td>
<td>• Budgets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Purchase Orders</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• All institutional data made available to the general public by the Open Records Act</td>
</tr>
</tbody>
</table>
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 your due diligence in keeping data secure.

DO:

• Understand NKU’s Data Classification Categories (see addendum):
  • 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.
    o Examples of Confidential data include, but are not limited to social security numbers, drivers license numbers, credit card or banking information, student academic information such as grades or GPA, etc.
    o Examples of Private data include but are not limited to academic reports, research data, technical reporting such as system logs, faculty tenure evaluations, etc.
    o Public data items include campus promotional materials, class schedules, catalog information, annual reports, press releases, directory information, etc.
  • For a more comprehensive list of examples and legal requirements, please visit: http://datagovernance.nku.edu/content/dam/DataGovernance/docs/Data%20Classification.pdf
  • 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 information regarding NKU and FERPA guidelines, see http://www.nku.edu/~registrar
  • Use Encryption for Laptops: All NKU owned laptops will be encrypted. 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.
  • 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, provided through NKU. Storing such data on hard drives (laptops, desktops, tablets, etc.) can subject the data to breach by viruses, malware, hacking, physical loss of device, etc. IT can assist if you require storage quotas that exceeds currently allocated amounts.
  • Use Virtual Private Network (VPN) to access data when not on campus (home, travel, etc.) Our VPN technology provides security when used from remote locations. See http://oit.nku.edu/vpn.html
  • Only access confidential and/or private data through encrypted or secure networks when on campus
  • A secured login must be used when leaving your device unattended. (i.e. When leaving your computer unattended, you must lock your screen and require login to re-access)
  • Do 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.
  • Do report any breaches, inappropriate disclosures, abuses, data loss, or unauthorized alterations to abuse@nku.edu
  • Do require personnel handling confidential or private data to sign non-disclosure statements.
  • 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 and Third Party Data Services: The use of individual “cloud” based storage services such as Google Docs, Drop Box, 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.

• Store Confidential or Private data on 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 Service Center.

• 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.

• Email Messages: Do not send Confidential or Private data through 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
• subject to legal actions from internal and external agencies.

Please see the Acceptable Use Policy for additional details on IT Usage and Policy enforcement, and contact the IT Help Desk or (x6911) for assistance with security needs.

VI. EXCEPTIONS

Exceptions are limited in regards to data and information protection measures. If an individual is required to store highly sensitive, Confidential or Private data for a business need 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

RELATED POLICIES
<table>
<thead>
<tr>
<th>REVISION TYPE</th>
<th>MONTH/YEAR APPROVED</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Policy</td>
<td>07/2016</td>
</tr>
<tr>
<td>Choose an item.</td>
<td></td>
</tr>
<tr>
<td>Choose an item.</td>
<td></td>
</tr>
<tr>
<td>Choose an item.</td>
<td></td>
</tr>
<tr>
<td>Choose an item.</td>
<td></td>
</tr>
<tr>
<td>Choose an item.</td>
<td></td>
</tr>
</tbody>
</table>
INFORMATION SECURITY

APPROVALS

FINAL APPROVAL

SENIOR VICE PRESIDENT FOR ADMINISTRATION & FINANCE

CONTACT DIVISION OF ADMINISTRATION & FINANCE 7/2/2016
Signature Date

Sue Hodges Moore Printed Name

PRESIDENTIAL APPROVAL

PRESIDENT

CONTACT DIVISION OF ADMINISTRATION & FINANCE 7/2/2016
Signature Date

Geoffrey S. Mearns Printed Name

BOARD OF REGENTS APPROVAL

BOARD OF REGENTS (IF FORWARDED BY PRESIDENT)

☒ This policy WAS NOT forwarded to the Board of Regents.
☐ This policy WAS forwarded to the Board of Regents.

☐ 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.)

POLICY COORDINATOR

Signature 7/2/2016 Date

Justin M. Duncan Printed Name