SECURITY POLICY

POLICY NUMBER: RESERVED FOR FUTURE USE
POLICY TYPE: ADMINISTRATIVE
RESPONSIBLE OFFICIAL TITLE: CHIEF INFORMATION OFFICER (CIO)
RESPONSIBLE OFFICE: OFFICE OF INFORMATION TECHNOLOGY

I. POLICY STATEMENT

1.0 Overview:

Northern Kentucky University recognizes the obligation to protect confidentiality, maintain the integrity, and ensure appropriate availability of information about students, faculty, staff, alumni, and customers, and to provide proper administrative, technical and physical safeguards to protect university information assets

2.0 Scope:

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.
The NKU Information Technology Security Policy includes:

- information and data that is acquired, transmitted, processed, transferred and/or maintained by NKU organizations;
- 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;
- faculty, staff, administrators, students, alumni, and consultants employed by NKU organizations and other persons having access to NKU information and data resources.

Examples of sensitive and confidential data includes, but is not limited to social security numbers, driver's license numbers, credit card or banking information, student academic information such as grades or GPA, etc.

3.0 Policy:

Each member of the NKU campus community is personally responsible for the security and protection of electronic information resources over which he or she has control, and must adhere to the *Acceptable Use Policy*. Resources to be protected include data stored on laptops, desktops, mobile devices (including cell phones), and any data which is accessed, transferred or stored, regardless of format (text, graphic, audio). The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, inappropriate or unsafe storage of confidential data, 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 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.

As of July 1, 2010, all newly deployed Windows laptops will be encrypted using Bitlocker. Exceptions will only be allowed with VP approval. In addition, the university forbids the storage of highly sensitive data on any data storage device or media other than a centrally managed server, or a secure NKU networked file storage area. If an individual is required to store highly sensitive data for a business need that is outside NKU managed networks, that individual must obtain permission from the *Chief Information Office and the area Vice President*. The written request for authorization must state the unique business need, the type of data that will be stored, the type of data storage device that will be used, and the mitigating controls that will be employed to protect the highly sensitive data.

Any university employee, student or non-university individual who stores highly sensitive 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.
In addition, The Family Education Rights and Privacy Act (FERPA) guidelines are maintained and adhered to for students rights control disclosures of their records. For information regarding NKU and FERPA guidelines, see http://www.nku.edu/~registrar.

4.0 Enforcement:

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 service center at http://it.nku.edu/itsc or (x6911) for assistance with security needs.

5.0 Exceptions:
Exceptions are limited in regards to data and information protection measures. Please contact your area vice president for exception requests.

II. ENTITIES AFFECTED

Faculty, Staff, Students, Contactors, Alumni and individuals authorized by affiliated institutions or organizations

REVISION HISTORY

REVISION TYPE	MONTH/YEAR APPROVED
Choose an item.	
Choose an item.	
Choose an item.	
Choose an item.	
Choose an item.	
Choose an item.	
Choose an item.	