I. POLICY STATEMENT

Reason for this Policy

In today’s society, identity theft is one of the fastest-growing white-collar crimes in the United States. According to the federal government fact sheets on social security number (SSN) security, incidents of identity theft may triple in the coming years. Universities are becoming the latest targets due to historically relaxed and widespread usage of SSN’s and other forms of sensitive information.

Northern Kentucky University is dedicated to ensuring the privacy and proper handling of SSNs of its students, employees, and individuals associated with the University. The primary purpose of this Social Security Number policy is to ensure that the necessary procedures and awareness exist so that University employees and students comply with both the letter and the spirit of Family Educational Rights and Privacy Act (FERPA) 20 U.S.C. § 1232g and Kentucky Law; KRS § 160.720 and KRS § 61.878. SSNs have been used within University systems to uniquely identify students and employees and to permit students and employees to gain access to their own confidential information.

This policy is guided by the following objectives:

1. Broad awareness of the confidential nature of the SSN.
2. Reduced reliance upon the SSN for identification purposes.
3. Increased emphasis on secure use, transmission, and storage of the SSN throughout the Northern Kentucky University Information Systems.
4. A consistent policy toward and treatment of SSNs throughout the University.
5. Increased confidence by students and employees that SSNs are handled in a confidential manner.

Statement of Policy

It is Northern Kentucky University’s intent to protect the SSNs of its students, staff, and faculty to minimize the growing risks of identity theft. Accordingly, the SSN should not be used as a common identifier or used as a database key in any electronic information system. Although our current legacy applications use SSN as a key, it is the intent that the new system (SAP) will use a unique identifier within the new applications. All other 3rd party software and record storage will be evaluated for use and storage of any data which is considered confidential in nature. The SSN may be collected and used when necessary for employment records, financial aid, and other purposes as permitted by law.
records, and a limited number of other business and governmental transactions, as required by law. In all cases, storage and retrieval of sensitive information will be protected from mishandling and theft. Northern Kentucky University will be working toward elimination of the use of the SSN wherever possible.

The following are Northern Kentucky University policy regulations that apply to all systems:

- All new systems purchased or developed by Northern Kentucky will not use SSN as identifiers except where such use is specifically permitted or required under this policy. Such systems should not visually display the SSN on any system output, including monitors and printed forms, unless required by law or required by Northern Kentucky University as needed in execution of its duties.
- No new system or technology, where the SSN is a consideration, will be developed or purchased by Northern Kentucky unless it is compliant with this policy or approved by the office of Information Technology in its use.
- All University forms and documents that collect SSNs will use the appropriate language to indicate whether request is voluntary or mandatory. Unless the University is legally required to collect an SSN, individuals will not be required to provide their SSNs verbally or in writing at any Point of Service, nor will they be denied access to those services should they refuse to provide an SSN. However, individuals may volunteer their SSNs if they wish as an alternate means of locating a record.

Compliance

Each Department head, dean, or director will be responsible to ensure adherence and to monitor compliance with this policy. An employee, student, volunteer, representative, contractor, or any other agent of Northern Kentucky University who has substantially breached the confidentiality of SSNs may be subject to disciplinary action or sanctions up to and including discharge or dismissal, in accordance with University policy and procedures.

Any new and existing business needs which are unable to comply with these policy requirements must be documented clearly and approved by the IT Security organization at Northern Kentucky University, and the area Department Head.

Procedures

SSN Usage:
SSN’s will not be verbally requested in public places.
Grades and other pieces of personal information may not be publicly posted or displayed in a manner where the complete SSN, or partial SSN, are used to identify an individual.

In all new systems, SSNs will be transmitted electronically only through encrypted mechanisms.

SSN’s may not be stored on laptops or unsecured personal computers.
Paper and electronic documents containing SSNs will be disposed of in a Secure Fashion in accordance with data-handling requirements, such as shredding and sufficient deletion/purge procedures.
SSNs will be released by the University to external entities only:
As allowed or required by law; OR
When permission is granted by the individual; OR
When the external entity is acting as the University's contractor or agent and adequate security measures and agreements are in place to prevent unauthorized dissemination to third parties. The SSN may continue to be collected and stored as a confidential attribute associated with an individual. The SSN will be used as required by law as a method to identify individuals.

Phased Compliance Strategy:
Northern Kentucky University will adopt a Phased Compliance Strategy for its existing systems. All Colleges, Departments, Divisions, and Business Units will be required to comply with system and process modifications related with this policy as soon as reasonably possible. The new ERP system will begin the elimination of SSN usage as a unique identifier, and all other systems will need to be evaluated for similar changes.

Who Should Know This Policy
- President
- Provost and Vice Presidents
- Deans/Department Chairs
- Directors/Department Heads
- All Faculty, Staff, and Students

II. ENTITIES AFFECTED
Faculty, Staff, Students, and the University Community

REFERENCES & FORMS
Related Documents
The following documents provide further information related to FERPA and the Privacy Act of 1974:
http://www.usdoj.gov/foia/privstat.htm
The following document provides information on State guidelines:
http://www.lrc.ky.gov/KRS/061-00/878.PDF
http://www.lrc.ky.gov/KRS/160-00/720.PDF

Additional Resources:
Questions regarding this NKU SSN Security should be directed to the Office of Information Technology and / or Legal Affairs.

Contact Telephone
Office of Information Technology (859) 572-5139
Office of Legal Affairs (859) 572-5588

REVISION HISTORY

<table>
<thead>
<tr>
<th>REVISION TYPE</th>
<th>MONTH/YEAR APPROVED</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Policy</td>
<td>3/22/2006</td>
</tr>
</tbody>
</table>

Choose an item.