UNIVERSITY OF NEBRASKA UNK KEARNEY

Social Security Number Policy Guidelines

Information Technology Services

All departments were instructed to be in compliance with the University of Nebraska at Kearney Social Security Number Policy by January 1, 2008.

These guidelines will help departments and individuals remain in compliance with the policy.

- Documents should not collect and processes should not use Social Security Number unless required by law, such as for payroll purposes. Documents can be paper or electronic.
- If a unique identifier is needed for each person, consult with Information Technology Services to determine the appropriate data field.
- If Social Security Number is required, you must request an exemption from the Social Security Number Policy through Information Technology Services.
- Do not send Social Security Numbers via email unless the email message is encrypted. Encryption may not be possible if email message are destined for off-campus addresses.
- Paper documents with Social Security Numbers must be stored in locked cabinets in a locked room.
- Paper documents that have been retained beyond the date specified in the NU records retention schedule should be destroyed by cross-cut shredding. Until the documents are destroyed, they should be protected as described above.
- Identify removable media, such as flash drives, CDs, DVDs etc. that store Social Security numbers. Keep such media in a locked cabinet in a locked room, similar to paper documents. If the removable media is no longer needed, physically shred or destroy the media to dispose of it. Social Security Numbers must not be stored on removable media without an exemption from the Social Security Number Policy.
- Apply for an exemption from the Social Security Number Policy if you must retain documents, either paper or electronic, with social security numbers.
    - An exemption request is NOT required for direct access to SAP/HR and SIS/PeopleSoft application data. However, if you have Social Security Numbers from these systems stored on your workstation or removable media, an exemption must be requested.
    - An exemption request is required for paper documents for SAP/HR and SIS/PeopleSoft.
    - An exception request is required if you store Social Security Numbers from the paper documents on your workstation or on removable media.
    - An exemption request is required if you store paper documents with Social Security number in a document imaging system.
    - Exemptions that are granted will be reviewed annually.

Protecting the nonpublic personal information of our employees and students is an important responsibility. The practices listed below can help us ensure that information stays protected.

- Email is one method for attacking your computer or mobile device. It is easy for an attacker to send a message that can infect your device.
    - Use up-to-date anti-virus software.
    - Use encrypted email or do not send confidential information.
    - Do not open attachments you are not expecting.
    - Do not click on links to web pages that arrive in email.
    - Report any suspicious email messages you receive to the Technology Helpdesk.
    - Keep your preview pane closed.
    - Never respond to spam—even to "unsubscribe."
- Sensitive communication via email poses real risks. The most common disclosures result from email accidentally sent to the wrong person. Therefore, use special care when addressing email with sensitive information. For highly sensitive data, choose methods other than email.
- Use special care when faxing sensitive information. Be sure that the fax number is correct and that someone on the other end will promptly retrieve the faxed document.
- Use special care when handling paper documents. Do not leave documents with Social Security Numbers on your desk when you leave. Do not share Social Security Numbers over the telephone when your conversation can be overheard by others.
- Choose a strong password, that is, one that is difficult to guess. If you think your password has been compromised or shared, change it immediately.
- Do not share passwords and do not allow anyone to work on a computer that you have logged into.
- Recognize when your computer may be compromised. It can be difficult to tell when your computer system has suffered a security compromise. If you notice your computer behaving slowly, rebooting by itself, or exhibiting any unusual behavior, notify an IT support person.
- Avoid risky web and email activities:
    - Be skeptical of email and web sites that ask you to provide personal information, such as Social Security Number, to download software or files.
    - Confirm that an embedded web link in the body of an email goes where it is expected to go before you click on it.
    - "Free stuff on the Internet is like candy from a stranger." Be aware that seemingly harmless games, utilities, and other "fun stuff" can work behind the scenes and install spyware or other malicious software (malware) on your computer. They can harbor viruses and even open a "back door" giving access to your computer.
    - Identity theft is the intentional use or theft of a person's private information to obtain goods or services. Any purchase at a web site or any online transaction,

such as online banking, increases your risk of identity theft. Take precautions to ensure the confidentiality of your private information.
    - Only download from well-known software vendors.
- Any security incidents involving systems that store and/or have access to Social Security Number must be reported promptly to the Technology Helpdesk. Security incidents include, but are not limited to, virus infections, spyware infections, rootkits, compromises such as hacks and inappropriate use, and lost media or lost devices.

History

Original – 2007

Reviewed, updated, reformatted – December, 2015