Current methods for collection, use, and storage of Social Security numbers in a variety of campus administrative and academic departmental processes create an ongoing risk to the University. Historical use of Social Security number as the University’s student ID number, as well as its formal and informal use in a wide variety of business practices has created a large collection of sensitive data spread throughout University department’s electronic storage and files. The University is at risk of SSN exposure and associated costs until the sensitive information is removed where not required and new business processes of ensuring the privacy and proper handling of SSNs are put in place.

You are encouraged to follow these guidelines when handling Social Security Numbers:

**Paper Guidelines**

**Do not...**
- Do not leave papers and forms containing SSN unsecured.
- Do not make unnecessary copies of forms containing SSN.

**Instead...**
- Secure papers and forms containing SSN in a locked cabinet or office.
- Redact SSN using a black marker/white out.
- Make a scan or copy of papers and forms containing SSN after redacting. Then destroy the original.
- Shred/destroy unnecessary paper containing SSN by placing papers in the Shred-It Bins located on campus.*

*Adhere to the University's records retention schedules which can be found at [http://archives.nd.edu/records](http://archives.nd.edu/records)

**Removable Media Guidelines**

**Do not...**
- Do not leave removable media containing SSN unsecured.
- Do not use un-encrypted media to transfer files and data containing SSN.

**Instead...**
- Use encrypted removable media.
- Password protect files and data containing SSN.
- Remove sensitive files and data before sharing removable media.
- Adhere to the University’s electronic retention schedule for sensitive data reports, forms, and spreadsheets.
- Store sensitive information on a CORPFS drive rather than removable media.

**General Guidelines**

- Use 9-digit NDID as identifier (instead of SSN/TIN/EIN).
- Utilize the Shred-It Bins located on campus to shred/destroy papers, forms and files containing sensitive information.
- Run Identity Finder tool regularly and fully remediate the results.
- Follow University records retention schedules which can be found at [http://archives.nd.edu/records](http://archives.nd.edu/records)

**Electronic Guidelines**

**Do not...**
- Do not store data files containing SSN on local hard drives.
- Do not send unencrypted/unsecure data files containing SSN in email. Use the Identity Finder Shred capability or Eraser to permanently delete email containing SSN.

**Instead...**
- Store data files containing SSN in CorpFS Filespace.
- Password protect files and data containing SSN.
- ERASE data files containing sensitive information.
- Adhere to the University’s electronic retention schedule for sensitive data reports, forms, and spreadsheets.