A. Statement
North Dakota State University (NDSU) recognizes that it collects and maintains Social Security numbers (SSNs). The University, in the course of its operations, is dedicated to ensuring the privacy and proper handling of this information.

B. Purpose/Rationale
Social Security numbers are highly confidential and legally protected data. The University is committed to protecting individuals’ SSNs; therefore, the use of SSNs as identification numbers must be limited. This document provides standards and guidelines on the proper use and disclosure of SSNs.

The Federal Privacy Act of 1974, the Family Education Rights and Privacy Act (FERPA), and related amendments establish guidelines regarding the use of and requests for Social Security numbers. It is the duty of the University:

- To inform individuals when the collection of SSNs is required;
- To identify the authority that specifies the need for SSNs;
- To define the principle purpose(s) for collection and use of SSNs;
- To outline the consequences that may occur when SSNs are not provided.

C. Scope
NDSU has adopted a phased compliance strategy for all divisions, current administrative systems, and campus applications. This strategic plan includes:

- Increasing awareness of the confidential nature of SSNs;
- Reducing reliance upon SSNs for identification purposes;
- Ensuring consistent and appropriate handling of SSNs throughout the University;
- Eliminating non-essential use of SSNs.

D. Standards and Guidelines

1. NDSU recognizes the North Dakota University System ID number (EmplID) as the primary identification number for students, employees, and persons with a recurring business, educational, and/or research relationship with NDSU. EmplIDs are used in all electronic and paper data systems to identify, track, and serve individuals associated with the University, except in cases where the use of SSNs is mandated by federal or state law.

2. All occurrences of SSNs in electronic and paper format must be reported using the “Social Security Number Registration Form” (www.ndsu.edu/vpfa/forms/). This form is submitted to the NDSU Audit and Advisory Services.

3. NDSU does not use SSNs as common identifiers and/or primary keys in databases, except where required for employment, financial aid, and in a limited number of other
Social Security Numbers Standards and Guidelines
North Dakota State University

authorized University-related processes. Other identifiers, such as EmplIDs or application specific identifiers must be used in place of the SSNs.

4. Displaying grades and other student-related information using SSNs, or any portion thereof, is prohibited.

5. Reasonable precautions must be taken to protect the privacy of SSNs, but SSNs must be available to University employees when required to complete University-related processes.

6. SSNs must be stored as confidential and protected attributes associated with individuals’ institution records.

7. Access to this information by University employees is required by job function and authorization. Persons with such access are required to sign confidentiality agreements and complete data privacy training.

8. Access to SSNs by non-university persons and entities is governed by contractual agreements.

9. Access to electronic and paper records must be monitored through the use of logs, which are monitored on a regular basis to determine if there are anomalies. Any unusual activity/anomaly must be reported to the supervisor.

10. Electronically stored and transmitted SSNs must be protected by secure methods, such as encryption.

11. Paper documents containing SSNs must be stored using appropriate security controls to maintain confidentiality of the SSNs.

12. Paper documents containing SSNs must be disposed of in a secure manner, such as shredding or through the use of a licensed and bonded vendor.

13. SSNs may be released to entities outside the University only:
   a. As allowed by law;
   b. When permission is granted by the individual; or
   c. When the external entity is contracted by the University and adequate security measures are guaranteed to prevent unauthorized dissemination to third parties.

14. University forms and documents that collect SSNs must state if the request is required or optional.

15. The University does not disclose SSNs for any purpose that is not consistent with applicable law.
   a. Federal regulations require that financial aid applicants provide their SSNs when completing the “Free Application for Federal Student Aid” (FAFSA). SSNs are the identifiers used to validate database matches (e.g., Social Security, Selective Service, loan default, etc.) to confirm financial eligibility, and for reporting purposes from the institution to the Department of Education.
   b. The University is required by federal law to report to the IRS the students’ names and SSNs, the amount billed for qualified tuition and related expenses less any
qualified waivers, and the total amount of scholarships or grants disbursed to the students for tuition and related expenses.

c. The University is required by federal and state laws to report income and benefits along with SSNs for all persons to whom compensation is paid.

d. Research subjects who are compensated may be asked to provide basic information including names, mailing addresses and SSNs. This information allows the University to meet government reporting obligations. Subjects may be given the opportunity to waive receipt of payments should they decline to provide identifying information.

16. When necessary, patient systems within NDSU may be required to use SSNs for billing and health care coordination purposes. When SSNs identify protected health information, their use is regulated by the Health Insurance Portability Accountability Act (HIPAA), FERPA, and/or state law.

17. SSNs are required on certain forms used to petition for immigration benefits, such as U.S.A. work authorization and/or legal presence, as well as permanent residency applications.

18. Any employee or student who has breached the confidentiality of SSNs may be subject to disciplinary action or sanctions up to and including discharge and dismissal in accordance with University policies and procedures. Violation may also result in criminal prosecution.

19. Any applications or systems used by the University that store SSNs are subject to audits and assessments conducted by the NDSU Audit and Advisory Services.

E. Roles and Responsibilities

1. Each division’s vice president or designee is responsible for:
   a. Overseeing and protecting SSNs;
   b. Ensuring that all occurrences of SSNs, where not required, are removed from electronic and hard copy files.

2. NDSU Audit and Advisory Services is responsible for:
   a. Knowing which divisions collect, store, and maintain SSNs both in hard copy and electronic format;
   b. Auditing and assessing the standards and guidelines;
   c. Providing education and recommendations to divisions who are not in compliance.

3. Oversight and maintenance of the standards and guidelines is the responsibility of the working group consisting of representatives from the following divisions.
   - Academic Affairs
   - Agriculture and University Extension
   - Alumni Association/Development Foundation
Social Security Numbers Standards and Guidelines
North Dakota State University

F. Definitions

**EmplID**: A unique identification number assigned to an NDSU employee, student, or non-university person.

**Social Security number (SSN)**: A nine-digit number issued to U.S. citizens, permanent residents, and temporary (working) residents under section 205(c)(2) of the Social Security Act, codified as 42 U.S.C. § 405 (c)(2). The number is issued to an individual by the Social Security Administration, an independent agency of the United States government. Its primary purpose is to track individuals for taxation purposes.

**Confidentiality Agreement**: An agreement restricting a person from disclosing confidential, intellectual, or proprietary information.

**Non-university person**: A person that is neither an employee nor student of NDSU, but has a valid interest in NDSU as a vendor, researcher, scholar or other.

**Electronic data system**: The transfer of structured data, by agreed message standards, from one computer system to another.

**HIPAA**: The Health Insurance Portability and Accountability Act was enacted by the U.S. Congress in 1996. This Act provided for national standards for electronic health care transactions and code sets, unique health identifiers, and security. The final Privacy Rule (adopted in August 2000) set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, healthcare clearing houses, and health care providers who conduct the standard health care transactions electronically.

(www.hhs.gov/ocr/privacy/hipaa/administrative/index.html/)

**FERPA**: The Family Education Rights and Privacy Act is a federal law which was passed in 1974. The law protects the privacy of student educational records and provides rights to students for access to and amendment of those records. FERPA applies to any higher education institutions receiving federal funds administered by the Department of Education (DOE).
Red Flag Rule: Rules and guidelines implementing Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA), known as the RED FLAG RULES. This Section requires that all organizations, subject to the legislation, must develop and implement a written "Identity Theft Prevention Program" to detect, prevent and mitigate identity theft in connection with the opening of certain new and certain existing accounts.

Federal Privacy Act 1974: The Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. The Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register. The Privacy Act prohibits the disclosure of information from a system of records absent the written consent of the subject individual, unless the disclosure is pursuant to one of twelve statutory exceptions. The Act also provides individuals with a means by which to seek access to and amendment of their records, and sets forth various agency record-keeping requirements.

G. References

Existing policies and practices

NDSU
Policy 158 Acceptable Use of Electronic Communications Devices;
Policy 509 Electronic Financial Transaction Policy;
Policy 513 Collection Policy;
Policy 600 Family Education Rights and Privacy Act of 1974 - FERPA and FERPA Notice;
Policy 703 Bison Card Terms and Conditions;
Policy 707 Card/Key Access and Building Security;
Policy 713 Records Management;
Policy 718 Public/Open Records;
NDSU Information Safeguarding (GLB);
NDSU HIPPA Privacy/Security Policy and Procedures

NDUS
Policy1901.2 Computing Facilities and corresponding Procedure 1901.2;
Policy 1901.3 Information Technology Project Management and corresponding Procedure 1901.3;
Policy 1912 Public Records and corresponding procedures:
Procedure 1912.1 Information Security Procedures;
Procedure 1912.2 Student Records - Directory Information;
Procedure 1912.3 Employee Personal Information
Social Security Numbers Standards and Guidelines
North Dakota State University

Existing federal and state regulations
The Federal Privacy Act of 1974
The Federal Information Security Management Act of 2002 (FISMA)
The Family Education Rights and Privacy Act of 1974 (FERPA)
The Gramm Leach Bliley Act of 1999 (GLBA)
The Health Insurance Portability Accountability Act (HIPAA)
The Fair Credit Reporting Act
The Children’s Online Privacy Protection Act
Fair and Accurate Credit Transaction Act of 2003 (FACTA)
Red Flag Rules – Interpretation of Sections 114 and 315 of FACTA
North Dakota Century Code, Chapter 44-04, Open Records

H. History

Created On: June 2009

Author(s) Chair persons: Assistant to General Counsel
Chief Information Technology Security Officer

Revised: October 2009

Approved by: