Social Security Number Protection

Introduction

Iowa State University recognizes that it collects and maintains confidential information relating to its students, employees, and individuals associated with the University and is committed to maintaining the privacy and confidentiality of an individual's Social Security Number (SSN). This policy applies to all individuals and University organizational units that have access to, collect, or use an individual's SSN.

Policy Statement

University ID shall replace SSN as the primary identifier used by the university. The university will discontinue the use of SSN as the primary identifier. Therefore, the use of SSN as an identification number within the university shall be limited as permitted by law.

To protect the privacy of persons whose SSN is collected, all university offices will follow procedures maintained by the policy administrator and managed by university-designated data stewards. These procedures were to be implemented by June 30, 2007, with requests for extensions of time to implement to be directed to the Policy Administrator prior to that date.

Persons responsible for breaching the privacy of another person by improperly obtaining, using or disclosing a SSN are subject to discipline as provided in the applicable faculty and staff handbooks or collective bargaining agreement and the Student Disciplinary Regulations.

The following rules of conduct apply:

- Employees and students shall comply with the provisions of this policy as well as related institutional policies and procedures.
- Employees may not request disclosure of a SSN from an individual if it is not necessary for the purposes of the university and the particular function for which the employee is responsible.
- Employees and students shall not disclose the SSN of another person to unauthorized persons or entities.
- Employees and students may not seek out or use the SSN of another person for their own interest or advantage.
- Employees responsible for the maintenance of records containing SSNs shall observe all institutionally-established administrative, technical, and physical safeguards in order to protect the confidentiality of such records.
35• Employees shall report promptly to their supervisor any inappropriate disclosure of a SSN.

36If SSNs are inappropriately disclosed and individuals have been put at risk of identity theft or other
37harm as a result of the disclosure, the Office of University Counsel shall be notified promptly.

38Definitions
39Primary Identifier
40The primary identifier is the unique number used for identification.

41University Identification Number
42The University Identification Number (University ID or UID) is an assigned number used for the
43exclusive purpose of identifying those who are affiliated with the university, or those who desire to
44acquire services or access resources owned or operated by the university. The University ID is
45displayed as the middle block of 9 digits on the ISUCard.

46Data Steward
47Data Stewards are university executive officers or their designees who have planning and policy-
48level responsibilities for data in their functional areas. These data stewards, as a group, are
49responsible for recommending policies and establishing procedures and guidelines for university-
50wide data administration activities. Data stewards, as individuals, have management responsibilities
51for defined segments of the institutional databases such as SSN.

52Resources
53Links
54• UID / ISUCard
55• UID / ISUCard - Confidential Data in Electronic Communications
56• Office of University Counsel
57• Student Disciplinary Regulations

58Files
59• SSN Protection Procedure [PDF]
60• SSN Protection FAQ [PDF]