3359-11-10.6 Social security number use policy.

(A) Introduction.

The university of Akron is dedicated to ensuring the proper handling of confidential information relating to its students, employees, and individuals associated with the university. The university understands that social security numbers are highly confidential and legally protected data. This policy establishes an official policy to migrate from using the social security number as a common identifier, by establishing regulations regarding the university's collection, maintenance, and distribution of social security numbers.

(B) Policy purpose.

To reduce, where necessary, the use of and reliance on social security numbers for identification purposes and for the following other purposes:

(1) To protect the privacy and legal rights of the members of the university community.
(2) To generate broad awareness of the confidential nature of the social security number.
(3) To foster compliance with the Family Educational Rights and Privacy Act and the Privacy Act of 1974.
(4) To promote confidence by students and employees that social security numbers are handled in a confidential manner.

(C) Policy.

(1) It is the university of Akron's policy that the use of the social security number as a common identifier and the primary key to

appropriate social security number administrator.

(D) Procedures/regulations.

(1) A unique identification number shall be assigned to all students, employees, and other individuals associated with the university. This university ID shall be assigned at the earliest possible point of contact between the individual and the university. The ID shall be used as the campus ID Card identifier and shall be used in all future electronic systems and on paper documents to identify, track, and provide service to individuals associated with the university. It shall be permanently associated with the individual to whom it is originally assigned. The ID shall be jointly maintained and administered by the registrar, department of residence and the division of information technology services (ITS).

(2) Personal information shall not be publicly posted or displayed in a manner where either the university ID or the social security number identifies the individual associated with the information.

(3) Encryption of social security numbers is required between server and client workstations and whenever data is transmitted over unsecured networks.

(4) All documents (paper and electronic) and any storage media containing social security numbers shall be disposed of in a timely and secure fashion consistent with the university's record retention policy.

(5) Except in those cases where the university is required to collect a social security number, individuals shall not be required to provide their social security number, verbally or in writing, at any point of service, nor shall they be denied access to those services should they refuse to provide a social security number. Individuals may volunteer their social security number if they wish, however, as an alternate means of locating a record.

(6) The university shall release social security numbers to entities outside the university (contractors, vendors, service providers) as allowed by law or when the individual grants such permission. University contracts with outside entities shall include, if relevant,

language identifying the responsibility and restrictions on the use of social security numbers by the third party.

(7) Social security numbers may continue to be stored as a confidential attribute associated with an individual. The social security number shall be used as allowed by law; and as an optional key to identify individuals for whom an ID is not known.

(8) The university division of finance and administration shall assign an existing administrator to oversee social security number use relating to employees and other individuals (anyone other than students, prospective students, parents, and alumni) associated with the university. The division of student affairs shall assign an existing administrator to oversee social security number use relating to students, prospective students, parents and alumni.

(9) All university forms and documents that request social security numbers shall include an approved disclosure statement, and shall indicate whether the request is voluntary or mandatory. Existing forms and documents shall be modified as they are reprinted. Approved statements shall be available through the social security number administrators.

(10) Information technology services (ITS), in conjunction with the social security number administrators and the information technology security policy committee (ITSPC), shall develop a set of standards and guidelines addressing the handling of social security numbers in electronic systems. Adherence to these guidelines in all future development shall be considered a requirement of this policy statement.

(E) Implementation.

(1) The university, through its ITSPC, shall develop objectives to improve campus-wide awareness of the confidential nature of social security numbers, the need for consistent use of social security numbers, and increased confidence by students, faculty and staff that social security numbers are handled in a confidential manner.

(2) Each social security number administrator shall have the responsibility to:

(a) Coordinate communications to faculty, staff, and students concerning their rights and responsibilities regarding the university's social security number (SSN) policy.

(b) Oversee implementation and adherence to university's SSN policy.

(c) Provide support and guidance for offices working with social security numbers.

(d) Consult with the university auditor when an opinion on the release or exchange of social security numbers is required.

(e) Authorize the use of social security numbers in new systems, as appropriate.

(f) Maintain a list of entities (contractors, vendors, service providers) approved by the university operations auditor, to which social security numbers may be released.

(g) Maintain a set of approved disclosure statements for use on university forms and documents that collect social security numbers.

(F) Compliance.

(1) Compliance with this policy shall be attained through a phased approach. The goal is to attain complete compliance with this policy within three years of its adoption.

(2) The information technology security officer (ITSO) shall be re0/TT0 1 Tf0.0002 433bleBT/TT0 1 Tf0.001 Tc 12 0 012 0 0 be att4c-55n0.0uentities

An employee or student who knowingly violates this policy and/or in any