I. INTRODUCTION (Purpose and Intent)

The threat of identity theft has been growing at an unprecedented rate and the University of South Florida System (USF System) commits to provide enhanced security for its students, staff, faculty and patients. Accordingly, the USF System will no longer use nor permit the use of a Social Security Number (SSN) as an identifier for a person in any USF System information system unless the use of a SSN is imperative for the performance of the USF System’s duties and responsibilities as prescribed by law. All uses of a SSN as an identifier must be approved in writing by the Information Technology Management Council (ITMC).

The purpose of this policy is to:

• Establish a heightened awareness of the confidential nature and proper use of the Social Security Number;

• Mandate elimination of the use of the Social Security Number as the primary identifier in information systems and replace it with an alternate identification number;

• Protect the confidentiality of Social Security Numbers collected by the USF System; and

• Establish an increased confidence by the USF System community that Social Security Numbers are handled in an appropriate and confidential manner reducing the risk of identity theft.
II. DEFINITIONS

USFID

USFIDs are unique, randomly generated numbers issued to all faculty, staff and students in the USF System.

SSN

SSN refers to the Social Security Number or any derivative of SSN.

FERPA

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education, including the USF System.

EMPLID

The EMPLID is the number assigned by the USF Human Resource System, GEMS, as the unique identifier for each individual that is entered into the System. The EMPLID is an integer. The number is assigned at the first entry point for those individuals whose records are stored in GEMS and remains the unique identifier for the individual in that System.

III. SCOPE

This policy applies to the University of South Florida System including all of its component departments, colleges, divisions, centers, direct support organizations, separately accredited institutions and branch campuses.

IV. STATEMENT OF POLICY

The Social Security Number shall be used only as specifically authorized by law or when imperative for the performance of the USF System’s duties and responsibilities as set forth in the USF Statement of Collection and Use of Social Security Numbers. It shall not be used for any other purposes not set forth
therein or in any information system or process for the purpose of identification or authentication of individuals without the approval of the ITMC.

For the Student Information System (OASIS), the primary identifier for each individual will be the USFID. The USFID will be used to access student education records in OASIS. It will be used in all future electronic and paper data systems that identify, track and service individuals associated with OASIS.

The USFID is the property of the USF System and its use and governance shall be at the discretion of the USF System, within the constraints of the law.

All of the information that the USF System holds in its student information systems and any reports generated from the systems which utilize identification numbers will use the USFID instead of SSN as the primary identification number. Faculty and staff will request that students provide their USFID for any transactions involving the institution that require information system access to records.

The only USF System units that will be allowed to collect, electronically transmit, store or use the SSN are offices authorized by the ITMC and in accordance with standards mandated by the Office of Information Security. In accordance to Florida Statute §119.071, the Office of Information Security may require approved units to distribute the USF Statement of Collection and Use of Social Security Numbers to persons from whom SSNs are collected.

Once a unit is authorized by the ITMC to store and/or electronically transmit SSNs, it is the responsibility of that unit to ensure that appropriate controls and processes are in place to determine a user's level of access to the system. Access to areas of the system containing SSNs will be restricted to need-to-know only.

The USFID or SSN should never be used as a password or as a single authentication token.
Institutionally assigned identification numbers like the USFID are considered personally identifiable information under FERPA; that is, specific information that would make a student’s identity easily traceable in the same manner as the student name. As a result, USF System staff are prohibited from releasing, transferring, or otherwise communicating the USFID in situations where the student identity should remain confidential. The USFID is not considered directory information.

The USF Human Resources System will utilize the EMPLID as the primary identifier for all individuals entered into that System.

Grades and other forms of personal information will not be publicly posted or displayed where USFID or SSN identifies the individual associated with the information.

Paper and electronic files containing Social Security Numbers will be disposed of in a secure fashion in accordance with state and federal retention and disposal policies.

Upon the initial collection of a Social Security Number from an individual, USF shall provide a written statement describing the reasons for the collection and potential uses.

Except in instances specifically authorized by this policy, individuals will not be required to provide their SSN, verbally or in writing, at any USF System point of service, nor will they be denied access to those services should they refuse to provide a SSN. Individuals may volunteer their SSN if they wish, as an alternate means of locating an institutional record.

V. RESPONSIBILITIES

The ITMC, with the assistance of University Audit & Compliance and the Office of Information Security, will:

- Oversee and ensure the implementation of this Policy & Procedure and ensure compliance throughout the USF System.
- Maintain a list of all USF System units collecting Social Security Numbers and the purpose
for the collection.

- Provide support, direction and problem resolution for offices collecting, storing, electronically transmitting or utilizing Social Security Numbers.

- Annually recertify offices or units collecting, storing, electronically transmitting or utilizing Social Security Numbers.

VI. VIOLATION OF POLICY

Violations of this policy may result in disciplinary action up to and including discharge or dismissal in accordance with USF System and Campus policy and procedures.

*Current Responsible Office: Information Technology

*Refer to the appropriate Responsible Office website for a current name of the Vice President or other Responsible Officer.