



UNIVERSITY OF CENTRAL FLORIDA

Office of the President

SUBJECT: Collection and Use of Social Security Numbers	Effective Date: 12/5/2018	Policy Number: 4-012.1	
	Supersedes: 4-012	Page 1	Of 4
	Responsible Authority: Vice President for Information Technologies and Resources		

APPLICABILITY/ACCOUNTABILITY

This policy applies to all University of Central Florida employees, contractors, consultants, and agents of the above who collect, maintain, or have access to university data or documents containing Social Security Numbers (SSNs).

BACKGROUND

Using the SSN as an identifier makes its use vulnerable to misuse, including identity theft.

POLICY STATEMENT

The University of Central Florida is committed to ensuring the privacy of confidential information it collects and maintains on students, employees, and others. Social Security Numbers are sensitive data that are required by many university business processes but whose misuse or inadvertent disclosure can pose privacy risks to individuals as well as compliance or reputational risks to the university. It is the policy of UCF to request and use SSNs only as required for the performance of the university's duties and responsibilities and to secure this information from inappropriate release or disclosure.

Violation of this policy may result in immediate loss of network and computer access privileges, seizure of equipment, loss of research laboratory access, or removal of inappropriate information posted on university-owned computers or university-supported

Internet sites. In addition to these corrective actions, failure to comply with this policy may result in disciplinary action up to and including termination.

DEFINITIONS

FERPA. The Family Educational Rights and Privacy Act of 1974, also known as the Buckley Amendment. FERPA is a federal law that protects the privacy of student academic records.

NID – Network Identification Number. A UCF-issued identifier used by university employees and students to access enterprise computer systems and applications. NIDs are classified as restricted data.

Personally Identifiable Information (PII). Information from which an individual may be uniquely and reliably identified or contacted.

Pseudo Social Security Number. A unique nine-digit numerical personal identifier assigned by the University of Central Florida to foreign nationals and other individuals who do not have an SSN in order to include those individuals in university business processes that require use of the SSN.

Social Security Number. A unique nine-digit numerical personal identifier assigned by the federal Social Security Administration. The SSN is regarded as highly restricted data, as described in university policy 4-008-1, *Data Classification and Protection*.

UCFID – Employee Identification Number. A unique seven-digit numerical identifier assigned to the record of all university personnel in the university's PeopleSoft business system. The UCFID, when used in accordance with university policy 4-008.1, *Data Classification and Protection*, is regarded as unrestricted data.

PROCEDURES

A. Collection of SSNs

1. Florida Statute 119.071(5) requires that the university, as an agency, may not collect SSNs unless the university has stated in writing the purpose for such collection and further requires that:
 - a. agencies must provide a copy of the written statement to each individual whose SSN is collected;
 - b. agencies may not use SSNs for purposes other than those for which they were collected; and
 - c. collection of the SSN is imperative for the performance of the agency's duties and responsibilities as prescribed by law.
2. When requesting a SSN from an individual, the federal Privacy Act of 1974 requires that any federal, state, or local agency:

- a. tell the individual whether disclosing the SSN is mandatory or voluntary;
 - b. state the statutory or other authority under which the request is being made; and
 - c. state what uses it will make of the individual's SSN.
3. SSNs may not be collected for use as a personal identification number. For purposes of UCF identification, the UCFID should be used.

B. Use of SSNs

1. No part of an SSN may be displayed or distributed electronically via email, whether in the body of the email message or in an attachment, unless encryption is used along with a strong password to protect the SSN. The password must be communicated separately from the email message itself (e.g., via phone call or texting, etc.)
2. Public display of partial SSNs is not acceptable because of the ease with which the missing digits can be obtained from various sources.
3. Only those individuals with a need to know are authorized to access student or employee SSNs. Prior to accessing SSNs, these individual should receive appropriate information security training from the Information Security Office and have signed the university's confidentiality statement.
4. Documents containing student or employee SSNs may not be distributed to or viewed by unauthorized individuals. Such documents should be stored only in secured rooms inside locked cabinets. In high-traffic areas, such documents should not be left on desks or other visible areas.
5. SSNs may be contained in historical university records and documents that cannot be altered. Such records should be considered highly restricted information and stored and handled accordingly.
6. UCF employees are authorized to release SSNs to third parties only as allowed by law, when authorization is granted in writing by the individual, or when the Office of the General Counsel has approved the release and after a security review has been performed on the third party according to UCF policy 4-014. An example would be release of student SSNs to the National Student Loan Clearinghouse.

RELATED DOCUMENTS

UCF Policy 4-008.1 *Data Classification and Protection*

<https://policies.ucf.edu/>

UCF Policy 4-007.1 *Security of Mobile Computing, Data Storage, and Communication Devices*

<https://policies.ucf.edu/>

UCF Policy 2-100.5 *Florida Public Records Act–Scope and Compliance*

<https://policies.ucf.edu/>

UCF Policy 4-014 *Procurement and Use of Cloud Computing and Data Storage Services*
<https://policies.ucf.edu/>

UCF Human Resources Confidentiality Agreement
<http://hr.ucf.edu/files/ConfidentialityAgreement.pdf>

UCF statement on the collection and use of Social Security Numbers
<http://generalcounsel.ucf.edu/files/2016/01/Notice-of-SSN-Usage-Updated-Jan15-FINAL1.docx>

INITIATING AUTHORITY Vice President for Information Technologies and Resources

POLICY APPROVAL (For use by the Office of the President)	
Policy Number: 4-012.1	
Initiating Authority: <u>Joel L. Nachman</u>	Date: <u>11-30-18</u>
University Policies and Procedures Committee Chair: <u>[Signature]</u>	Date: <u>11/19/18</u>
President or Designee: <u>[Signature]</u>	Date: <u>12-5-18</u>