Social Security Number (SSN) Protection Policy

I. Purpose

The University of South Alabama (USA) collects social security numbers (SSNs) in the process of performing activities for the expressed purpose of supporting the University's mission. An individual's SSN is private and confidential, and every effort must be made to prohibit disclosure and/or improper usage. The purpose of this policy is to limit access to SSNs stored in USA's files and databases to persons who require them in order to perform their jobs.

II. Scope

This policy applies to all persons with access to any official University records.

III. Policy

The SSN shall not be requested on forms (electronic or paper) except as administered by those offices whose responsibilities require them to obtain SSNs for essential business purposes, including interaction with external agencies for which the SSN is the primary identifier. No reference to a SSN will be on any forms when such forms can use the USA assigned identification number (Jag #).

Once a person has a USA assigned Jag #, that number will be used as the unique identifier for internal records and among USA information systems.

Active measures will be taken to identify and secure, remove and/or destroy documents that contain SSNs. If records cannot be destroyed in compliance with The Records Disposition Authority Policy then, when possible, the SSNs will be masked.

All University systems/servers hosting files which contain SSNs must be maintained and operated by the Computer Services Center (CSC).

Each department will assign a Data Custodian who will assist and determine the electronic files/records to be destroyed that contain SSNs. If the file cannot be destroyed, then arrangements must be made to move the file to a CSC file server.

Storage of physical documents that contain SSNs must be approved by the Director of Information Security.

When possible, forms and documents that are being scanned for permanent storage will have the SSN masked prior to scanning, and will not be indexed by SSN (this excludes records of students who attended USA prior to conversion to the Banner Student System. SSNs are the only unique student identifiers for these records and must be used).

Access to screens or forms containing SSNs will be restricted to those individuals with an official need to access the SSNs.

Electronic files containing SSNs shall not be stored on desktops, laptops, departmental servers, cloud services, portable media devices, or stored in email without explicit written permission from the Director of Information Security. The files containing SSNs approved for local storage must be encrypted; all unapproved files must be deleted

Any accidental disclosure or suspected misuse of SSNs must be reported immediately to the Director of Information Security, infosec@southalabama.edu, or at 460-6161.

IV. Enforcement

Deliberate violation of this policy is subject to disciplinary action including the individual's use of information technology resources (such as suspension or termination of access, or removal of online material); the individual's employment (up to and including immediate termination of employment in accordance with applicable University policy); the individual's studies within the University (such as student discipline in accordance with applicable University policy); civil or criminal liability; or any combination of these, up to and including dismissal.

V. Exclusions

Electronic records created when the SSN was the official University identifier and that have not been converted to non-SSN indexed ID, may continue to be indexed by SSN, but access to these records must be approved by the Director Information Security. Such access shall be restricted to those individuals with an official need to access the record.

Research projects, grant work, and contract work must follow the IRB, state, federal, and/or client laws or guidelines governing that work.

VI. Effective Date

June 5, 2017