Social Security Number (SSN) Protection Policy

I. POLICY STATEMENT

Auburn University 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 Auburn University's files and databases to persons who require them in order to perform their jobs.

II. POLICY PRINCIPLES

1. The SSN will only be requested on forms (electronic or paper) administered by those offices whose responsibilities require them to obtain SSNs, to interact with and respond to external agencies (e.g., IRS, ACT testing, Federal Aid Programs, NCAA, Healthcare Enrollment, Voluntary Retirement Plans, RSA retirement applications, etc.) for which the SSN is the primary identifier. No reference to a SSN will be on any forms when such forms can use either the Auburn University assigned identification number or username.

2. Once a person has an Auburn University assigned identification number, that number or their username will be used as the unique identifier for internal records and among Auburn University information systems.

3. Active measures will be taken to remove and destroy documents that contain SSNs. If records cannot be destroyed in compliance with the AU Record Retention Policy, then, when possible, the SSNs will be masked.

4. Storage of physical documents that contain SSNs must be approved by the Auburn University Office of Audit, Compliance & Privacy.

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

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

7. All systems/servers hosting files which contain SSNs must be housed in a secure physical location and operated only by authorized personnel as approved by the Office of the CIO.

8. Electronic files containing SSNs may not be stored on desktops, laptops, non-secure departmental servers, cloud services, portable media devices, or stored in email. Servers/systems which meet the Confidential Data/Server Security Standards may host SSNs upon approval by the Office of the CIO.

9. If SSNs must be stored locally, the storage device must be encrypted.

10. Any accidental disclosure or suspected misuse of SSNs must be reported immediately to the University Information Security Officer, abuse@auburn.edu, or at 844-0888.

III. EFFECTIVE DATE

January 11, 2017

IV. APPLICABILITY

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

V. POLICY MANAGEMENT

Responsible Office: Office of the Chief Information Officer

Responsible Executive: Executive Vice President and Provost

Responsible Officer: Chief Information Officer

VI. DEFINITIONS

Form: Any document, written or electronic, that a user is asked to complete.

SSN Masking: Consistent with IRS regulations, SSN masking allows organizations to display the last 4 digits of a social security number and to mask the remaining portion with either an asterisk (*) or the letter X.

Data Masking: Data masking is a method of creating a structurally similar but inauthentic version of an organization's data that can be used for purposes such as software testing and user training. The purpose is to protect the actual data while having a functional substitute for occasions when the real data is not required.

Data Obfuscating: Data obfuscation (DO) is a form of data masking where data is purposely scrambled to prevent unauthorized access to sensitive materials. This form of encryption results in unintelligible or confusing data. DO is also known as data scrambling and privacy preservation.

Encryption: Encryption is the conversion of electronic data into another form, called cipher text, which cannot be easily understood by anyone except authorized parties.

VII. POLICY PROCEDURES

- Within one month of the approval of this policy, all offices shall cease to collect SSNs except as allowed in Section II.1., *supra.*
- Within one month of the approval of this policy, all users of desktops and laptops shall either delete or encrypt SSNs as required in Section II.8., *supra.*
- Within five months of the approval of this policy, all areas must have made a good faith effort to purge SSNs from all records under their control and shall continue the effort until the objective is reached.

- If deadlines cannot be met, the Dean, Director, or Department Head must contact the Office of the CIO (University Information Security Office) in writing to describe the barriers, request assistance if needed, and offer an alternative deadline.
- Removal of SSNs from departmental records may be subject to review by the Office of Audit, Compliance & Privacy.
- Departments should perform and document their own reviews on a regular basis.

VIII. SANCTIONS

Deliberate violation of this policy will be considered a Group I infraction under the Auburn University Personnel Policies and Procedures Manual and is subject to disciplinary action, up to and including dismissal.

IX. 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 Office of the Chief Information Officer. 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.

X. INTERPRETATION

The Auburn University Chief Information Officer has the authority to interpret this policy.