Sensitive Personally Identifying Information Protection Policy

I. POLICY STATEMENT

Auburn University collects Sensitive Personally Identifying Information (S-PII) in the process of performing activities for the expressed purpose of supporting the University's mission. An individual's S-PII 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 S-PIIs stored in Auburn University's files and databases to persons who require them in order to perform their jobs.

II. POLICY PRINCIPLES

1. S-PII will only be requested on forms (electronic or paper) administered by those offices whose responsibilities require them to obtain S-PIIs, 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 S-PII is the primary identifier. No reference to an S-PII 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 S-PII. If records cannot be destroyed in compliance with the AU Record Retention Policy, then, when possible, the S-PII will be masked.

4. Storage of physical documents that contain S-PII 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 S-PII masked out prior to scanning, and will not be indexed by S-PII (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 S-PII will be restricted to those individuals with an official need to access the S-PIIs.

7. All systems/servers hosting files which contain S-PII 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 S-PII 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 S-PIIs upon approval by the Office of the CIO.

9. If S-PII must be stored locally, the storage device must be encrypted.

10. For the purpose of this policy Banner ID is not considered S-PII.

11. Any accidental disclosure or suspected misuse of S-PII must be reported immediately to the Chief Information Security Officer, abuse@auburn.edu, or at 844-0888.

III. EFFECTIVE DATE

January 11, 2017
Revised: January 30, 2019

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*:** Chief Operations Officer

***Responsible Officer*:** VP & Chief Information Officer

VI. DEFINITIONS

Sensitive Personally Identifying Information: (Alabama Breach Notification Law) A first name/initial and last name in combination with one or more of the following:

1. A non-truncated Social Security number or tax identification numbers
2. A non-truncated driver's license number, state-issued identification card number, passport number, military identification number, or other unique identification issued on a government document used to verify the identity of a specific person.
3. A financial account number, including a bank account number, credit card number, or debit card number, in combination with any security code, access code, password, expiration date, or PIN, that is necessary to access the financial account or to conduct a transaction that will credit or debit the financial account.
4. Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.
5. An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.
6. A user name or email address, in combination with a password or security question and answer that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information.

The term does not include either of the following:

1. Information about an individual which has been **lawfully made public** by a federal, state, or local government record or a widely distributed media.
2. Information that is truncated, encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable, **including encryption of the data**, document, or device containing the sensitive personally identifying information, unless the covered entity knows or has reason to know that the encryption key or security

credential that could render the personally identifying information readable or useable has been breached together with the information.

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 S-PIIs except as allowed in Section II.1., *supra*.
- Within six months of the approval of this policy revision, all users of desktops and laptops shall either delete or encrypt S-PIIs as required in Section II.8., *supra*.
- Within six months of the approval of this policy, all areas must have made a good faith effort to purge S-PIIs 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 S-PIIs 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.