Auburn University at Montgomery
Policies and Procedures

Title: Social Security Number (SSN) Protection Policy

Responsible Office: Office of Information Technology Services

I. PURPOSE

At times, Auburn University Montgomery collects the SSNs of employees and students 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 students' and employees' SSNs stored in Auburn University Montgomery's files and databases to persons who require them in order to perform their jobs.

II. POLICY

1. The SSN will only be requested on forms administered by those offices whose responsibilities require them to obtain SSNs to interact with and respond to external agencies (ex. IRS, ACT testing, Federal Aid Programs, NAIA, etc.) for which the SSN is the primary identifier. No reference to a SSN will be on any non-Banner forms, such as Leave Slips, Travel Vouchers, etc. The SSN field will be removed from all non-Banner forms, and may be replaced by either the UserName or Banner ID.
2. Access to the SSNs of Auburn University Montgomery applicants for admission, students, and employees is limited to those persons who require that information in order to communicate with external agencies for which the SSN is the primary identifier.
3. Once a person has a Banner ID number, that number or the UserName will be used as the unique identifier for internal records and among Auburn University Montgomery information systems.
4. Active measures will be taken to remove and destroy documents that contain SSNs. If records cannot be destroyed in compliance with the AUM Record Retention Policy, then the SSNs will be masked.
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 AUM prior to conversion to the Banner Student System. SSN is the only unique student identifier 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 SSN.
7. All servers hosting files which contain the SSN must be housed in a secure location and operated only by authorized personnel.
8. Electronic files containing SSNs may not be stored on personal desktops, laptops, departmental servers, removable data storage devices (i.e., flash drives, floppy discs, cds, etc.), or AUM Office servers, except those AUM Office servers that are password protected. In the few cases where SSNs must be stored locally, they must be encrypted. Such cases must be approved by the office of Information Technology Services. (Desktops and laptops tend to reside in less secure locations than central servers and departmental servers, and AUM Office servers may be housed in secure locations but are generally mapped drives on desktops and laptops).

9. Any accidental disclosure or suspected misuse of SSNs must be reported immediately to the Chief Information Officer (CIO).

III. EFFECTIVE DATE

Immediately upon approval of this policy

IV. APPLICABILITY

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

V. RESPONSIBILITY

Areas with responsibility for handling employee and student records. Internal Auditing will include a review of SSN Protection Policy compliance to general departmental audits.

VI. DEFINITIONS

N/A

VII. PROCEDURES

- Within one month of the approval of this policy, all offices shall cease to collect SSNs except as allowed in II.1 above.
- Within one month of the approval of this policy, all users of desktops and laptops shall either delete or encrypt SSNs as required in II.8 above.
- 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 CIO in writing to describe the barriers, request assistance if needed, and offer an alternate deadline.
- Removal of SSN's from departmental records will be subject to review by Internal Auditing.
- 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 Montgomery 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 ID 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 Information Technology Services. Such access shall be restricted to those individuals with an official need to access the SSN.

This policy applies only to records of students and employees of Auburn Montgomery. 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 CIO in consultation with Senior Staff and/or the Dean's Council.

APPROVAL TO PROCEED: ______________________________ DATE: ___________