LOYOLA
UNIVERSITY MARYLAND

Information Security Policy Addendum: Social Security Numbers

This addendum to the Information Security Policy contains additional requirements and responsibilities pertaining to social security number (SSN) data beyond those requirements and responsibilities described in the Security Policy.

The collection and retention of Social Security Number information (SSN data) is required by federal and state agencies and laws. Given the sensitivity of this national identifier, Loyola University Maryland is committed to protecting SSN data from unauthorized use or unnecessary disclosure. Therefore, it is the policy of Loyola to implement and maintain reasonable security procedures and practices to protect SSN data from unauthorized access, use, and disclosure.

In order to support sound University-wide information security practices, compliance with various State and Federal legislation, and with various industry standards and best practices, this addendum to the *Information Security Policy* ("Security Policy") applies to all organizations within the University, and to all authorized users of University information resources. Instances of non-compliance must be reported to the Office of the CIO and reviewed with the Administrative Core Technology Committee or the appropriate Data Steward to determine steps needed to meet compliance guidelines.

I. PURPOSE

While student records, including the SSN data, are protected by the Family Educational Rights and Privacy Act (FERPA) and other laws, and by the University Information Security Policy and other policies, a policy addendum is needed to provide additional requirements and responsibilities specific to SSN data.

II. SCOPE

1) This addendum covers SSN data collected, retained, processed, or distributed by the University, whether electronically or non-electronically, and all computer systems or any subsidiary systems that contain or process SSN data, which are owned or in the custody of the University, regardless of physical location.

2) This addendum also applies to, but is not limited to, all faculty, staff, administrators, students, alumni, consultants, and any person or agency employed or contracted by the University or any of its auxiliary organizations, who have an authorized need to access restricted or sensitive University information.

3) This addendum applies regardless of whether the computer systems used in conjunction with University information resources are owned or controlled by the University or by some other party, including users' personally-owned computer systems, and regardless of physical location.

III. DEFINITIONS

Terms in this policy addendum are used as they are defined in the Security Policy.

IV. POLICY

A. USE OF SSN DATA

1) Prior to the creation of a unique Loyola ID number for an individual, the individual's SSN may be used as a unique identifier.

2) Once a unique Loyola ID number has been created for an individual, the University shall no longer use SSN data as the primary identifier for that individual in University information systems.

3) No new information systems will be purchased or developed by Loyola that use SSN data as a primary key in databases or as a user login, except where required by law.

4) New information systems purchased or developed by Loyola will only use SSN data as data elements where required by law or business necessity.

B. ACCESS TO AND DISTRIBUTION OF SSN DATA

1) Only employees determined by their supervisors to require access to SSN data based upon job duties are authorized to access this information.

2) Loyola may release SSN data to third parties as allowed or required by law, when authorization is granted by the individual, or when the authorized third party is acting as Loyola's agent after appropriate security is guaranteed.

C. DISPLAY OF SSN DATA

When being displayed electronically or printed, the first five digits of any SSN shall be masked except where the display or printout of the full SSN is required for business or legal purposes. This applies to the display of SSN data in all University information systems and records, including those managed by third parties.

D. RETENTION OF SSN DATA

SSN data is included in certain archived databases, files, paper records, and imaged documents, which act as historical records and cannot be altered because of legal or business requirements. Any such records that include SSN data will be treated as restricted data as described in the Security Policy.

V. PENALITIES AND ENFORCEMENT

As described in the Security Policy.

VI. EFFECTIVE DATE, REVIEW AND REVISION OF POLICY

This policy addendum will be effective as of the date of signature by the approving authority, and will be subject to review and revision at least yearly and as updates are needed. In cases where immediate compliance with this policy is not reasonably feasible, a detailed plan must be developed for becoming compliant, and that compliance plan must be registered with and approved by the ISO and the TSAC ISS.

VII. APPROVALS:

Reviewed and approved by the Technology Services Advisory Committee

Reviewer Name and Title: **Louise Finn, Chief Information Officer**

Reviewer Signature: ***Louise Finn***

Date: **12-15-2011**

Reviewed and approved by the Loyola Conference

Final Approval Name and Title: Brian Linnane, S.J., President

Final Approval Signature: ***Brian Linnane, S.J.***

Date: **12-20-2011**