



Personal Information Protection (PIP) Policy

Title: Loyola Protected Data & Loyola Sensitive Data Identification Policy

Approved: March 4, 2008

Author: Personal Information Risk Group (PIRG)

Version: 1.0

Scope

This policy covers all computers and electronic devices capable of storing or transmitting electronic data that are owned or leased by Loyola University Chicago, consultants or agents of Loyola University Chicago and any parties who are contractually bound to handle data produced by Loyola.

Purpose

The purpose of this policy is to ensure that Loyola Protected or Loyola Sensitive data is not inappropriately stored on Loyola computers and electronic devices through systematic electronic examination.

Policy

Frequency

All departments will perform a Personal Information Security Compliance (PISC) Review at least every 6 months. Departments are free to perform PISC Reviews more frequently if they see a need to do so. All departments must maintain a schedule for performing their PISC Reviews.

Covered Systems

During a PISC Review, departments are responsible for scanning workstations, laptops, portable devices, and any servers that are managed by the department. Portable devices that store electronic data should be attached to a computer during the PISC Review. ITS will perform PISC Reviews for all servers that they manage.

Collection Method & Methodology

Scan results shall be stored on each machine that is scanned. The primary data steward or the alternate data steward in each department will be responsible for examining each scan result to determine if the machine or device houses Loyola Protected or Loyola Sensitive data.

Measurement & Reporting

The primary data steward or the alternate data steward in each department will create and send a summary of their scan results to ITS. This summary of scan results will include the number of computers and electronic devices that contain either Loyola Protected data or Loyola Sensitive data, and the number that

contain neither. Scan results will also include any machines which were believed to not contain Loyola Protected data or Loyola Sensitive data but were found to contain either data type. ITS will create and provide a summary report to the Information Technology Executive Steering Committee.

Follow-up & Training

Any users who regularly use a computer or electronic device identified by a scan as inappropriately containing Loyola Protected data or Loyola Sensitive data without proper authorization may be required to complete online training on the use and storage of Loyola Protected data and Loyola Sensitive data.

Software

ITS will install software that is capable of scanning for Loyola Protected data and Loyola Sensitive data on all Loyola computers and electronic devices subject to this Policy. Only software approved by ITS to scan for and identify Loyola Protected data and Loyola Sensitive data may be used during a PISC review.

Search Terms

The scanning software will search for the patterns that are specified in the Appendix. If additional patterns are identified that need to be identified, they will be added to the Appendix.

Questions about this policy

If you have questions about this policy, please contact the Information Security team at DataSecurity@luc.edu.

Policy adherence

Failure to follow this policy can result in disciplinary action as provided in the Staff Handbook, Student Worker Employment Guide, and Faculty Handbook. Disciplinary action for not following this policy may include termination, as provided in the applicable handbook or employment guide.

Appendix

Policies referenced

PIP policy – Data Classification policy

PIP policy – Personal Information Protection Compliance Review Protocol

Definitions

Personal Information Security Compliance (PISC) Review – Occurs when a department follows the Personal Information Security Compliance Review Protocol.

Regular expression – A pattern, such as 9 consecutive digits or 3 consecutive digits then 2 consecutive characters. Any item which matches the regular expression will be flagged by the scanning software.

Search Terms

The following regular expressions will be flagged by the scanning software as possible matches for sensitive data:

- SSN9 – 9 consecutive digits
- SSN324 – 3 consecutive digits, a dash, 2 consecutive digits, a dash, and 4 consecutive digits
- AMEX – 4 consecutive digits, a dash, 6 consecutive digits, a dash, and 5 consecutive digits
- VMCD – 4 consecutive digits, a dash, 4 consecutive digits, a dash, 4 consecutive digits, a dash, and 4 consecutive digits