Protected-Sensitive Data Identification Policy

Policy Title:
Protected-Sensitive Data Identification Policy

Responsible Executive(s):
Jim Pardonek, Director and Chief Information Security Officer

Responsible Office(s):
University Information Security Officer (UISO)

Contact(s):
If you have questions about this policy, please contact the University Information Security Office.

I. Policy Statement

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. This policy ensures that Loyola Protected or Loyola Sensitive data is not inappropriately stored on Loyola computers and electronic devices through systematic electronic examination.

II. Definitions

Not applicable.

III. 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 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.

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

Jim Pardonek, Director and Chief Information Security Officer	Enforcing the Policy at the University by setting the necessary requirements.

VI. Related Policies

Please see below for additional related policies:

- Security Policy

Approval Authority:	ITESC	**Approval Date:**	March 4th, 2008
Review Authority:	Jim Pardonek	**Review Date:**	March 7th, 2024
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu