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 agent2 II. Definitions

III. Policy

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.

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.

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.

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.

Any users who reg04(u) molho (l)t2gbr aAAAAAAAAAAAAAASMD 4( )0(d[(AAc).)]T0Trgy L4(e)1(4(y)4(m)6 (oe)1(

- Security Policy