Personal Information Protection Compliance Review Policy

Policy Title:
Personal Information Protection Compliance Review Policy

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

Responsible Office(s):
University Information Security Office

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

I. Policy Statement

The Personal Information Protection Compliance Review Policy covers all users of computers, electronic devices, and media capable of storing Loyola Protected data or Loyola Sensitive data as defined by the Data Classification Policy.

The purpose of this policy is to ensure that all divisions and departments of Loyola University Chicago are in, and remain in, compliance with the policies established for the security of Loyola Protected data or Loyola Sensitive data.

II. Definitions

Primary data steward: The person responsible for the security of information within their division. This will be the same person who is responsible for ensuring the department performs the necessary scans as defined in Loyola Protected Data & Loyola Sensitive Data Identification Policy.

III. Policy

Each division will conduct compliance reviews in accordance with the Loyola Protected Data & Loyola Sensitive Data Identification Policy.

Each division or department head will designate one individual as the department's primary data steward and one individual as the department's alternate data steward. If the primary data steward is unable to perform their listed duties, the alternate data steward will perform those duties. The duties of the two data stewards cannot be delegated further. Each division or department will communicate the names of the designated data stewards to ITS. The primary data steward has primary responsibility for the security of information within their division. This will be the same person who is responsible for ensuring the department performs the necessary scans as defined in Loyola Protected Data & Loyola Sensitive Data Identification Policy. The role of the designated individual may be rotated. The alternate data steward will assist the primary data steward and perform the functions of the primary data steward if the primary data steward is unavailable to do so.

The primary data steward will be responsible for conducting the review of his/her department or division, reviewing scan results, ensuring compliance with all policies listed in the appendix in the Applicable Policies Covered section, confirming that all devices covered by the Loyola Protected Data & Loyola Sensitive Data Identification Policy were scanned, and certifying on the certification form shown in the appendix that their office meets the identified security standards.

ITS and HR will train the data stewards on information security policies. Each department shall provide additional training to their data stewards on the local, state and federal regulations or standards on information security that apply to their department. The primary data steward will be responsible to make certain that all staff members, department heads, student workers in, and outside parties used by, their department are fully aware of Loyola University Chicago's information security policies. They will arrange special training as needed by contacting subject matter experts listed in the appendix.

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

Jim Pardonek, Associate 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
- Encryption Policy
- Data Classification 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