



Personal Information Protection (PIP) Policy

Title: Personal Information Protection Compliance Review Protocol

Approved: March 4, 2008

Author: Personal Information Risk Group (PIRG)

Version: 1.0

Scope

The Personal Information Protection Compliance Review Protocol 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

Purpose

The purpose of this protocol 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.

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.

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

Subject Matter Experts

LOCUS – Nick Jones, Provost's Office – njones2@luc.edu

FERPA – Eric Pittenger, Registration and Records – ferpa@luc.edu

Data Protection technology – Joe Bazeley, ITS – security@luc.edu

Applicable Policies Covered

PIP Policy – Data Classification Policy

PIP Policy – Physical Security of Loyola Protected Data & Loyola Sensitive Data

PIP Policy – Electronic Security of Loyola Protected Data & Loyola Sensitive Data

PIP Policy – Loyola Protected Data & Loyola Sensitive Data Identification

PIP Policy – Disposal of Loyola Protected Data & Loyola Sensitive Data

PIP Policy – Loyola Encryption Policy

PIP Policy – Data Breach Response Policy

Definitions

Primary data steward – The person who 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.

Alternate data steward – The person who 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.

DATA SECURITY COMPLIANCE REVIEW

I, _____, the designated data steward for
(department) _____, certify that, to the best
of my ability and knowledge, our data systems and staff usage of data for the time period
_____ are in compliance with Loyola University

Chicago's Personal Information Security policies as indicated:

- All Loyola Protected data or Loyola Sensitive data encrypted in accordance with the Loyola Encryption Policy
- Loyola University Chicago approved programs and data are stored and used in accordance with the Loyola Encryption Policy and the Electronic Security of Loyola Protected Data/Loyola Sensitive Data Policy
- Staff members are accessing only such Loyola Protected data or Loyola Sensitive data as are needed to complete their assigned or authorized tasks and are communicating such information only to other parties authorized to have access to such information
- All staff members have been trained and/or retrained in the State, local or federal rules governing the Loyola Protected data produced, collected or used in this office
- Access Control policy at <http://www.luc.edu/safety/keypolicy.shtml> is followed
- Password standards at http://www.luc.edu/its/security_passwords.shtml are followed
- Disposal of Loyola Protected Data & Loyola Sensitive Data Policy is followed
- Printer and Fax in secure a limited access area if required by the Physical Security of Loyola Protected Data/Loyola Sensitive Data Policy
- Scan of all electronic data devices for Loyola Protected data or Loyola Sensitive data is performed every 6 months
- Scan summary for Loyola Protected data or Loyola Sensitive data sent to ITS (attach this Compliance Review certification)
- Where a clean desk policy is present, it is adhered to
- All members of the department completed Individual Compliance Review forms for this time period
- All vendors who handle Loyola Protected data or Loyola Sensitive data on behalf of the department have confirmed that they follow all applicable Loyola Personal Information Security policies
- Any contracts signed since the last Personal Information Security Compliance Review included language that the Vendor follow Loyola's Personal Information Security policies

Areas of concern or goals for improvement and timeline to implement improvements:

Signed by: _____ Date: _____