



Personal Information Protection (PIP) Policy

Title: Encryption Policy

Approved: March 4, 2008

Author: Personal Information Risk Group (PIRG)

Version: 1.0

Scope

This policy covers all computers, electronic devices, and media capable of storing electronic data that house Loyola Protected data or Loyola Sensitive data as defined by the Data Classification Policy. This policy also covers the circumstances under which encryption must be used when data is being transferred.

Purpose

The purpose of this policy is to establish the types of devices and media that need to be encrypted, when encryption must be used, and the minimum standards of the software used for encryption.

Policy

Devices and Media Requiring Encryption

Encryption is required for all laptops, workstations, and portable drives that may be used to store or access Loyola Protected data. Encryption is recommended for all laptops, workstations, and portable drives that may be used to store or access Loyola Sensitive data. ITS will provide, install, configure, and support encryption where it is needed. Departments who have a laptop, workstation, or portable drive that needs to be encrypted should contact the ITS Information Security team at DataSecurity@luc.edu.

Electronic Data Transfers

Any transfer of unencrypted Loyola Protected data or Loyola Sensitive data must take place via an encrypted channel. Encrypted Loyola Protected data or Loyola Sensitive data may be transmitted via encrypted or unencrypted channels. All email communications that involve email addresses outside of Loyola use an unencrypted channel, and therefore require that messages containing Loyola Protected data or Loyola Sensitive data be encrypted. Approved methods of encrypting electronic data transfers are listed in the appendix. If the encryption method includes a password, that password must be transferred through an alternative method, such as calling the individual and leaving the password on their voice mail. Email messages containing encrypted data may never include the password in the same message as the encrypted data. Individuals who are unsure if they are correctly encrypting electronic data transfers should contact the ITS Information Security team at DataSecurity@luc.edu.

Physical Transfer of Electronic Data

Any time Loyola Protected data or Loyola Sensitive data is placed on a medium such as a CD, DVD, or portable drive to facilitate a physical transfer, either entirely within Loyola or between Loyola and a 3rd party, that data must be encrypted. Archiving Loyola Protected data or Loyola Sensitive data to a physical medium is not recommended, but is permitted if the data is encrypted. All archiving should be done electronically, so that it is stored in a controlled data center and backed up by ITS.

Software

ITS will install software that is capable of encrypting the entire hard drive on all identified Loyola computers and electronic devices subject to this Policy. Users who require encryption software should contact ITS to arrange installation of encryption software.

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

Examples of portable drives

1. Flash drives
2. Thumb drives
3. Memory sticks
4. USB hard drives
5. iPods

ITS will make the following approved encryption methods available for electronic data transfers

1. Transport Layer Security (TLS) / Secure Socket Layer (SSL)
2. SSH File Transport Protocol (SFTP)
3. Connecting via an ITS-approved Virtual Private Network (VPN)

Methods for encrypting email

The approved method of encrypting email is outlined at http://www.luc.edu/its/encrypt_email.shtml. If you have any questions about the process, please contact the Information Security team at DataSecurity@luc.edu.

Other policies referenced by this policy

PIP policy – Data Classification Policy