Encryption Policy

Policy Title:
Encryption Policy

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

Responsible Office(s):
University Information Security Officer

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

I. Policy Statement

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.

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.

II. Definitions

Not applicable.

III. 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.

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, so messages containing Loyola Protected data or Loyola Sensitive data are 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.

Cardholder Data Transfers (PCI-DSS)

All transmissions of credit card data must use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, ensuring that, only trusted keys and certificates are accepted, the protocol in use only supports secure versions or configurations, and the encryption strength is appropriate for the encryption methodology in use.

Physical Transfer of Electronic Data

Any time Loyola Protected data or Loyola Sensitive data is placed on portable medium 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 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.

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

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
- Data Classification Policy

Approval Authority:	ITESC	**Approval Date:**	March 4, 2008
Review Authority:	Jim Pardonek	**Review Date:**	July 16, 2024
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu