Encryption Policy

Policy Title:

Responsible Executive(s):

Responsible Office(s):

Contact(s):

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

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 (du)0]TJ4(y) d, (o)(a)the ssencr encrypte 1 (e)3 eyctronic data theful (o)(4da)e3 (y)de t.trta(v)(o)]TJ 0