Policies and Procedures Manual

Title: Data Encryption
Policy #: 1-0104
Prepared by: Information Security Task Force
Policy Administrator: Timothy Mines
Approved by: Information Security Task Force

Scope:
This policy covers all data encryption used by the College of the Holy Cross, its employees, student workers, consultants or agents during the course of College business.

Purpose:
The purpose of this policy is to identify the types of protection provided to specific data classifications and to provide guidelines for and examples of data encryption for each.

Data Classification:
All data protection covered by the Scope of this policy will be classified as Holy Cross Protected data, Holy Cross Sensitive data, or Holy Cross Public data. Please see Data Classification Policy #1-0101 for definitions of the data types. Data protection is based on the classification of data.

1.0 Data Encryption of Holy Cross Protected Data
Any electronic transmission of Holy Cross Protected data must be encrypted using security industry standards for strong encryption. Any Holy Cross Protected data stored on portable devices (laptops, CD-ROMS, flash drives, etc.) must be encrypted.

2.0 Data Encryption of Holy Cross Sensitive Data
Any electronic transmission of Holy Cross Sensitive data must be encrypted using security industry standards for strong encryption. Encryption is encouraged for Holy Cross Sensitive data stored on portable devices.

3.0 Data Encryption of Holy Cross Public Data
Holy Cross Public data need not be encrypted during transmission nor while at rest on a storage device.
**Frequency of Review:**

This policy will be reviewed annually.

**Policy Adherence:**

Failure to follow this policy can result in disciplinary action as provided in the Employee Handbook, Student Handbook, or Faculty Handbook, as appropriate.