HOLY CROSS

Policies and Procedures Manual

Title: **Data Retention and Storage**
Policy #: 1-0102
Prepared by: Information Security Task Force
Policy Administrator: General Counsel
Approved by: Information Security Task Force

Version: 1.0
Revised: 04/30/2010
Last Reviewed: 11/15/2013

Purpose:

This policy provides for data retention of College data to comply with federal and state law, ensure that data is retained for only the period necessary to conduct business, and ensure the continuity of business practices until authorized to dispose of or destroy the data in accordance with the data destruction policies and procedures.

In the event that a lawsuit, claim or administrative charge has been filed - or there exists a reasonable belief that a lawsuit, claim or charge will be filed - all relevant records, including e-mails, must be preserved and safeguarded until the litigation or proceeding has terminated and the time for all appeals has expired. With rare exception, all such documents may be subject to discovery in litigation and the destruction of such records potentially subjects the College and the individuals who take such action to court-ordered sanctions.

Policy:

1.0 Legal Requirement and Penalties

This Data Retention and Storage policy is intended to ensure the College's compliance with all applicable laws and regulations governing the retention of records. Federal and state laws and regulations require the College to maintain certain types of records for particular periods. Failure to maintain such records may subject the College and/or individuals to penalties and fines or may compromise the College's position in litigation.

2.0 Documents Covered by Policy

Records, documents, email and correspondence of all kinds must be managed according to the procedures outlined in this document. This policy applies to data in any form (including paper or electronic) however or by whomever created that belong to the College or were created by College employees, including faculty, as part of their work for the College or volunteers as part of their service to the College and are classified as Holy Cross *Protected* or Holy Cross *Sensitive* data as defined in the *Holy Cross Data Classification Policy and Procedure.*

3.0 Responsibilities

It is the responsibility of each Department to destroy the data that it originates or receives in accordance with this Data Destruction Policy.

Departments that maintain College data are responsible for establishing appropriate data management procedures and practices. Each department's administrative manager or a designee must:

- Be familiar with the College's data retention policy;
- Develop the department's and/or office's data management procedures and practices, consistent with this policy;
- Educate staff within the department in understanding sound data management practices;
- Restrict access to Holy Cross *Protected* and Holy Cross *Sensitive* data and information; and
- Coordinate the destruction of data as provided in the applicable procedures.

4.0 Data Security

In all cases, appropriate steps should be taken to provide sufficient physical and electronic security for Holy Cross *Protected* data. Those steps include securing paper data in locked file cabinets, or requiring limited and controlled password access to computerized data. In addition, an emergency back-up plan to reconstruct or salvage critical data, in the event of a disaster such as a fire, flood or computer malfunction should be in place. It is encouraged that physical and electronic security for Holy Cross *Sensitive* data include similar steps as described for *Protected* data, as determined by the departments with consultation from Data Security Coordinators.

Procedures:

Departments that maintain College documents should complete the following procedures for all data they retain, process or create.

1.0 Review Data to Verify Classification and Retention

Departments assigned the responsibility of maintaining College data should review the data and determine its classification according to the Data Classification Policy and properly set a schedule for retaining that data. The data retention schedule will be communicated to other departments that process, access, or maintain paper or electronic data. Data should not be retained beyond the period that it is needed for business processes or business continuity.

2.0 Review Data Access

Departments shall conduct reviews of the security afforded Holy Cross *Protected* and Holy Cross *Sensitive* data under the department's control to determine that it is safe from unauthorized access or accidental destruction. The College of the Holy Cross Security Policy and Procedure Framework defines procedures for password protection, password cycling and access controls for electronic data.

3.0 Prepare Data for Storage

Departments shall conduct reviews of data in all forms, separating them into appropriate storage media with the objectives of maintaining the data for the appropriate retention period and providing for ease of retrieval when needed. Proper logs should be kept to identify the data being stored and their respective retention periods. When the retention period is reached a review will be conducted to authorize destruction of the data. The Data Destruction Policy defines the proper destruction of data according to data classification. The College of the Holy Cross Security Policy and Procedure Framework defines procedures for backing up and restoring electronic data.

4.0 Securing Data

After conducting a review of departmental data to determine its classification in accordance with the Data Classification policy; data that is found to be Holy Cross *Protected* data will be secured based upon data form. Data that is electronic will be encrypted and access to the encryption keys will be limited to just those that need access to the information. The College of the Holy Cross Security Policy and Procedure Framework defines procedures for encrypting electronic data. Data that is paper will be placed in a locked filing cabinet in a limited access space. Access keys and combinations will be limited to just those that are authorized. It is encouraged that sensitive data be protected similarly to protected data, as determined by the Departments in consultation with the Data Security Coordinators.