HOLY CROSS

Policies and Procedures Manual

Title: **Written Information Security Plan**	Version: 1.3
Policy #: 1-0100	Revised: 3/2/2017
Prepared by: IT Policy & Security Committee	Last Review: 3/2/2017
Policy Administrator: General Counsel	
Approved by: IT Policy & Security Committee	

Purpose:

The purpose of the Plan is to:

(a) Ensure the security and confidentiality of personal information;

(b) Protect against any anticipated threats or hazards to the security or integrity of such information

(c) Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

Discussion:

Our objective, in the development and implementation of this comprehensive written information security plan ("Plan"), is to create effective administrative, technical and physical safeguards for the protection of personal information of Faculty, Staff, Students, Alumni and customers and residents of the Commonwealth of Massachusetts, and to comply with our obligations under 201 CMR 17.00. The Plan sets forth our procedure for evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information of residents of the Commonwealth of Massachusetts. For purposes of this Plan, "personal information" means a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Written Information Security Plan

In formulating and implementing the Plan, we will

- ❖ Identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information;
- ❖ Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;
- ❖ Evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks;
- ❖ Design and implement a plan that puts safeguards in place to minimize those risks, consistent with the requirements of 201 CMR 17.00; and
- ❖ Regularly monitor the effectiveness of those safeguards: The College data security program includes the policies, practices and procedures spelled out in latest version of The College of the Holy Cross Security Policy and Procedure Framework

1.0   DATA SECURITY MANAGER

We have designated the Information Security Officer as Data Security Manager to implement, supervise, and maintain the Plan. The Data Security Manager will be responsible for:

- ❖ Initial implementation of the Plan;
- ❖ Regular testing of the Plan's safeguards;
- ❖ Evaluating the ability of service providers to comply with 201 CMR 17.00 in the handling of personal information for which we are responsible, ensuring there are included in our contracts with those services providers provisions obligating them to comply with 201 CMR 17.00 in providing the contracted for services, and obtaining from such service providers written certification that such service provider has a written, comprehensive information security program that is in compliance with the provisions of 201 CMR 17.00.
- ❖ Reviewing the scope of the security measures in the Plan at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing personal information.
- ❖ Reporting any violations to the Office of Consumer Affairs and Business Regulation and to the Attorney General of the Commonwealth of Massachusetts.

2.0   DATA SECURITY COORDINATOR

The Chief Information Officer is designated as Data Security Coordinator and as such will coordinate with the Data Security Manager on:

- ❖ Protecting personal information collected as written or digital data college wide by ensuring all employees handling personal identification data are properly trained:

❖ Conducting an annual training session for all owners, managers, employees and independent contractors, including temporary and contract employees who have access to personal information on the elements of the Plan. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with the firm's requirements for ensuring the protection of personal information.

❖ Ensuring campus wide compliance with this policy and The College of the Holy Cross Security Policy and Procedure Framework.

3.0   INTERNAL RISKS

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately.

❖ A copy of the Plan must be made available to all employees.

❖ Annual re-training of employees will be offered on the detailed provisions of the Plan.

❖ The amount of personal information collected must be limited to that amount reasonably necessary to accomplish our legitimate business purposes, or necessary to us to comply with other state or federal regulations.

❖ Access to records containing personal information shall be limited to those persons who are reasonably required to know such information in order to accomplish your legitimate business purpose or to enable us comply with other state or federal regulations as detailed in The College of the Holy Cross Security Policy and Procedure Framework.

❖ Electronic access to user identification after multiple unsuccessful attempts to gain access must be blocked as detailed in The College of the Holy Cross Security Policy and Procedure Framework.

❖ All security measures shall be reviewed at least annually, or whenever there is a material change in our business practices that may reasonably implicate the security or integrity of records containing personal information. The Data Security Manager shall be responsible for this review and shall fully apprise management of the results of that review and any recommendations for improved security arising out of that review in accordance with The College of the Holy Cross Security Policy and Procedure Framework.

❖ Terminated employees must return all records containing personal information, in any form, that may at the time of such termination be in the former employee's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.)

❖ A terminated employee's physical and electronic access to personal information must be immediately blocked.

❖ Terminated employees shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the College's premises or information. Moreover, such terminated employee's remote

electronic access to personal information must be disabled; his/her voicemail access, e-mail access, Internet access, and passwords must be invalidated. Exceptions to this clause must be documented and approved by a Data Security Manager. The Data Security Manager shall maintain a highly secured master list of all lock combinations, passwords and keys.

❖ Current employees' user-ID's and passwords must be changed periodically in accordance with <u>The College of the Holy Cross Security Policy and Procedure Framework.</u>

❖ Access to personal information shall be restricted to active users and active user accounts only.

❖ Employees will be encouraged to report any suspicious or unauthorized use of customer information.

❖ Whenever there is an incident that requires notification under M.G.L. c. 93H, §3, there shall be an immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes in our security practices are required to improve the security of personal information for which we are responsible in accordance with <u>The College of the Holy Cross Security Policy and Procedure Framework.</u>.

❖ Employees are prohibited from keeping open files containing personal information on their desks when they are not at their desks.

❖ At the end of the workday, all files and other records containing personal information must be secured in a manner that is consistent with the Plan's rules for protecting the security of personal information and those detailed policies provided in the <u>The College of the Holy Cross Security Policy and Procedure Framework.</u>

❖ Each department shall develop rules (bearing in mind the business needs of that department) that ensure that reasonable restrictions upon physical access to records containing personal information are in place, including a written procedure that sets forth the manner in which physical access to such records in that department is to be restricted; and each department must store such records and data in locked facilities, secure storage areas or locked containers. These departmental policies can not remove or negate policies set forth by <u>The College of the Holy Cross Security Policy and Procedure Framework.</u>

❖ Access to electronically stored personal information shall be electronically limited to those employees having a unique log-in ID; and re-log-in shall be required when a computer has been inactive for more than a few minutes

❖ Emailing, instant messaging, or otherwise transferring protected data via unapproved messaging technologies is forbidden.

❖ Visitors' access must be restricted. Visitors shall not be permitted to visit unescorted any area within our premises that contains personal information.

❖ Paper or electronic records (including records stored on hard drives or other electronic media) containing personal information shall be disposed of only in a manner that complies with M.G.L. c. 93I.

4.0   EXTERNAL RISKS

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately:

- ❖ There must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information, installed on all systems processing personal information in accordance with the <u>The College of the Holy Cross Security Policy and Procedure Framework.</u>

- ❖ There must be reasonably up-to-date versions of system security agent software; which must include malware protection and reasonably up-to-date patches and virus definitions, installed on all systems processing personal information in accordance with polices and procedures detailed in <u>The College of the Holy Cross Security Policy and Procedure Framework</u>.

- ❖ To the extent technically feasible, all personal information stored on laptops or other portable devices must be encrypted, as must all records and files transmitted across public networks or wirelessly, to the extent technically feasible. Encryption here means the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further defined by regulation by the Office of Consumer Affairs and Business Regulation. Encryption of data and classifications of data are detailed in <u>The College of the Holy Cross Security Policy and Procedure Framework.</u>

- ❖ All computer systems must be monitored for unauthorized use of or access to personal information as detailed in <u>The College of the Holy Cross Security Policy and Procedure Framework.</u>

- ❖ There must be secure user authentication protocols in place, including:

- ❖ Protocols for control of user IDs and other identifiers;

- ❖ A reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;

- ❖ Control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;

- ❖ Restriction of access to active users and active user accounts only; and

- ❖ Blocking of access to user identification after multiple unsuccessful attempts to gain access.

- ❖ The secure access control measures in place must include assigning unique identifications plus passwords, which are not vendor-supplied default passwords, to each person with computer access to personal information.