WRITTEN INFORMATION SECURITY PROGRAM

Issuing Department:	Approved Date:	Effective Date:	Last Updated:
Information Technology	March 1, 2016	As of March 1, 2016	March 1, 2016

Program: PMC Written Information Security Program

1.0 Program Statement

The purpose of the Written Information Security Program ("Program" or "WISP") is to:

(a) Ensure the security and confidentiality of Personal Information ("PI") under 201 CMR 17.00; and

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

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

2.0 Administrative Oversight & Responsibility

The protection of PI owned or licensed by Pine Manor College (PMC) pursuant to the Program, and the general administration and implementation of the Program is overseen by the IT Governance Committee ("ITGC").

The ITGC is responsible for:

(a) Initial implementation of the Program;

(b) overseeing regular testing of the WISP safeguards;

(c) in consultation with the PMC academic or administrative departments, offices, and other business and operational units that generate or maintain records (each being a "Responsible Department") oversee the process of identifying PI, assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PI, evaluating the effectiveness of current safeguards, assigning appropriate access to identified PI and properly disposing of PI when no longer necessary to accomplish our legitimate business purposes, or necessary to us to comply with other state or federal regulations;

(d) evaluating the ability of service providers to comply with 201 CMR 17.00 in the handling of PI for which we are responsible, ensuring there are included in our contracts with those service 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;

(e) reviewing the scope of the security measures in the Program at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing PI;

(f) assure regular and appropriate training is provided to employees with access to PI; and

(g) monitor compliance with the Written Information Security Program and report any violations to the College's Chief Information Officer.

The Chief Information Officer shall act as employee, vendor and PMC affiliate liaison to the ITGC.

3.0 Objectives of Written Information Security Program

The objective of this Program is to create effective administrative, technical and physical safeguards for the protection of PI which is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. To fulfill PMC's obligations under MA 201 CMR 17.00, this Program sets forth PMC's procedure for evaluating its electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting such personal information.

For purposes of this Program, "personal information" or "PI" means a person'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 (including passport); 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 financial account; provided, however, that PI 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.

4.0 Written Information Security Program

4.1 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. To the extent that any of these measures require a phase-in period, such phase-in must begin immediately:

1. A copy of the Program must be distributed to each employee, student or temporary worker, independent contractor, vendor or PMC affiliate with access to PI who shall, upon receipt of the

Program, acknowledge in writing or electronically that he/she has received a copy of the Program.

2. Regular ongoing training and retraining of employees, student or temporary workers, independent contractors, vendors or PMC affiliates with access to PI will be offered by PMC.

3. Mandatory disciplinary actions will be taken for violation of security provisions of the Program (*The nature of the disciplinary action will be determined by the ITGC with Human Capital Management (HCM) and may depend on a number of factors including the nature of the violation and the nature of the personal information affected by the violation)*.

4. Regular evaluation of the ability of independent contractors, vendors or PMC's affiliates to comply with 201 CMR 17.00 in the handling of personal information for which the PMC is responsible, ensuring there are included in 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.

5. The amount of PI collected must be limited to that amount reasonably necessary to accomplish the PMC's legitimate educational and business purposes, or necessary to comply with other state or federal regulations.

6. Access to records containing PI shall be limited to those persons who are reasonably required to know such information in order to accomplish the PMC's legitimate educational and business purpose or to enable PMC to comply with other state or federal regulations.

7. When systems are available, electronic access to system and files with PI after multiple unsuccessful attempts to gain access shall be blocked.

8. All security measures shall be reviewed at least annually, or whenever there is a material change in the PMC's business practices that may reasonably implicate the security or integrity of records containing personal information. The ITGC shall be responsible for overseeing this review and shall consider for implementation recommendations for improved security arising out of that review.

9. A terminated employee, student or temporary worker, independent contractor, vendor or PMC affiliate with access to PI shall be required to return all records containing PI, in any form, which may at the time of such termination be in the person's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.)

10. Terminated employees, students temporary workers, independent contractors, vendors or PMC affiliates shall be immediately blocked from physical and electronic access to PI. Such terminated person shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to PMC's premises or information. Moreover, such terminated person's remote electronic access to PI shall be disabled and his/her voicemail access, email access, internet access, and passwords shall be invalidated. The CIO and Director

of Technology shall maintain a highly secured master list of all lock combinations, passwords and keys.

11. User ID's and passwords for current employees, student or temporary workers, independent contractors, vendors or PMC affiliates with access to PI shall be changed at least bi-annually.

12. Access to PI shall be restricted to active users and active user accounts only.

13. Employees, student or temporary workers, independent contractors, vendors or PMC affiliates with access to PI will be encouraged to report any suspicious or unauthorized use of customer information.

14. 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 PI for which we are responsible in accordance with 201 CMR 17.00 Standards for the Protection of Personal Information of Residents of the Commonwealth.

15. During the workday, employees, student or temporary workers, independent contractors, vendors or PMC affiliates must lock computers (requiring re-entry of a password) with access to personal information when they leave their desks. All files and other records containing PI must be secured in locked offices, file cabinets or locked drawers when unattended. As a safeguard, all office computers will be programmed to automatically lock (requiring re-entry of a password) after a specified time of no activity.

16. At the end of the workday, employees, student or temporary workers, independent contractors, vendors or PMC affiliates must either shut down or lock computers (requiring re-entry of a password) with access to personal information. All files and other records containing PI must be secured in locked file cabinets or locked drawers.

17. Fax machines, printers, multifunction, and other devices receiving or printing PI shall not be located in areas accessible to the general public but rather must be in secure areas that can be locked at night. When printing or receiving faxed PI, immediately remove the fax transmission from the fax machine and deliver it to the recipient. The department director or designee is responsible for limiting access to these devices and ensuring that faxes and printouts are properly handled.

18. Each department shall consider developing rules (bearing in mind the business needs of that department) that ensure that reasonable restrictions upon physical access to records containing PI 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.

19. Access to electronically stored PI shall be electronically limited to those employees having a unique logon; and re-logon shall be required when a computer has been inactive after a certain period of time.

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

21. Credit Card Holder data defined by the Payment Card Industry Data Security Standard (PCI DSS) including a credit card number with or without any required security code or expiration date are never to be written down or stored on the PMC network, laptop or portable devices or transmitted electronically through email.

22. It is prohibited to email or forward personal information from a work-related email account to a personal account. Personal Information cannot be store on a non-PMC owned computer, device or storage system or service. All PMC laptops and devices will be password protected and require a username and password that complies with PMC policy.

4.2 EXTERNAL RISKS

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PI, 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. To the extent that any of these measures require a phase-in period, such phase-in must begin immediately:

1. There must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the PI, installed on all systems connected to the internet processing PI.

2. 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 PI.

3. To the extent technically feasible, all PI stored on laptops or other portable devices must be encrypted, as must all records and files containing PI transmitted across public networks or wirelessly, to the extent technically feasible. Encryption here means the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

4. There must be secure user authentication protocols in place, including:

   (a) Protocols for control of user IDs and other identifiers;

   (b) A reasonably secure method of assigning and selecting passwords;

   (c) 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;

   (d) Restriction of access to active users and active user accounts only; and

   (e) Blocking of access to user identification after multiple unsuccessful attempts to gain access, when possible.

5. 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, and restricting access to records and files containing personal information to those who need such information to perform their job duties.