Nichols College
Written Information Security Program

1.0 Policy Statement

The Nichols College Written Information Security Program (WISP) is intended as a set of comprehensive guidelines and policies designed to safeguard all sensitive data maintained at the College, and to comply with applicable laws and regulations on the protection of Personal Information, as that term is defined below, found on records and in systems owned by the College.

2.0 Overview

The WISP was implemented to comply with regulations issued by the Commonwealth of Massachusetts entitled "Standards For The Protection Of Personal Information Of Residents Of The Commonwealth" (201 Code Mass. Regs. 17.00). In accordance with federal and state laws and regulations, Nichols College is required to take measures to safeguard personally identifiable information, and to provide notice about security breaches of protected information at the college to affected individuals and appropriate state agencies.

In addition, Nichols College is committed to protecting the confidentiality of all sensitive data that it maintains, including information about individuals who work or study at the College. Nichols College has implemented a number of policies to protect such information, and the WISP should be read in conjunction with these policies that are cross-referenced at the end of this document.

3.0 Purpose

The purposes of this document are to:

- Establish a comprehensive information security program for Nichols College with policies; designed to safeguard sensitive data that is maintained by the College, in compliance with federal and state laws and regulations;
- Establish employee responsibilities in safeguarding data according to its classification level; and
- Establish administrative, technical and physical safeguards to ensure the security of sensitive data.

4.0 Scope

This Program applies to all Nichols College employees, whether full- or part-time, including faculty, administrative staff, contract and temporary workers, hired consultants, interns, and student employees, as well as to all other members of the Nichols College community (hereafter referred to as the "Community"). The data covered by this Program includes any information stored, accessed or collected

at the College or for College operations. The WISP is not intended to supersede any existing Nichols College policy that contains more specific requirements for safeguarding certain types of data, except in the case of Personal Information, as defined below. If such policy exists and is in conflict with the requirements of the WISP, the other policy takes precedence.

4.1 Definitions

Personal Information (PI), as defined by Massachusetts law (201CMR17.00), is the first name and last name or first initial and last name of a person in combination with any one or more of the following:

- Social Security number;
- Driver's license number or state-issued identification card number; or
- Financial account number (e.g. bank account) or credit or debit card number that would permit access to a person's financial account, with or without any required security code, access code, personal identification number, or password.

For the purposes of this Program, PI also includes passport number, alien registration number or other government-issued identification number.

4.2 Data Classification

All data covered by this policy will be classified into one of three categories outlined below, based on the level of security required for each, starting with the highest level.

Confidential

Confidential data refers to any data where unauthorized access, use, alteration or disclosure of this data could present a significant level of risk to Nichols College or the Community. Confidential data should be treated with the highest level of security to ensure the privacy of that data and prevent any unauthorized access, use, alteration or disclosure.

Confidential data includes any data that is protected by federal or state laws or regulations, including, but not limited to, data protected under the following privacy laws: 201CMR17.00 (Mass Security Regs), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Family Educational Rights and Privacy Act (FERPA), and the FTC's Red Flag Rules. Information protected by these laws includes, but is not limited to, PI, Protected Health Information (PHI), student education records and financial aid information.

Confidential data also includes other sensitive personal and institutional data where the loss of such data could harm an individual's right to privacy or negatively impact the finances, operations or reputation of Nichols College. This data includes, but is not limited to, donor information, intellectual property

(proprietary research, patents, etc.), College financial and investment records, employee salary information, or information related to legal or disciplinary matters.

Internal Use Only

Internal Use Only data refers to any data where unauthorized access, use, alteration or disclosure of this data could present a moderate level of risk to Nichols College. This data should be limited to access by individuals who are employed by or matriculate at Nichols College and who have legitimate reasons for accessing such data. Any non-public data that is not explicitly designated as Confidential should be treated as Internal Use Only data. A reasonable level of security should be applied to this classification to ensure the privacy and integrity of this data.

Public (or Unrestricted)

Public data includes any information for which there is no restriction to its distribution, and where the loss or public use of such data would not present any harm to Nichols College or members of the Nichols College community. Any data that is not classified as Confidential or Internal Use Only should be considered Public data.

5.0 Policy

5.1 Responsibilities

All data at the College is assigned a data owner according to the constituency it represents. Data owners are responsible for approval of all requests for access to such data. The data owners for each constituency group are designated as follows:

- Faculty data - the Provost (or his or her designee) serves as data owner
- Staff data - the Vice President for Administration (or his or her designee) serves as data owner
- Student data - ownership is distributed across many departments. The Information Security Officer (ISO) will act as a conduit for questions regarding how to gain access to student data, or who the owner is.
- Alumni & donors – The Vice President for Advancement (or his or her designee) serves as data owner

Information Technology (IT) staff serve as the data steward for all data stored centrally on the College's servers and administrative systems, and are responsible for the security of such data.

Human Resources will inform IT staff about an employee's change of status or termination as soon as is practicable but before an employee's departure date from the College. Changes in status may include terminations, leaves of absence, significant changes in position responsibilities, transfer to another department, or any other change that might affect an employee's access to College data. IT staff will

terminate all of the employee's account access upon the employee's termination date from the College, as specified by Human Resources.

Department heads will alert IT at the conclusion of a contract for individuals that are not considered Nichols College employees in order to terminate access to their Nichols College accounts.

The Nichols College Information Security Officer (ISO) is in charge of maintaining, updating, and implementing this Program. The Chief Information Officer (CIO) has been designated as the ISO for Nichols College.

All members of the Community are responsible for maintaining the privacy and integrity of all sensitive data as defined above, and must protect the data from unauthorized use, access, disclosure or alteration. All members of the Community are required to access, store and maintain records containing sensitive data in compliance with this Program.

5.2 Identification and Assessment of Risks to College Information

Nichols College recognizes that it has both internal and external risks to the privacy and integrity of College information. These risks include, but are not limited to:

- Unauthorized access of Confidential data by someone other than the owner of such data
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of Confidential data by employees
- Unauthorized requests for Confidential data
- Unauthorized access through hard copy files or reports
- Unauthorized transfer of Confidential data through third parties

Nichols College recognizes that this may not be a complete list of the risks associated with the protection of Confidential data. Since technology growth is not static, new risks are created regularly. Accordingly, IT will actively participate and monitor advisory groups such as the Educause Security Institute, the Internet2 Security Working Group and SANS for identification of new risks.

Nichols College believes the College's current safeguards are reasonable and, in light of current risk assessments made by IT, are sufficient to provide security and confidentiality to Confidential data maintained by the College. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

5.3 Policies for Safeguarding Confidential Data

To protect Confidential data, the following policies and procedures have been developed that relate to protection, access, storage, transportation, and destruction of records, computer system safeguards, and training.

Access

- Only those employees or authorized third parties requiring access to Confidential data in the regular course of their duties are granted access to Confidential data, including both physical and electronic records.
- Computer and network access passwords are disabled upon termination of employment or relationship with Nichols College.
- Upon termination of employment or relationship with Nichols College, physical access to documents or other resources containing Confidential data is immediately prevented.

Storage

- Members of the Community will not store Confidential data on laptops or on other mobile devices (e.g., flash drives, smart phones, tablets, CDs, external hard drives). In rare cases where it is necessary to transport Confidential data electronically, the mobile device containing the data must be encrypted.
- To the extent possible, making sure that all Confidential data is stored only on secure servers maintained by the College and not on local machines, unsecure servers, or portable devices.
- Paper records containing Confidential data must be kept in locked files or other secured areas when not in use.
- Electronic records containing Confidential data must be stored on secure servers, and, when stored on authorized desktop computers, must be password protected.
- Massachusetts PI must not be stored on any cloud storage provider (such as Google Docs or Microsoft OneDrive).

Removing Records from Campus

- Members of the Community are strongly discouraged from removing records containing Confidential data off campus. In rare cases where it is necessary to do so, the user must take all reasonable precautions to safeguard the data. Under no circumstances are documents, electronic devices, or digital media containing Confidential data to be left unattended in any insecure location.
- When there is a legitimate need to provide records containing Confidential data to a third party, electronic records shall be password-protected and encrypted, and paper records shall be marked confidential and securely sealed.

Traveling Abroad with Students' Personal Information

- In the event that transmission of student passport information is required by the hotel or program abroad in advance of the travel, only the relevant information requested (e.g., Name, Passport Number, Date of Expiry, and Date of Birth) will be provided, not complete copies of the passport images. This information should first be transmitted via Fax, provided that the Nichols College department arranging the travel confirms the accuracy of the Fax number by sending an initial confirmation message before the actual data. If Faxing is unavailable, the data may be sent via secure email, provided that the same confirmation of transmission takes place.
- Faculty/staff who need to retain these passport numbers for arranging travel will store this data in spreadsheets that are saved on the College's secure servers. Any spreadsheets containing student passport information will be routinely deleted when not needed.
- Faculty/staff who are traveling with the students abroad that need student passport and visa information for hotel check-in will keep a paper record on their person that contains relevant information (such as the passport and visa numbers and their expiry dates) and the last names of the students only. Faculty/staff must not retain or travel with copies of student passports.
- In extreme circumstances involving travel to a remote location where access to technology would be limited and would prohibit retrieval of a lost passport, a program director may request an exemption to this policy allowing for him or her to retain copies of the students' passports during travel. This request will be made to the Chief Information Officer for approval. If the request is approved, the program director will sign the "Faculty/Staff Agreement for Traveling with Secure Data" to acknowledge their understanding of the WISP and their responsibilities in protecting the passports. The program director also agrees to alert IT immediately if the copies of passport are lost.

Destruction of Confidential Data

- Paper and electronic records containing Confidential data must be destroyed in a manner that prevents recovery of the data. **Massachusetts General Law 93I** specifies the manner in which records containing PI must be destroyed.

Third-Party Vendor Agreements Concerning Protection of Personal Information

- Nichols College exercises appropriate diligence in selecting service providers capable of maintaining appropriate security safeguards for PI provided by the College to them. The primary budget holder for each department is responsible for identifying those third parties providing services to the College that have access to PI. All relevant contracts with these third parties are reviewed and approved by the Nichols College Purchasing Department to ensure the contracts contain the necessary language regarding safeguarding PI. It is the responsibility of the primary

budget holders to confirm that the third parties are required to maintain appropriate security measures to protect PI consistent with this Program and Massachusetts laws and regulations.

5.4 Computer system safeguards

The ISO monitors and assesses information safeguards on an ongoing basis to determine when enhancements are required. The College has implemented the following to combat external risk and secure the College network and data containing PI:

- Secure user authentication protocols
- Unique passwords are required for all user accounts; each employee receives an individual user account.
- Server accounts are locked after multiple unsuccessful password attempts.
- Computer access passwords are disabled upon an employee's termination.
- User passwords are stored in an encrypted format; root passwords are only accessible by system administrators.
- Secure access control measures.
- Access to specific files or databases containing PI is limited to those employees who require such access in the normal course of their duties.
- Files containing PI transmitted outside of the Nichols College network are to be encrypted.
- The ISO ensures regular internal network security audits are performed for all server and computer system logs to discover to the extent reasonably feasible possible electronic security breaches, and to monitor the system for possible unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of PI.
- All College-owned computers and servers are firewall protected and regularly monitored.
- Operating system patches and security updates are installed to all servers in a timely manner.
- Antivirus and anti-malware software is installed and kept updated on all servers and workstations. Virus definition updates are installed on a regular basis, and the entire system is tested and checked at least once per month.

5.5 Employee Training

All employees who access Confidential data via the firewall or who otherwise have access to PI are required to complete a yearly training on data security and their responsibilities related to this Program. The training is also strongly recommended for all employees. The ISO maintains records of all such training.

5.6 Reporting Attempted or Actual Breaches of Security

Any incident of possible or actual unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of PI, or of a breach or attempted breach of the information safeguards adopted under this Program, must be reported immediately to the Information Security Officer (ISO).

The ISO is charged with the identification of all data security incidents where the loss, theft, unauthorized access, or other exposure of sensitive College data is suspected. The ISO reports any such incidents to the Vice President for Administration. The Vice President for Administration is responsible for determining appropriate actions in response to the breach.

The ISO will document all breaches and subsequent responsive actions taken. All related documentation will be stored in the Financial Operations Office.

For more information about incident response, including specific procedures for responding to a breach, see the **Nichols College Security Incident Response Plan**.

6.0 Enforcement

Any employee or student who willfully accesses, discloses, misuses, alters, destroys, or otherwise compromises data classified as Confidential or Internal Use Only without authorization, or who fails to comply with this Program in any other respect, will be subject to disciplinary action, which may include termination in the case of employees and expulsion in the case of students.

7.0 Policies cross-referenced

The following Nichols College policies and related documents provide advice and guidance that relates to this Program:

- **Acceptable Use Policy**
- **Data Retention Policy**
- **Data Security Policy**
- **PCI Compliance Policy**
- **PCI Compliance – Identity Authentication Process**
- **Red Flag Policy for Identity Theft**
- **Security Incident Response Plan**

8.0 Effective date

This Written Information Security Program was implemented January 1, 2015. The College will review this Program on a regular basis and reserves the right to change, modify, or otherwise alter this Program at its sole discretion and at any time as it deems circumstances warrant.