Written Information Security Plan (WISP)

"PERSONAL INFORMATION SECURITY PLAN AND POLICY OF NORTH SHORE COMMUNITY COLLEGE"

NORTH SHORE COMMUNITY COLLEGE

I. Introduction

At North Shore Community College. ("NSCC") we are sensitive to the need to protect the security and confidentiality of the personal information of our students and employees or others contained in our business records. It is the policy of this public institution of higher education that personal information contained in our records is limited to that reasonably necessary to accomplish legitimate business purposes, and to comply fully with state and federal regulations. Our objective in the development and implementation of this comprehensive written personal information security plan is to create effective administrative, technical and physical safeguards for the protection of personal information at NSCC, and to comply with our obligations under Federal and State laws and regulations, including those related to protecting the personal information of Massachusetts residents.

This comprehensive written information security program ("WISP") sets forth our procedures for evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information, especially the personal information of residents of the Commonwealth of Massachusetts. For purposes of this WISP, "personal information" means the 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: (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 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.

The purpose of the WISP 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.

In formulating and implementing the WISP, (1) identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information; (2) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information; (3) evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks; (4) design and implement a WISP that puts safeguards in place to minimize those risks, consistent with the requirements of Chapter 93H (Massachusetts residents); and (5) regularly monitor the effectiveness of those safeguards.

II. Limited Access to Personal Information

Access to personal information in our business records such as name, social security number, driver's license information and any financial account information is strictly limited to those persons who are required to know such information to perform their job functions. Generally, this means the administrative managers and staff

whose jobs require them to manage or enter data for business purposes must understand their responsibilities and have procedures in place to be in compliance with this policy. The VP for Administration and the Chief Information Officer (CIO) are the designated Data Security Officers for overall purposes of this Plan and Policy. Other College managers have delegated responsibility that employees in their areas are trained and understand the plan and policy, and have procedures in place as appropriate for ensuring the protection of personal information.

The following mandatory requirements apply to all NSCC employees having access to personal information:

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

- Employees *are required* to report any suspicious or unauthorized use of personal information. Failure to report any such actual or suspected unauthorized access, possession or use of personal information when such becomes known to an employee or reasonably should be known, may lead to disciplinary action, up to and including suspension and/or termination. (refer to escalation policy)

- Employees are prohibited from keeping open files containing personal information on their desks or computer "desk tops" when they are not at their desks.

- At the end of the work day, all files and other records containing personal information must be secured in a manner that is consistent with the procedures for protecting the security of personal information.

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

- Visitors' access must be restricted for each office in which personal information is stored. Visitors shall not be permitted to visit unescorted any area within our premises that contains personal information.

- All files and other records containing personal information must be replaced in the designated secure and locked location/cabinet immediately after use. Files containing personal identifying information shall not be kept in any common areas. This prohibition pertains to active as well as archival files.

- Employees are prohibited from sharing electronic passwords for computer and electronic records access if such passwords allow access to personal information.

- The amount of personal information collected should 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.

- Electronic access to user identification after multiple unsuccessful attempts to gain access must be blocked.

- Current employees' user ID's and passwords must be changed periodically.

- 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.

III. The Data Security Officer (DSO) Position

The College has designated the functions of Data Security Officers to the VP of Administration and Chief Information Officer to ensure compliance with this policy. The DSOs performs bi-annual or as-needed data security reviews to ensure the continued effectiveness of all security measures taken to protect personal information. They are also responsible for ensuring that all appropriate regulatory bodies and authorities are notified promptly in the event of a security breach involving personal information

IV. Responsibilities of DSOs

The DSOs are responsible for initial implementation of this policy and procedure;

a. the appropriate training of employees, in conjunction with college managers and under the overall training responsibility of the VP of Human Resources; the College has implemented an Information Security Awareness and Training program online.
b. regular monitoring and testing of stated and required security safeguards; evaluating the ability of each of our third party service providers to protect, in the manner consistent with our obligations under Chapter 93H, the personal information to which we have permitted them access; and taking the steps reasonably necessary to ensure that such third party service provider is applying to such personal information comprehensive security measures at least as stringent as those required to be applied to such information under 201 CMR 17.00;
c. Reviewing the scope of security measures 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. The DSOs shall be responsible for this review and shall fully apprise management of the results of the review and any recommendations for improved security arising out of said review;
d. Conducting an annual training session for all managers that supervise employees who have access to personal information. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with the requirements for ensuring the protection of personal information; all College employees are asked to complete the online Information Security and Massachusetts Privacy course; College employees who deal with credit card information are required to complete the online PCI course. College managers are responsible for ensuring their staff completes the appropriate online courses; the VP of Human Resources oversees the overall training of College employees, the completion of required online courses, and training of new employees.
e. in the event of a security breach or unauthorized acquisition/use of personal information, ensuring that the required notices in the proper form are sent to the appropriate state authorities and affected Massachusetts residents;
f. Ensuring that all documents and electronic devices containing personal information are properly disposed of in accordance with the requirements of G.L. c. 93I.

V. Responsibility for Terminated Employees

The VP for Human Resources, in conjunction with the Chief Information Officer (CIO) where applicable, shall ensure that terminated employees return all company records and devices including those containing employee or other's personal information. The CIO shall also put procedures in place to ensure that a terminated employee's access to personal information — whether physical or electronic — is immediately blocked.

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, custody or control (including all such information stored on laptops or other portable devices or media, and in any hard-copy files, records, work papers, etc.).

Such terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the firm's premises or personal information. Moreover, such terminated employee's remote electronic access to personal information shall be disabled; his/her voicemail access, e-mail access, internet access, and passwords shall be invalidated immediately.

VI. Master Log of Access Methods, Passwords and Identifiers

The Campus Police Chief shall maintain a highly secured master list of all lock combinations and keys, and access codes to Campus Safety equipment/software. The CIO shall maintain a highly secured master list of passwords, access codes and any other electronic identifiers, and the corresponding identities of all those individuals holding same or with access to same for any college systems other than those related to Campus Safety. Generally, it is considered a violation of this policy to swap, exchange, or utilize assigned passwords and/or access codes which have been specifically assigned to an individual employee. Disciplinary action up to and including suspension or termination may result for violations of this policy.

VII. Limited Access to Personal Information/Penalties for Violation

NSCC limits the physical location of personal information to storage in locked and secure areas and storage units which are purposefully located outside of and beyond the reach of common areas in our offices. Access to these locked and secured areas is limited to those employees needing same to do their job and under the supervision of College managers of those areas. College Archive areas are under the supervision of the Auxiliary Services Staff Assistant and Asst. VP of Administration. Access to electronic information is under the purview of the Chief Information Officer and VP of Administration. To the extent any personal information is contained in electronic format, access to such records is at all times password protected. To the extent technically feasible, records containing personal information are encrypted if subject to electronic transmission, or removal from the business premises via electronic means and devices. Any non-conforming use of, access to or exchange of personal information is strictly prohibited and against company policy. Disciplinary action up to and including suspension or termination may result for violations of this policy and is the responsibility of the VP of Human Resources and ultimately the President of the College

VIII. Transportation of Personal Information and Encryption

It is the policy of NSCC that personal information not be stored, maintained or transported on lap-top or other portable electronic devices unless absolutely necessary. In those rare instances when such information may have to be transported via lap-top or other portable electronic device, laptops shall be encrypted. Use of Mobile devices must conform to the College's Mobile Device Policy and procedures. The electronic transmittal/handling of this information is strictly limited to those few persons specifically assigned to handle these tasks. *Current employees' user-IDs and passwords must be changed periodically*. Access to electronically stored personal information shall be limited at all times to those few employees on a need-to-know basis who shall be assigned a unique log-in I.D. Re-log-in is required when the computer is not in use more than a few minutes. All computer systems and devices used to store or access employee personal information are routinely monitored for unauthorized use, possession or access. Employees of NSCC do not have a reasonable expectation of privacy in any electronic devices issued or provided by the college, or any information stored,

maintained, placed or reviewed thereon by the employee. Unauthorized use, possession or access of such devices may result in disciplinary action up to and including suspension or termination.

IX. Destruction of Records Containing Personal Information

It is the policy of NSCC to carefully and fully dispose of all documents and things containing personal indentifying information. The Auxiliary Services Staff Assistant (and Asst. VP for Administration to whom the employee reports) is responsible for ensuring that all records retention regulations are met, and that when appropriate, on an institutional level, the documents, records and things containing personal identifying information are shredded, pulverized or otherwise disposed of in such a way as to ensure their complete destruction. All managers of areas that handle psychical documents or records that contain personal identifying information must, on a regular basis, see that procedures for secure shredding and safe disposal of documents are executed, often in conjunctions with the Auxiliary Services department.

X. 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 must be completed on or before June 30, 2011:

External Threats:

- 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.
- 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.
- All computer systems must be monitored for unauthorized use or access to personal information.

- There must be secure user authentication protocols in place, including: (1) protocols for control of user IDs and other identifiers; (2) a reasonably secured method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; (3) control of data security passwords to ensure that such passwords are kept in a location.
- Contractually requiring that such 3rd party providers/vendors comply with all State regulations - this contractual requirement is covered when the 3rd party provider/vendor signs a State Contract form which lists the State Terms and Conditions.

Any questions concerning the content of this Plan and Policy should be addressed to Gary Ham , the designated Data Security Officer for the College.