2550
INFORMATION SECURITY

1. General

The College is committed to protecting and safeguarding all data and information that it creates, collects, generates, stores, and/or shares during the generation and transmission of knowledge as well as during the general operation and administration of the College. The College is also committed to complying with all federal and state laws pertaining to securing this data and information and preventing its disclosure to unauthorized individuals. These laws include, but are not limited to, the Financial Services Modernization Act of 1999, also known as the Gramm- Leach-Bliley Act or GLBA. In 2003, the Federal Trade Commission (FTC) confirmed that higher education institutions are considered financial institutions under this federal law and promulgated the GLBA Safeguards Rule, 16 CFR Part 314, which requires higher education institutions to have an information security program to protect the confidentiality and integrity of personal information. This policy describes the basic components of the Northern Information Security Program which applies to employees (student, staff, and faculty), contractors, vendors, volunteers, and all other individuals who work with Northern data and information.

2. Northern Information Security Program

The Northern Information Security Program is designed to protect the confidentiality, integrity, and availability of protected information; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of protected information that could result in substantial harm to any student, parent, employee, or customer of the College. This program includes the process for identification of risks and defines responsibilities for safeguarding information, monitoring the effectiveness of the safeguards, evaluating service providers, and updating the program itself.

2.1. Protected Information

The GLBA Safeguards Rule mandates that the Northern Information Security Program be designed to safeguard non-public, personally identifiable financial information

- that is provided to the College,
- results from any transaction with the consumer or any service performed for the consumer (i.e. students, faculty, staff, employees, associates, donors, patients), or
- is otherwise obtained by the College.

The Northern Information Security Program defines what specific data elements and information (and in what context) constitute to-be-protected non-public, personally identifiable financial information, which includes but is not limited to:

- social security numbers,
- credit card number, and
- bank routing and account numbers when used in conjunction with the account owner's name.

2.2. Information Security Plan Coordinator

The College Director of Information Technology is designated as the Information Security Program Coordinator, a specific role required by the GLBA. This position is responsible for:

- developing and implementing the Northern Information Security Program;
- identification of risks to confidentiality, integrity, and availability of protected information;
- designing and implementing appropriate safeguards;
- evaluating the security program; and
- making adjustments to reflect relevant developments or circumstances that may materially affect these safeguards, including changes in operations or the results of security testing and monitoring.

2.3. Risk Assessment

The Northern Information Security Program will include processes and procedures to assess the risk to the College's information systems. Information systems include the hardware and software components of the computing infrastructure as well as individual personal computers, personal digital assistants, phones, servers, networks, and peripheral technologies used for the processing, storage, transmission, retrieval, and disposal of information. Risks to the College's information systems extend beyond computer-related hardware and software to include, for example, hiring procedures; data handling procedures; individuals who have access to information systems and the data therein; and the buildings and equipment that contain any aspect of an information system including the transmission of protected information.

2.4. Employee Management and Training

The success of the Information Security Program depends largely on the employees who implement it. The Director of Information Technology will coordinate with deans, directors, and heads of departments that have access to protected information to evaluate the effectiveness of departmental procedures and practices relating to access to and use of protected information. The Northern Information Security Program details recommended administrative safeguards designed to train personnel, increase awareness, and reduce risks to the confidentiality, integrity, and availability of protected information such as:

- mandatory information assurance training;
- periodic audits to ensure individuals have only the appropriate level of information system access rights and permissions required to perform their jobs;
- periodic reviews of job descriptions and position requirements to ensure the appropriate levels of reference and background checks are conducted before hiring decisions are made;
- non-disclosure and confidentiality statements required when appropriate; and
- periodic evaluations of each individual's understanding of college and/or departmental data handling procedures.

2.6. Departmental Responsibilities

Deans, directors, and heads of departments that have access to protected information are responsible for informing employees of ongoing updates to security measures, ensuring employees have attended required information security training, and notifying departmental computer system administrators and Information Technology Services (ITS) when employees no longer require access due to reassignment or termination.

2.7. College-Wide Responsibilities

All breaches of information security must be reported immediately to campus safety and security office or the IT department accordance with the procedures listed in the NORTHERN Information Security Program.

3. Compliance by Service Providers

Service providers and/or contractors who provide services that may allow them to access protected information must comply with the GLBA safeguard requirements, the College's Information Security Program, and applicable College policies listed herein. The College Purchasing Department is responsible for reviewing prospective service providers and/or contractors to ensure they have and will maintain appropriate safeguards for protected information.

4. Monitoring and Testing

The Director of Information Technology will regularly monitor the Northern Information Security Program and periodically test the required and recommended safeguards. Based on these assessments, the Director of Information Technology will work with all appropriate individuals to implement, correct, design, or improve safeguards.

5. Evaluation and Adjustment

The Director of Information Technology is responsible for adjusting the Northern Information Security Program to ensure that the required and recommended administrative, physical, and technical safeguards are appropriate to the College's size and complexity, the nature and scope of its activities, and the sensitivity of the data and information the College handles.