

# **Saint Michael's College**

## **Information Security Plan:**

### **Policy and Procedures**

May 2003

The information security plan at Saint Michael's College is designed to protect non-public and financial information about our students, applicants, alumni, donors, employees and other constituents by developing reasonable physical, administrative and technical safeguards that:

- (1) Ensure the security and confidentiality of this information, whether electronic or hard copy,
- (2) Protect against threats to the security and/or integrity of such records, and
- (3) Protect against unauthorized access to or use of such data that could result in substantial harm or inconvenience to any constituent.

The Vice President for Finance and the Director of Finance are the designated GLBA compliance officers for Saint Michael's College. Any questions about this policy should be directed to the Office of Finance, Room 103, Founders Hall, or by telephone: (802) 654-2512.

This policy is designed in accordance with the Safeguarding provisions of the Gramm Leach Bliley Act (GLBA or "the Act"), as codified by 16 CFR Part 314, and is effective May 23, 2003.

#### **1. Risk assessment**

A process of risk assessment was initially undertaken during April – May 2003, and will be updated annually as outlined in section 10. Any risks or control weaknesses identified in this process shall be noted, and procedures developed to mitigate any material risks.

Identified risks include:

- Unauthorized access of information by someone other than authorized faculty, staff and agents of the College
  - Telephone requests for information
  - Third party transfer of data
  - Access to hard copy files
- Compromised system security as a result of unauthorized computer system access
  - Interception of data during electronic transmission
  - Loss of data integrity due to corruption
- Physical loss of data due to accident, fire, flood, or other disaster

#### **2. Classification of documents and customer information**

Non-public and financial information is defined for this policy to include social security number, bank and credit card account numbers, financial information such as copies of income tax returns and FAFSA forms, and other income and credit histories (hereafter referred to as "classified information").

#### **3. Appropriate use of physical and electronic files**

The College recognizes that many departments on campus have legitimate business needs for certain classified information about our constituents. However, access to such information should be physically restricted within the department having the immediate need for hard copy information, and electronic access should be limited by appropriate system login and access security methods as established and maintained by the Department of Information Technology.

#### **4. Protection of hard copy classified information**

Classified information as defined in section 2 shall be maintained in locked filing cabinets or in a locked file room with limited overnight access. Office doors shall be locked when offices containing this information are vacant or otherwise unattended during office hours. Classified information should be adequately controlled during processing, and should be reasonably secured while not in use. Classified information sent to other departments on campus should be hand-delivered or sent via campus mail in a sealed envelope marked "confidential."

## **5. Destruction and retention of hard copy classified information**

Relevant college personnel should shred any hard copy classified information in accordance with applicable records retention procedures, and such information should be stored securely until such time as it is shredded. If an outside vendor is used for destruction of such records, the vendor should be contractually obligated to maintain the confidentiality of this information, and precautions should be taken to ensure the protection of this information. Refer to section 9 re: contracts with vendors and service providers.

## **6. Information Systems**

The Department of Information Technology shall maintain proper policies and procedures to ensure appropriate physical, administrative, and technical safeguards as outlined in the Act.

## **7. Managing System Failures**

### **a. Intrusion Detection**

The Information Technology department shall maintain appropriate electronic intrusion detection systems, and shall take the necessary steps to identify breaches of confidentiality in accordance with this policy. In addition, Managers of departments that maintain custody of hard copy classified information shall contact the Office of Security should a breach of physical security be discovered in their office; Security shall undertake an investigation and coordinate or recommend the appropriate response given the circumstances.

### **b. Response program**

In the event of system failure, the College shall notify constituents potentially affected by the safeguarding violation or possible violation in writing within a reasonable time after such breach is detected. Responses shall be initiated by the compliance officers, and coordinated with the Chief Information Officer and Director of Public Relations (if applicable), and the President's Cabinet and/or the President.

## **8. Disaster recovery and business continuation**

The Department maintaining classified information shall develop written disaster recovery and business continuation plans as appropriate, and shall make these plans available to the compliance officers upon request. These contingency plans should be reviewed and updated as business conditions change, but not more than annually as required by section 10.

## **9. Service Providers**

### **a. Due Diligence and Monitoring**

The College shall exercise due diligence by ensuring that all outside service providers that have access to classified information take appropriate steps to ensure the safeguarding of such information.

### **b. Contracts**

The Director of Purchasing and Auxiliary Services shall review and/or negotiate all relevant contracts prior to execution, and shall ensure that all relevant contract terms are provided to address safeguarding of classified information related to the services to be provided. These terms might include some or all of the following:

- A statement of compliance with the provisions of the Act
- An explicit acknowledgement that the College allows the service provider access to classified information
- A specific definition of classified information as related to the services being provided
- A stipulation that the classified information will be held in strict confidence and used only for the business purposes as outlined by the contract
- A guarantee from the service provider that it will ensure compliance with the safeguarding provisions contained in the contract, as defined by the GLBA

- A provision addressing return or destruction of all such classified information upon termination of the contract, subject to records retention requirements
- A provision defining remedy for breach of safeguarding provisions under the contract, including termination without penalty
- A provision allowing or requiring audit of the service provider's safeguarding provisions, as applicable (independent assessment, internal audit review, or SAS 70 report).
- A provision ensuring that the contract's protective requirements survive any termination agreement.

## **10. Ongoing review**

### **a. Testing**

The compliance officers will perform or initiate appropriate testing of controls in high-risk areas, which may include internal audit by relevant staff members or independent examination by external auditors.

### **b. Reporting**

A risk assessment will be performed and updated annually to identify and assess relevant risks. Relevant department heads will submit risk assessment reports to the compliance officers annually beginning July 1, 2003. Interim reviews will occur during each fiscal year to identify emergent risks and changes that may be necessary due to changes in the internal and external business environment, changes in the sensitivity of information, changes in technology or business arrangements.

The compliance officers shall report annually to the Operations Committee of the Board of Trustees at their fall meeting.

## **11. Employee management and training**

### **a. Segregation of duties**

Where possible, the College shall take all appropriate measures to ensure appropriate segregation of duties, within the confines of the size of our staff and the scope of the Act.

### **b. Employee hiring procedures**

The Office of Human Resources will perform or coordinate background checks and other such due diligence as deemed necessary under this policy when hiring new employees. In addition, certain employees may be required to sign confidentiality agreements. The Office of Human Resources shall develop disciplinary procedures to address any infractions of these policies.

### **c. Office procedures**

Offices that maintain classified information shall develop and maintain relevant written procedures to comply with this policy, such as locking filing cabinets and office doors, maintaining security of computer user accounts through password-protected screensavers, strong passwords, and periodic password changes and other procedures as applicable to the department and as outlined in sections 4-6 of this policy statement. These policies and procedures shall be reviewed and updated annually, and submitted to the compliance officers in accordance with section 10b of this policy.

### **a. Training**

The College will provide appropriate training for all employees and volunteers. New employees will receive a copy of relevant policies and procedures upon hiring, and will participate in a new employee orientation session at which these policies will be reviewed. In addition, employees of certain departments as identified in the risk assessment will participate in annual training updates, which the GLBA compliance officers will coordinate with FERPA compliance efforts. This training shall include fraud recognition and appropriate responses as outlined in section 7.