Saint Michael's College

Information Security Policy:
Information Security Awareness and Training Policy

1. Purpose

The purpose of the Saint Michael's College (SMC) Information Security Awareness and Training Policy is to address security issues related to the safety and integrity of information maintained on SMC computerized information systems. This policy is not intended to address the proprietary interests of intellectual property and/or copyright issues.

2. Scope

This policy applies to all SMC faculty, staff, students, and others (e.g. vendors, grant or independent contractors, etc.) accessing or attaching to computers operated by SMC.

3. Policy

3.1 Persons using or attaching to SMC computer resources will acknowledge compliance with the Acceptable Use Policy when userids and passwords are assigned, and in some cases, when a software application is accessed.

3.2 Computer resources are valuable assets and unauthorized use, alteration, destruction, or disclosure of these assets is a computer-related crime, punishable under Vermont statutes and federal laws, as well as through administrative and/or civil sanctions.

3.3 Computer software purchased using SMC funds is SMC property and shall be protected as such.

3.4 Unauthorized/unlicensed use of software (software piracy) will not be tolerated and such software will be removed by the appropriate administrators.

3.5 Use of SMC systems to attack other computer systems, internal or external to SMC, is a violation of this policy subject to administrative, civil, and/or criminal sanctions.

3.6 Attempting to circumvent security or administrative access controls for computer resources is a violation of this policy, as is assisting someone else or requesting someone else to circumvent security or administrative access controls. Persons violating this policy will be subject to appropriate administrative, civil, and/or criminal sanctions.

3.7 Violations of the policy will be reported to the SMC Security and Safety Office. All computer incidents involving SMC computer systems must be reported to the SMC Security and Safety Office, whether or not damage, unauthorized review and/or unauthorized use of information contained on the system occurred.

3.8 Willful violations of the policy that may be violations of state and federal laws will also be reported to the SMC Security and Safety Office.

3.9 Userids and passwords must control access to all computer resources except for those specific resources identified as having public access. All servers must require strong passwords.

3.10 Passwords must be changed periodically by the user. All computer resources will require passwords to be changed at least twice during the academic year. Passwords must be unique up to or exceeding three previous passwords.

3.11 Users are responsible for managing their passwords and for all actions and functions performed by their userids.

3.12 All computer resources must provide a notice before logon stating that the unauthorized access is not permitted; and that usage may be monitored.

3.13 Information, which by law is confidential, must be protected from unauthorized access or modification. Data, which is essential to critical functions, must be protected from loss, contamination, or destruction.

3.14 Confidential information shall be accessible only by personnel who are authorized by the owner on a basis of strict "need to know" in the performance of their duties.

3.15 All employees accessing an administrative application must receive appropriate training for using the application and must acknowledge the security and privacy requirements for the data contained in the application. Employees will be trained by their immediate supervisors.

3.16 When an employee terminates employment their access to Computer resources will be terminated.

3.17 All computer resources used for mission critical applications shall have a cost effective, written contingency plan that will provide for prompt and effective continuation of critical missions in the event of a disaster. IT will maintain a list of computer resources that have been designated as used for mission critical applications and file duplicate copies in the appropriate VPs office.

3.18 All microcomputer end-user workstations should have virus protection software installed or other, appropriate security measures.

3.19 All information processing areas used to house computer resources supporting mission critical applications must be protected by physical controls appropriate for the size and complexity of the operations and the criticality or sensitivity of the systems operated at those locations. Physical access to these areas shall be restricted to authorized personnel.

3.20 Individuals who believe they have experienced computer generated harassment or discrimination should contact the Information Technology office to file a complaint.

3.21 Individuals who have reason to believe that their personal information or computer intrusion/tampering have occurred with respect to their accounts should contact the Information Technology office immediately.

3.22 Students may not set up servers in their residence hall rooms. Exceptions to this policy must be approved by the Assistant Director of IT - Network Operations. Exceptions will be approved on a case-by-case basis.

3.23 Employees may not use SMC computer resources to set up services or accounts the purpose of which is not in accordance with the non-profit, educational mission of the college. Individuals with questions concerning the appropriate use of a college computer should contact the Information Technology office

3.24 Electronic mail is provided to faculty, staff, and students as part of the computer resources of SMC to conduct the business of SMC. Electronic mail is intended to be a convenient way for the faculty, staff, and students to communicate with one another and colleagues at other locations. It is not the practice of SMC to monitor the contents of electronic mail messages. However, the information in electronic mail files may be

subject to disclosure under certain circumstances; for example, during audit or legal investigations. SMC does not routinely monitor (e.g. via cookies) the Internet browsing habits of its students and employees.

4. Enforcement

Violation of this policy may result in disciplinary action which up to and including termination for employees and temporaries; a termination of the contract without compensation in the case of contractors or consultants; or dismissal for interns and volunteers. Additionally, individuals are subject to loss of Saint Michael's College information resource access privileges, civil, and criminal prosecution or other legal action. They may also be held financially liable.