## 1.0 Purpose

The purpose of this policy is to define the basic set of procedures that Information Technology (IT) department uses to maintain protection of Saint Michael's College (SMC) information technology resources. Access to the variety of information technology resources is based on the role of the individual.

## 2.0 Scope

This policy applies to all users of all information systems that are the property of Saint Michael's College. Specifically, it includes:

- All employees, whether employed on a full-time or part-time basis by Saint Michael's College.
- All contractors and third parties that work on behalf of and are paid directly by Saint Michael's College.
- All contractors and third parties that work on behalf of Saint Michael's College but are paid directly by an alternate employer.
- All employees of partners and clients of Saint Michael's College that access Saint Michael's College's non-public information systems.
- All students, graduate and undergraduate, whether enrolled full time or part-time at Saint Michael's College.
- Guests of the College.

## 3.0 Definitions

3.1 **Data Center**: Any room primarily used for housing servers or network infrastructure equipment. Other terms used are computer room and server room.

3.2 **Third Party**: A vendor partner employee or organization employee affiliated with the College.

## 4.0 Policy

4.1 User Access

Access control procedures shall be used to authenticate all users who access Mikenet resources. Such controls shall include, at a minimum, a unique logon ID and a password for each user. The network operating system shall be configured to encourage a periodic expiration of all passwords as well as to establish a suitable minimum length for passwords; these rules are outlined in the Password Standard documentation.

Logon IDs which have supervisor or root privileges shall be highly secured and named. Such IDs shall be reserved for system management tasks and shall not be used as the IDs for normal day-to-day work by the users having these privileges.

Access rights and privileges for all authorized users shall be maintained and managed so as to secure access to data in a manner appropriate to the needs of the user and the value of the data.

Confidential data shall be protected against unauthorized access regardless of form, computing environment or location. Serious access control problems can be created when confidential data is downloaded or otherwise transferred from a secure environment to a less secure environment.

When equipment is transferred to another user, the hard drive will be wiped clean by applying a new desktop image prior to the transfer. The hard drives of any equipment to be disposed of will undergo a Department of Defense level wipe. Machines will be randomly audited to ensure that the DOD wipes are successful.

All information system accounts will be actively managed by appropriate administrative staff. Active management includes the acts of establishing, activating, modifying, disabling, and removing accounts from information systems.

Information system accounts will be constructed to enforce the most restrictive set of rights/privileges or accesses required for the performance of tasks associated with that account. In order to eliminate any conflict of interest, accounts shall be created such that no one account can authorize, perform, review, and audit a single transaction.

4.2 Physical Access

Access to facilities, information systems and information system display mechanisms will be limited to authorized personnel only. Authorization will be demonstrated through the use of ID badges that have been issued by Saint Michael's College. A list of authorized personnel will be established and maintained such that newly authorized personnel will immediately be appended to the list of authorized personnel, and those personnel who have lost authorization will immediately be removed from the list.

Only authorized persons are allowed unescorted in Data Centers. Non-authorized persons in Saint Michael's College's Data Centers must be escorted by an authorized person at all times and must sign the IT Visitor Log located at the main entrance to the Data Centers.

Before any computer and/or network equipment housed in Saint Michael's College Data Centers is removed from Saint Michael's College oversight and control, data and configuration information must be removed.

Access to Saint Michael's College's Data Centers must be controlled by physical security systems. Access to all Data Center facilities will be controlled at defined access points by locked doors. Authorized personnel are required to authenticate themselves at these access points before physical access to facilities, information systems or information system display mechanisms is allowed. The delivery and removal of information systems will also be controlled at these access points. No equipment will be allowed to enter or leave the facility without prior authorization.

4.3 Third Party Access

The level of access granted to vendors and other third-party non-affiliates will be limited to those information technology resources that are required to carry out the specified business need of the College. The access must be enabled for specified tasks and functions, and limited to specific individuals and only for the time period required to accomplish approved tasks. Vendor access must be uniquely identifiable, and password management must comply with the most current college password policies. Appropriate procedures for terminating access must be followed upon the departure of a vendor employee from the contract/agreement or upon the termination/completion of the contract/agreement.

Prior to granting a vendor employee or other third-party non-affiliate access to Saint Michael's College information technology resources, the individual will be required to sign an agreement/contract with the College that specifies:

- The Saint Michael's College information technology resource(s) to which the third party individual will be granted access
- The business purpose for which access is to be granted and limiting access to that purpose
- The information to which the individual should have access
- A statement indicating that the individual agrees to comply with all applicable Federal and State statutes and College policies with respect to preserving the confidentiality of the information to which they have access and that they will not disclose in any way the information or the existence of the information
- The acceptable method(s) for the return, destruction or disposal of the College's information in the individual's possession at the end of the contracted period or completion of the service

- A statement indicating that any information acquired by the vendor employee in the course of the contract/agreement cannot be used for the vendor's own purposes or divulged to others
- That the vendor will restrict access to Saint Michael's College data/resources to only those vendor employees who are required to provide the service
- Vendor employees will take all reasonable steps, based upon relevant industry standards to protect the College's data/resources from corruption, tampering, or other damage

Vendors and other third-party non-affiliates are expected to adhere to all applicable Federal and State statutes and College policies, including the College's Security policy and the Individual Responsibilities with Respect to Appropriate Use of Information Technology Resources policy, and must follow all applicable Saint Michael's College change control processes and procedures.

Third parties must agree to accept responsibility for costs associated with errors they commit related to data security. All Statement of Work (SOW) documents will include contract language to this effect.

Saint Michael's College – Information Technology will provide a point of contact for the vendor. This contact person will work with the vendor to make certain that the vendor is in compliance with these statutes and policies.

Each vendor will notify the appropriate Saint Michael's College contact person(s) within 48 hours of any vendor employee changes related to work at Saint Michael's College.

Each vendor employee with access to Saint Michael's College confidential and/or sensitive information must be approved to access that information by the data owner of that information.

Any vendor employee who is required to be on site at Saint Michael's College in order to carry out the terms of the contract/agreement is expected to be able to provide adequate identification if requested, and the custodian of the specific information technology resource is expected to take the appropriate steps to verify the authorization for the vendor employee to access that specific resource.

**5.0 Standards and Forms**

- Password Standard
- Third Party Account Application Form
- Colleague Account Application Form

**6.0 Enforcement**

Violation of any of the constraints of this policy or procedures may be subject to discipline as outlined in the employee and student handbooks, or a termination of the contract in the case of contractors or consultants. Additionally, individuals may be subject to loss of Saint Michael's College information resource access privileges, may be subject to legal action, and may also be held financially liable.

The College reserves the right to revoke access privileges at its sole discretion in the event of a threat to network security or a security breach.

Notification of possible violations shall be made to the Helpdesk at 802.654.2020 or to abuse@smcvt.edu.