

Saint Michael's College

Information Security Policy: Access Control Policy

1. 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 SMC resources is based on the role of the individual.

2. Scope:

This policy applies to all users of the SMC network (Mikenet). This includes students, faculty, staff, vendors, visitors, partners, and guests.

3. Policy

- 3.1. 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.
- 3.2. 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.
- 3.3. 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.
- 3.4. 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.
- 3.5. Hard drives of any equipment that is transferred or disposed of will first undergo a Department of Defense level wipe. The machines are randomly audited to make sure the DOD wipe has been successful.
- 3.6. When equipment is transferred to another department, the hard drive will be wiped clean (DOD level) prior to the transfer.

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.