Saint Michael's College

Information Security Policy:
Identification and Authentication Policy

1. Purpose

Saint Michael's College Information Technology department establishes rules for creating, issuing, using, and authenticating electronic identifiers and their corresponding passwords, as well as rules for password complexity.

2. Scope

This policy affects all users of Saint Michael's College technology and information resources: faculty, staff, students, vendors, partners and guests.

3. Policy

Identification and authentication methods will be commensurate with the type of access and the sensitivity of the data involved. The business or department owners or designees for the data area involved will, with input from others, make the decision about the level and type of authentication that will be deployed

- 3.1. Restricted access to physical location may be used for equipment, applications and services where it is important to restrict access to authorized personnel or vendors.
- 3.2. Password protection may be used for applications where access to data or information systems requires individual (personal) identification, and where this single password is sufficient to authenticate this identity. It must be determined that unauthorized access to the data will cause minimal harm to the data, the individual who may be the subject of the data, and the associated Saint Michael's College operation.

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.