Saint Michael's College

Information Security Policy
Incident Response Policy

Policy Owner	Joann Trottier
Related Documents	IT Security Breach Response Procedure, SMC Information Security Incident Response Plan, IT Incident Report Form
Storage Location	Administrative\IT Files\IT POLICIES and PRACTICES\IT Security Policies
Effective Date	July 29, 2007
Next Review Date	November 2015

1.0 Overview

Incident response capabilities are used to monitor for security incidents, determine the magnitude of the threat presented by these incidents, and to respond to these incidents. Without an incident response capability the potential exists that, in the event that a security incident occurs, it will go unnoticed and the magnitude of harm associated with the incident will be significantly greater than if the incident were noted and corrected.

2.0 Purpose

The purpose of this policy is to outline the different responsibilities of the Information Technology department with regards to reacting and responding to various types of network and information security incidents that may occur at Saint Michael's College.

3.0 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

4.0 Policy

4.1. The appropriate compliance officer has the authority to take actions necessary to protect Saint Michael's College people, resources, data and/or communications in the event of a security incident.

4.2. The Information Security Officer and CIO serve as the investigative and operational leads for the conduct of all Saint Michael's College IT information security incident investigations. The Information Security Officer and CIO will be the primary authorities for invoking incident response procedures.

4.3. Various Saint Michael's College departments will provide members of the incident response team to assist with the security incident investigations. All incident response team members will be assigned duties based on the circumstances of the incident.

4.4. Incident response plans will be reviewed periodically.

5.0 Enforcement

Violation of any of the constraints of this policy or procedures will be considered a security breach and 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.

6.0 Review and Measurement

6.1. Date Created: 07/29/07

6.2. Revised On: 11/12/12

6.3. Timing and Frequency of Review: As needed or every three years from prior revision date.

6.4. Metrics:

6.4.1. Number of firewall breaches

6.4.2. Number of incidence reports as compared with number impacting data security

7.0 Standards

7.1. COBIT 5 Management Practice APO13.02, Define and manage an information security risk treatment plan

7.2. COBIT 5 Management Practice DSS05.07, Monitor the infrastructure for security-related events

8.0 Definitions and References

8.1. A Saint Michael's College security incident is defined as an event that exposes Saint Michael's College-held data to unauthorized individuals and impacts or has the potential to negatively impact safety or privacy, or the reputation of Saint Michael's College.

8.2. COBIT 5: Enabling Processes, ©2012 ISACA

8.3. Verizon Enterprise Risk and Incident Sharing (VERIS) Metrics Framework

9.0 Revision History

Version	Change	Author	Date of Change
1	Create	Billie Miles	07/29/07
2	Review & Update	Joann Trottier	11/12/12