

Saint Michael's College

Information Security Policy: Third Party Access Policy

1. Purpose

The purpose of this policy is to establish the rules for granting vendor access to the information technology resources and support services, define vendor responsibilities, and protect Saint Michael's College assets and information. It is expected that this policy will reduce the security and privacy risks and liability associated with granting non-College personnel/organizations access to the College's information technology resources.

2. Scope

There is often a business need for the College to provide vendors and other non-affiliated third parties access to the College's information technology resources. Vendors and other third parties often play an important role in the support of Saint Michael's College information technology resources. Some vendors can remotely view, copy and modify data and audit logs, correct software and operating system problems, monitor and fine tune system performance, monitor hardware performance and errors, modify environmental systems and reset alarm thresholds.

3. Policy

- 3.1. 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.
- 3.2. Prior to granting a vendor or other third-party non-affiliate access to Saint Michael's College information technology resources, the vendor will be required to sign an agreement/contract with the College that specifies:
 - 3.2.1. The Saint Michael's College information technology resource(s) to which the vendor will be granted access
 - 3.2.2. The business purpose for which access is to be granted and limiting access to that purpose
 - 3.2.3. The information the vendor should have access to
 - 3.2.4. A statement indicating that the vendor 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
 - 3.2.5. How the vendor intends to protect the College's information
 - 3.2.6. The acceptable method(s) for the return, destruction or disposal of the College's information in the vendor's possession at the end of the contracted period or completion of the service

- 3.2.7. A statement indicating that any information acquired by the vendor in the course of the contract/agreement cannot be used for the vendor's own purposes or divulged to others
- 3.2.8. 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
- 3.2.9. Vendor will take all reasonable steps, based upon relevant industry standards to protect the College's data/resources from corruption, tampering, or other damage
- 3.3. 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.
- 3.4. 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.
- 3.5. 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.
 - 3.5.1. 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.
 - 3.5.2. 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.
 - 3.5.3. Vendor personnel must report all security incidents directly to Saint Michael's College Safety and Security Office (802) 654-2374. After normal business hours, the vendor can reach Security by dialing '0' from any campus phone.
- 3.6. The CIO and Director of IT have overall responsibility for this policy.

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.