Saint Michael's College

Information Security Policy:
VPN Connection Security Policy

1. Purpose

The purpose of this policy is to establish and communicate requirements for creating and using Virtual Private Network (VPN) connections to and from the Saint Michael's College network in order to ensure that confidential information remains private over non-trusted networks.

2. Scope

The policy applies to both inbound and outbound VPN connections between Saint Michael's College network computing devices and non-Saint Michael's College network computing devices. All VPN connection types are included within the scope of this policy including client-initiated VPN connections and network-initiated VPN connections. This policy applies to all computer devices including personal computers, handheld computers, personal digital assistants (PDA's), smart phones, etc. All persons either who access Saint Michael's College VPN services from external networks or who access external VPN services from Saint Michael's College's network must adhere to this policy.

3. Policy

3.1 Client-to-LAN VPN Requirements

3.1.1 All computers connected to Saint Michael's College networks via VPN or other technologies must be maintained with installations of current operating system security patches per Saint Michael's College's Network Connection Policy and must be protected by active anti-virus software with current virus definitions installed per Saint Michael's College's Anti-virus Policy. By using VPN technology to access Saint Michael's College's network, users must understand that their computers are an extension of the Saint Michael's College network and must, therefore, be configured in accordance with all applicable corporate information security policies.

3.1.2 All persons connecting to Saint Michael's College's network via VPN or other technologies must comply with Saint Michael's College's Acceptable Use Policy.

3.1.3 Client computer devices connected to Saint Michael's College's VPN services will be disconnected from Saint Michael's College's VPN services after a period of inactivity in accordance with designated Saint Michael's College Information Technology (IT) requirements.

3.1.4 Client computer devices connected to Saint Michael's College's VPN services are limited to a maximum connection time in accordance with designated Saint Michael's College IT requirements.

3.1.5 All persons authorized by Saint Michael's College IT to connect a computer device to Saint Michael's College's network via VPN services must prevent other unauthorized persons from physically accessing or using the computer device while the VPN connection is active.

3.1.6 Only VPN client software that is approved by designated Saint Michael's College IT Department may be used to establish VPN connections to Saint Michael's College's VPN services.

3.1.7 Secure access controls must be enabled on Saint Michael's College's VPN services to ensure that only authorized VPN client software is allowed to establish a VPN connection to Saint Michael's College's network.

3.1.8 All persons must authenticate to Saint Michael's College's VPN services before VPN connections are granted.

3.1.9 Authentication credentials used for accessing Saint Michael's College's VPN services must be encrypted during transit over non-trusted networks.

3.1.10 A single VPN network connection is the only network connection that may be active on client computer devices that are connected to Saint Michael's College's VPN services. Additional simultaneous connections to other networks are prohibited, such as dial-up network connections, split-tunnel VPN configuration connections, etc.

3.1.11 All persons approved to connect client computer devices to Saint Michael's College's network via Saint Michael's College's VPN services may be subject to restricted network resource access per their specified business requirements.

3.1.12 Outbound VPN connections from Saint Michael's College's network to external networks are allowed under the following restrictions:

- VPN traffic originating from the remote external network must not be transmitted to Saint Michael's College's internal network. Forwarding or bridging network communications from the remote external network to Saint Michael's College's internal network via the VPN client is strictly prohibited.
- In accordance with Saint Michael's College's Network Security Policy, access control devices placed between Saint Michael's College's internal network and the Internet must be configured to deny connections initiated by Internet hosts directly to internal hosts. Thus, if an outbound VPN connection requires unique network sessions to be established across the Internet from remote VPN network devices to a VPN client located on Saint Michael's College's internal network, then an approved policy exception must be granted.
- In accordance with Saint Michael's College's Network Security Policy, changes required to Saint Michael's College's perimeter access control devices for outbound VPN connections must be approved by designated Saint Michael's College IT staff and must adhere to change control procedures.

3.2 LAN-to-LAN VPN Requirements

3.2.1 Tunnel encryption processes that are enabled between Saint Michael's College LAN-to-LAN VPN endpoints must be initiated with strong passphrases using symmetric or asymmetric key cryptography methods.

3.2.2 Cryptographic keys that initiate tunnel encryption processes between Saint Michael's College LAN-to-LAN VPN endpoints must be encrypted while in transit over non-trusted networks.

3.2.3 Firewall access control devices must be installed and active at Saint Michael's College LAN-to-LAN VPN endpoints in order to allow only authorized network traffic to pass through the VPN end points in accordance with Saint Michael's College's Security 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, vendors, partners, or consultants. 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.

5. Definitions

Access Control Device: A generic term referring to devices that control resource access between networks. Examples of access control devices include access routers, firewalls, content filters, and proxy servers.

Client-to-LAN VPN: Client-to-LAN VPN tunnels are usually initiated by mobile users who want to connect to the college LAN. The connection is initiated by the client with special client software to communicate with the security gateway protecting the destination LAN. Client software can also be hardware based.

Encryption: Encryption is a procedure used in cryptography to encode the contents of a message from plaintext into ciphertext (encrypted data) in order to prevent anyone except the intended recipient from reading the data.

Firewall: An access control device that acts as a barrier between two or more segments of a computer network or overall client/server architecture to protect internal networks or network segments from unauthorized network traffic.

LAN-to-LAN VPN: LAN-to-LAN VPN tunnels consist of a security gateway at each end point which serves as the interface between two LANs over the Internet. Users on either LAN can use the tunnel transparently to communicate with each other.

Non-trusted network: A non-trusted network is a network that is not under Saint Michael's College's administrative control or authority.

Split Tunneling: Split tunneling is a term used in VPN technology to describe a multiple-branch networking path. A tunnel is split when some network traffic is sent to a remote network through a VPN server while other traffic is sent directly to the client network without passing through the VPN server.

Tunnel Encryption: Tunnel encryption is an encryption method for transporting data in which packet and data headers are both encoded in ciphertext.

VPN: Virtual Private Network (VPN) is a collection of computer network services and protocols that use encryption to provide a secure network connection to an otherwise insecure network, such as the Internet.