Michigan Health Information Network
User VPN Account Request Form

Company Requesting VPN: _____

Requester Name: _____ **Phone Number:** _____
Email Address: _____

Who is using the VPN?

VPN User Name: _____ **Phone Number:** _____
Email Address: _____

Company Technical Contact:

Name: _____ **Phone Number:** _____
Email Address: _____

Reason for requesting VPN account:

List the specific systems needing access to the VPN Account.

Duration of requested access:

Begin Date: ___/___/___ **End Date:** ___/___/___

Maximum duration for this request is 1 year.

By signing below, I confirm that I have read and fully understand the MiHIN Virtual Private Network (VPN) policy (Appendix 1) and I consent to the terms and conditions.

Requester Name: _____ **Date:** ___/___/___
(Please Print)

Signature: _____

MiHIN Operations

Approval, Name: _____ **Date:** ___/___/___
(Please Print)

Signature: _____

MiHIN Security

Approval, Name: _____ **Date:** ___/___/___
(Please Print)

Signature _____

Appendix 1

Virtual Private Network (VPN) Policy		Document ID	MDI #00057
		Effective Date	7/23/13
Author	MiHIN	Revision Date	
Owner	Brian Seggie	Revision No.	
Owner – title / dept.	Security Director	Approved by	
Regulatory compliance		Regulation #	
Regulatory compliance		Regulation #	
Regulatory compliance		Regulation #	

Revision history

No.	Date Established (Revised)	Date Executed	Major Contents
0	7/23/13	7/23/13	Policy/Procedure/Checklist Inception
1			
2			
3			
4			

1. Overview

1.1 The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the requesting company's corporate network.

2. System

2.1 The policy applies to all of the company's employees, contractors, consultants, temporaries, and other workers including all personnel affiliates with third parties utilizing VPNs to access or connect to the MiHIN's network or resources.

3. Purpose

3.1 VPN requests must be made via the Michigan Health Information Network VPN Account Request Form.

3.2 The approved company's employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

4. Procedure

4.1 It is the responsibility of VPN account holders with VPN privileges to ensure that unauthorized users are not allowed access to the company's internal networks.

4.2 VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.

4.3 When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.

4.4 Dual (split) tunneling is NOT permitted; only one network connection is allowed.

4.5 VPN gateways will be set up and managed by MiHIN network operational groups.

4.6 All computers connected to the company's internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard; this includes personal computers.

4.7 VPN users will be automatically disconnected from the company's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not allowed used to keep the connection open.

4.8 Users of computers that are not company owned equipment must configure the equipment to comply with the MiHIN's VPN and Acceptable Use (AUP) policies.

4.9 Only approved VPN clients may be used.

4.10 By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the company's network, and as such are subject to the same rules and regulations that apply to the company's owned equipment, i.e., their machines must be configured to comply with Security policies including Acceptable Use Policy (AUP).

5. Enforcement

5.1 All VPN connections are subject to monitoring and inspection for violation of policy

5.2 This connection is only to be utilized for the exact purpose as described in the requesting form. Any deviation from the requested activity is a violation of the VPN policy.

5.3 Failure to meet any of the requirements of this policy is subject to immediate termination of VPN privileges and possible disciplinary action up to and including termination of employment or contract.

6. Definitions

MIHIN- "Michigan Health Information Network Shared Services" and its other names (d/b/a's) under which it does business.

VPN – Virtual Private Networks offer secure communications between network applications using a public or unsecured medium such as the Internet through the use of various technologies offering secure user authentication, date integrity, data confidentiality, and access control.

7. Related Links

None