	Maryland Institute for Emergency Medical Services Systems		
	Policy: Remote Access Policy		
	Originator: Information Technology		
	Policy Number	Effective Date	Revision Date
	137.07	August 3, 2015	N/A

MIEMSS permits and/or requires staff to work from remote locations other than their assigned work site. In order for an employee working from a remote location to access agency network resources, such as files, applications and databases, the agency provides a specific, secure, method to connect to the agency network. The method provided by the agency is known as a Virtual Private Network (VPN) connection. MIEMSS utilizes Cisco's "AnyConnect" VPN software for this purpose; no other remote software is supported or will be allowed. With this software, a user can securely access agency network resources from anywhere there is internet access.

1) VPN Guidelines

a) VPN access should be used over a secure, password protected connection such as a home office or other password protected internet service provider connectivity.
   i. VPN access should not be used on publicly available Wi-Fi such as those networks available at coffee shops, stores, libraries and other public locations.

b) In general, the agency provided VPN software will only be installed and utilized on devices provided by MIEMSS, e.g., workstations/laptops/smart phones, etc.
   i) Special permission is required to use the VPN on non-agency issued equipment. This need should be included on the Remote Access Request.
      (1) Users who may be permitted to use non-agency devices are required to meet additional security requirements. Requirement include using a MIEMSS supported operating system, apply software updates and enabling automatic updates, connecting to a secure network, enabling personal firewall, use of Antivirus/Antispyware Software, using secure web browsers, and applying power off and lock settings.

c) While utilizing the VPN users are required to follow the MIEMSS Information Security Policy 137.08 (Draft Version)

d) Using the VPN is effectively being at work. It should only be used for business use, and access should not be shared with anyone. All activities conducted via VPN will be seen as activities occurring on the MIEMSS network and subject to MIEMSS policies, State laws, regulations.

e) It is strongly encouraged that users access their desktop via VPN and Remote Desktop Connection (RDC) and conduct work on their agency located workstation and avoid downloading and working on documents on remote, non-agency equipment.

f) Screens must be locked when a workstation is unattended at any time.

g) When work related duties are completed, the VPN must be disconnected.

h) For any questions concerning security or privacy, or problems accessing the service, contact your supervisor or the Help Desk (computersupport@miemss.org).

i) Permitted VPN access may be revoked at any time.

j) Misuse of the VPN may result in revocation of VPN access and/or disciplinary action.

2) Requesting Remote Access Authorization.
   a) MIEMSS employees requesting remote access shall complete the MIEMSS Remote Access Request Form (Attachment A) and submit it to their immediate supervisor.
   b) The immediate supervisor shall review the form with the employee and either approve or deny the request. After completing the form the supervisor shall forward the form to the MIEMSS Information Security Officer.
      i) If the request is denied, the supervisor shall include justification for the denial.
   c) The MIEMSS Information Security Officer shall review the form and approve or deny the request. After approving the MIEMSS Information Security Officer shall forward the form to the Director of Information Technology.
      i) If the request is denied, the Information Security Officer shall include justification for the denial and return to the employee's supervisor. The Information Security Officer and employee's supervisor shall discuss the reason for the denial.
   d) The Director of Information Technology will provide the VPN connection to the employee, sign the form and then send it to the MIEMSS Human Resources (HR) Officer.
   e) The HR Officer shall place the completed form in the employee's personnel file.

Public/Private Designation: Public - This document is approved for publication and unrestricted distribution.

Policy approved by MIEMSS on August 4, 2015:

Kevin G. Seaman, MD, FACEP
Executive Director

Maryland Institute for Emergency Medical Services Systems		
Policy: Remote Access Policy		
Originator: Information Technology		
Policy Number	Effective Date	Revision Date
137.07	August 3, 2015	N/A

Attachment A

MIEMSS Remote Access Request Form

Employee Name: _____

Department: _____

Immediate Supervisor: _____

Reason for requesting remote access:

_____

_____

_____

Employee's Immediate Supervisor

Before approving the Remote Access Request the supervisor shall ensure the employee has read and understands the Remote Access Policy. This form shall be re-acknowledged on an annual basis. A copy of the policy may be attained at: http://www.miemss.org/home/Staff/tabid/200/Default.aspx

I ❑concur / ❑do not concur with the employee's need for remote access

If denied, reason for denial.

_____

_____

_____

Information Security Officer Acknowledgement

I ❑concur / ❑do not concur with the employee's need for remote access

If denied, reason for denial.

_____

_____

_____

_____
Name

_____ _____
Signature Date Received

Director of Information Technology

Remote access credential issued. (Serial # _____)

_____ _____
Name Date Received

Date: 7/15/2015, Version 1.0