University of Massachusetts Lowell

Policy Title:	VPN Policy
Policy Number:	IT-5-124
Effective As Of:	10/1/2016
Next Review Date:	10/1/2017
Responsible Office:	Information Technology
Responsible Position:	Information Security Officer

I. POLICY STATEMENT

UMass Lowell employees, students and authorized third parties (vendors, etc.) shall utilize the University's approved VPN product for remote access to campus electronic information resources. All approved users are subject to the UMass Lowell Acceptable Use Policy and Information Security Policy.

II. PURPOSE

The purpose of this Policy is to provide guidelines for Virtual Private Network (VPN) connections to the UMass Lowell trusted administrative network.

III. SCOPE

This Policy applies to all UMass Lowell authorized employees, students, contractors, consultants, temporaries, including all personnel affiliated with third parties utilizing VPN to access the UMass Lowell trusted network.

IV. DEFINITIONS

Electronic Information Resources: include data, networks, computers, and other devices that store or display data, communications and transmission devices, and software used on such devices.

VPN - Virtual Private Network, a way to extend the corporate/production (trusted) network using authentication and encryption.

V. PROCEDURES

General Requirements:

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to UMass Lowell internal networks via their VPN.

2. VPN use is to be controlled using password authentication. When actively connected to the administrative network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.

3. All VPN connections will utilize two factor authentication (2FA) upon login.

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

5. VPN gateways will be configured and managed by the UMass Lowell IT office.

6. All computers connected to UMass Lowell internal networks via VPN must use the most up-to-date anti-virus software in accordance with the UMass Lowell Antivirus Standard. This includes university-owed and personally-owned computers.

7. All computers connected to UMass Lowell internal networks via VPN must have the latest operating system security patches applied. Only supported Operating System releases from the manufacturer are allowed to connect via VPN.

8. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of UMass Lowell's network, and as such are subject to the same policies that apply to UMass Lowell-owned equipment, i.e., their machines must be configured to comply with all UMass Lowell Security Policies. All approved users are subject to the provisions as stated in the UMass Lowell Acceptable Use Policy.

VI. RESPONSIBILTY

Information Technology is the responsible organization for implementing the provisions of this policy. The University's Chief Information Officer and the Information Security Officer are the designated point of contacts.

VII. ATTACHMENTS

None

VIII. RELATED POLICES, PRODEDURES AND ANNOUNCEMENTS

Acceptable Use Policy, IT-5-101
Information Security Policy, IT-5-111 (reserved)
Remote Access Policy, IT-5-125 (reserved)

IX. APPROVAL AND EFFECTIVE DATE

On file with the Policy Office.