Manhattanville College

VPN Access & Usage Policy

The Manhattanville College Virtual Private Network (VPN) is provided for authorized faculty, staff and third parties (customers, vendors, etc.). Remote use requires a connection to the Internet which is not provided by the College. Requests for service must be forwarded to IT by the individual's manager by contacting the Support Center and providing the authorization form with the request. Individuals must be prepared to provide demonstrated need for remote VPN access prior to contacting their manager or IT. No reasonable request will be refused, but the process is required to balance limited connectivity with legitimate need.

It is the responsibility of those with VPN privileges to ensure that unauthorized users are not allowed to access College internal networks. When actively connected to the College network, the VPN will force all traffic to and from your workstation over the VPN tunnel: all other traffic will be dropped. Dual (split) tunneling is NOT permitted; only one network connection is allowed. When the user has completed accessing the College network, they must end the VPN session prior to normal web access.

VPN gateways/concentrators will be set up and managed only by IT. All computers connected to College internal networks via VPN or any other technology must use properly configured, up-to-date anti-virus software including all personally owned computers. IT reserves the right to configure the VPN concentrator to limit connection times to normal business hours or as determined by demonstrated need. Users of computers that are not College-owned equipment must configure the equipment to comply with all College VPN and technology policies. By using VPN technology with personal equipment, users acknowledge that their machines are a de facto extension of the College network, and as such are subject to the same acceptable use policy that applies to College-owned equipment. Therefore all such systems must be configured to comply with College security policies. Any exceptions to this Policy must be approved in writing by IT. Any security breech that is the result of a violation of this policy will be cause for disciplinary action per the Acceptable Use Policy. IT reserves the right to restrict any device or connection that does not comply with this policy.