QUINCY COLLEGE
PLYMOUTH, QUINCY & ONLINE

Remote Access Policy

1. Overview

Remote access to our corporate network is essential to maintain user productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our network. While these remote networks are beyond the control of Quincy College, we must mitigate these external risks the best of our ability.

2. Purpose

The purpose of this policy is to define rules and requirements for connecting to Quincy College's network from any host. These rules and requirements are designed to minimize the potential exposure to Quincy College from damages which may result from unauthorized use of Quincy College resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Quincy College internal systems, and fines or other financial liabilities incurred as a result of those losses.

3. Scope

This policy applies to all Quincy College employees, contractors, vendors and agents with a Quincy College-owned or personally-owned computer or workstation used to connect to the Quincy College network. This policy applies to remote access connections used to do work on behalf of Quincy College, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to Quincy College networks.

4. Policy

It is the responsibility of Quincy College employees, contractors, vendors and agents with remote access privileges to Quincy College's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Quincy College.

General access to the Internet for recreational use through the Quincy College network is strictly limited to Quincy College employees, contractors, vendors and agents (hereafter referred to as "Authorized Users"). When accessing the Quincy College network from a personal computer, Authorized Users are responsible for preventing access to any Quincy College computer resources or data by non-Authorized Users. Performance of illegal activities through the Quincy College network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. For further information and definitions, see the *Acceptable Use Policy*.

Authorized Users will not use Quincy College networks to access the Internet for outside business interests.

4.1 Requirements

4.1.1 Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see the *Password Policy*.

4.1.2 Authorized Users shall protect their login and password, even from family members.

4.1.3 While using a Quincy College-owned computer to remotely connect to Quincy College's network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

4.1.4 Use of external resources to conduct Quincy College business must be approved in advance by Information Technology and the appropriate department supervisor.

4.1.5 All hosts that are connected to Quincy College internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers.

5. Policy Compliance

5.1 Compliance Measurement

The Information Technology department will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and inspection, and will provide feedback to the policy owner and appropriate business unit manager.

5.2 Exceptions

Any exception to the policy must be approved by Remote Access Services and the Infosec Team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.