Remote Access Policy

1.0 Overview

Remote access to technical resources via VPN (Virtual Private Network) has been commonplace for several years now. Typically, a remote user connecting from home or anywhere outside the campus network uses a broadband provider such as Comcast or Verizon and is on the provider's network. By invoking the VPN software, which requires user authentication with College credentials, the remote computer is made to appear as though it is on the Wellesley College network. As a result, the computer from home will have very similar access to the technical services that a computer on the College network has.

This policy is necessary because we have an obligation to protect College resources and we have very little knowledge of the remote computer and how secure it is.

2.0 Purpose

The purpose of this policy is to define standards for connecting to the Wellesley College network from any host. These standards are designed to minimize the potential threat to Wellesley College information technology resources and thereby protect secure college data.

3.0 Scope

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

4.0 Policy

4.1 Responsibilities

It is the responsibility of Wellesley College employees, contractors, vendors and agents with remote access privileges to Wellesley College's network to ensure that their remote access connection is given the same consideration as the user's on-site connection. It also their responsibility to protect their user credentials to prevent unauthorized users from accessing the Wellesley College network. Any user authorized with remote access bears responsibility for the consequences should the access be misused.

4.2 Requirements

Secure remote access must be strictly controlled. Control will be enforced via domain password authentication. For information on creating a strong domain password see Wellesley College's Password Guidelines.

The login page for the VPN will state explicitly the responsibilities of the user, specifically the need to keep the operating systems, and virus protection and malware protection software updated on the remote computer. The page will also provide a link to the Wellesley College Acceptable Use Policy, which outlines general responsibilities a user must follow when accessing the network, whether remotely or on campus.

At no time should any Wellesley College employee provide their login or email password to anyone, including family members. Wellesley College employees and contractors with remote access privileges must ensure that their Wellesley College-owned or personal computer or workstation, which is remotely connected to the Wellesley College network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

4.3 Additional Requirements for Accessing Secure Data Remotely

There is a group of users who have access to sensitive data such as personally identifiable information about others. In order to access such data remotely, they will be required to attend a mandatory training session conducted by Library & Technology Services (LTS) and sign a statement agreeing to the WISP (Written Information Security Program) as required by the Commonwealth of Massachusetts. During the training, LTS will train the users on: security best practices such as not downloading spreadsheets or documents to their home computers that contain sensitive data unless absolutely necessary; the use of secure deletion software to delete files containing such data from their computers when they are ready to be removed; and their responsibility to inform LTS if such data were compromised in any way.

5.0 Enforcement

Failure to abide by the responsibilities outlined in this policy will result in the user's remote access capability being revoked until they produce proof that the problems have been remedied. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Policies Cross-Referenced

Acceptable Use Policy
Administrative Handbook
Copyright Policy
Employee Confidentiality Policy
Faculty Handbook
Google Apps for Education Agreement
Guidelines on Student Education Records
HIPAA Privacy Policy (policy under revision)
Password Guidelines
Policy Against Sexual Harassment and Unlawful Discrimination
Policy on Hateful Incidents (policy under revision)
Student Handbook
Written Information Security Program

7.0 Effective Date

Revised 5/11/2011