Remote Access Policy

Overview

The Patchogue-Medford Library has determined that remote access to our networks and/or computers is necessary and appropriate to maintain the Library's productivity. In many cases, however, this remote access originates from networks that the Library does not control. While these remote networks are beyond the control of the Library, this policy serves to mitigate external risks to the best of the Library's ability.

The purpose of this policy is to define rules and requirements for connecting to the Library's networks and/or computers from any host. These rules and requirements are designed to minimize the potential exposure to the Library from damages which may result from unauthorized use of the Library's resources. Damages include the loss of sensitive or confidential data, damage to public image, damage to critical Library internal systems, and "breaches of the security of the system," as defined in the Information Breach Notification Policy.

Scope

This policy applies to all Library employees, with a Library-owned or personally-owned computer or workstation which is used to remotely connect to the Library's computers and/or networks. This policy applies to remote access connections used to do work on behalf of the Library, including reading or sending email, viewing intranet web resources, and accessing Library programs and/or systems. This policy covers any and all technical implementations of remote access used to connect to the Library's networks.

Only Library employees who obtain prior authorization from the Director may access the Library's networks and/or computers remotely. It is the responsibility of Library's employees with remote access privileges to the Library's networks and/or computers to ensure that their remote access connection is given the same security considerations as the user's on-site connection to the Library.

General access to the internet for recreational use and/or for outside business interests through the Library's network is strictly prohibited. When accessing the Library's network from a personal computer, employees with remote access privileges are responsible for preventing access to any Library's computer resources or data by unauthorized users.

Requirements

Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases consisting of at least 6 characters that are a combination of upper and lower case letters, numbers and characters.

Employees with remote access privileges shall protect their login and password from all persons, including family members.

When remotely connecting to the Library's computers and/or network, employees with remote access privileges 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.

Use of external resources to conduct Library business must be approved in advance by the Director.

All hosts that are connected to the Library's computers and/or networks via remote access technologies must use the most up-to-date anti-virus software at its disposal, this includes personal computers.

Personal equipment used to connect to the Library's networks must meet the requirements of the Library's equipment for remote access.

When accessing the Library's computers and/or networks remotely, employees must abide by all Library policies, including but not limited to the Library's Employee Email, Computer Usage and Social Networking policy.

In the event an employee believes that Library information may have been compromised, the employee must make a report to the Director immediately so that the District may determine if an investigation under the Information Breach Notification Policy is warranted and/or whether any other mitigating measures are necessary.

Any exception to the policy must be approved by the Director in advance.

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

Adopted by the Board of Trustees: March 20, 2019