REMOTE ACCESS TO COMPUTER NETWORK

The purpose of this policy is to establish standards for connecting to the Patchogue-Medford UFSD network from any external host. These standards are designed to minimize the potential exposure to the district from damages that may result from unauthorized use of Patchogue-Medford resources. Damages include the loss of sensitive or organization confidential data, intellectual property, damage to public image, or damage to Patchogue-Medford internal systems.

This policy applies to all Patchogue-Medford employees, contractors, vendors and agents with a Patchogue-Medford-owned or personally-owned computer or workstation used to connect to the Patchogue-Medford network. This policy applies to remote access connections used to do work on behalf of Patchogue-Medford. Remote access implementations that are covered by this policy include, but are not limited to, VPN (Virtual Private Network), RDP (Remote Desktop Protocol), or similar remote access software.

It is the responsibility of Patchogue-Medford employees, contractors, vendors and agents with remote access privileges to Patchogue-Medford's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Patchogue-Medford. Remote access usage shall not violate any Patchogue-Medford policies, perform illegal activities, or be used for outside business interests.

End-users interested in obtaining remote access privileges shall contact the Executive Director of Technology for consideration and be authorized by the Superintendent or his/her designee. Each request for remote access will be evaluated on a case-by-case basis. A Remote Access Agreement (see Exhibits A and B) must be signed and submitted prior to access being granted.

Secure remote access will be strictly controlled. Control will be enforced via multi-factor authentification. At no time should any Patchogue-Medford employee or vendor provide login or email password to anyone. All hosts connected to Patchogue-Medford internal networks via remote access technologies must use the most up-to-date anti-virus/spyware software. This includes personal computers.

The internal claims auditor will review the VPN access logs on a monthly basis. The Business Office will provide these reports to the Board of Education in accordance with indicated agenda review deadlines. Any exceptions will be reported to the Board and Assistant Superintendent of Business and Operations, or designee.

Any employee, contractor or vendor found to have violated this policy shall have remote access rights revoked and may be subject to disciplinary action, up to and including termination of employment or contract as applicable. Restoration of remote access rights will occur on a case-by-case basis in consultation with the employee's supervisor and other authorities as needed. Vendors accessing the Patchogue-Medford network shall be subject to having access rights revoked with no liability on the District's part.

Adopted:
April 15, 2013
Revised:
February 26, 2018

Remote Access to Computer Network (Continued)

Revised:
June 29, 2020
Revised:
January 23, 2023
Revised:
August 21, 2023
Revised:
September 16, 2024
Reviewed:

Exhibit A

Remote Access to Computer Network

INDIVIDUAL CONFIDENTIALITY AND REMOTE ACCESS AGREEMENT

Please print or type:

Company: _____

Individual to be given access: _____

Primary contact person for this individual at Patchogue-Medford Union Free School District: _____

I am employed by (or work under contract with) the Company listed above, and in order to perform my work for the Company I will require access to the computer system of Patchogue-Medford Union Free School District ("Patchogue-Medford"). As a condition of being allowed such access, I agree that:

- I will use only the log-in ID assigned to me by Patchogue-Medford when logging on to Patchogue-Medford's computer system;
- I will log-off Patchogue-Medford's system immediately upon completion of each session of service;
- I will not allow other individuals to access Patchogue-Medford's computer system;
- I will keep strictly confidential the log-in ID and all other information that enables such access;
- I will not intentionally access any information or data other than that which I have been specifically authorized to access by Patchogue-Medford;
- I will not simultaneously access the Internet or any other third-party network while logged on to Patchogue-Medford's computer system;
- My access to Patchogue-Medford's computer system is subject to monitoring by Patchogue-Medford;
- I will not make any change to any of Patchogue-Medford's systems without Patchogue-Medford's prior written approval for the specific change.

I also agree to keep strictly confidential all information to which I have access or which I otherwise acquire. I agree that I will not, directly or indirectly, disclose any Patchogue-Medford information to any person except specified personnel of Patchogue-Medford and others providing services relating to Patchogue-Medford who have a need to know to fulfill their job responsibilities and business obligations and have undertaken a similar confidentiality obligation. I agree that I will not appropriate any information to my own use or to the use of any other person or entity. I further agree not to remove any information from Patchogue-Medford's premises or systems without express permission from the individual named above as "Primary contact person for this individual at Patchogue-Medford", or that person's delegate.

By signing below, I agree to be personally bound by this agreement.

_____ _____

Signature of individual to be given access Date

After completing this form, please submit to Patchogue-Medford UFSD, Attention: James Richroath at jrichroath@pmschools.org or cpantina@pmchools.org

Exhibit B

Remote Access to Computer Network

USER ACCESS DETAILS

This form is to be completed and retained by the Technology Department, alongside a copy of the signed Remote Access Agreement.

USER INFORMATION:

Name: _____

Title: _____ Company: _____

ACCESS DETAILS:

Reason for Access: _____

_____

Server/s:_____

Network IP or Range: _____

Applications: _____

Notes:

****

Activation Date: _____ De-Activation Date: _____

Completed by:_____ Date:_____