VPN Account Request Form/Policy - Administrative Staff

Directions: Fill out ***both*** pages of this form, submit for signatures, and return completed form to **Account Administrator, Tiffany Halbert (halbert@cpsboe.k12.oh.us)** *All fields are required.*

Please note that this form must be signed by the director of the department requesting VPN access.

VPN User Information – CPS Administrator			
Name			
School or Department Name			
School or Department Address			
VPN User Phone Number			
VPN User Email Address			
Date VPN access is required		Date VPN access will no longer be required	
Purpose for using CPS VPN access			
1. What anti-virus software are you running?			
2. How does your anti-virus software download current virus definition (dat) files? Are they pushed out by your company (managed) or does it go to the internet for updates (un-managed)?			
3. Please describe the process you follow for updating your machine with patches from Microsoft:			
Department Director Approval (for Principals, Director of Schools is Department Director)			
Name			
Signature			
Date			

VPN Users also need to sign and submit page 2 of this form. Both pages of the form should be submitted together.

Office Use Only:

CIO (initial)	
Date	

VPN Remote Access Policy

1.0 Purpose

The purpose of this policy is to define standards for connecting to Cincinnati Public Schools' network from any host. These standards are designed to minimize the potential exposure to Cincinnati Public Schools from damages which may result from unauthorized use of Cincinnati Public Schools resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image and damage to critical Cincinnati Public Schools internal systems.

2.0 Scope

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

3.0 Policy

3.1 General

1. It is the responsibility of Cincinnati Public Schools employees, contractors, vendors and agents with remote access privileges to Cincinnati Public Schools' corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to CPS.
2. In the case that an associate or family member inadvertently uses the CPS VPN connection the Cincinnati Public Schools employee, contractor or vendor is responsible to ensure the associate or family member does not violate any Cincinnati Public Schools policies, does not perform illegal activities, and does not use the access for outside business interests. The Cincinnati Public Schools employee, contractor or vendor bears responsibility for the consequences should this access be misused.

3.2 Requirements

1. Secure remote access must be strictly controlled.
2. At no time should any Cincinnati Public Schools employee, contractor or vendor provide their login or password to anyone, not even family members.
3. Cincinnati Public Schools employees and contractors with remote access privileges must ensure that their Cincinnati Public Schools-owned or personal computer or workstation, which is remotely connected to Cincinnati Public School's corporate 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. Cincinnati Public Schools employees, vendors and contractors with remote access privileges to Cincinnati Public School's corporate network must not use non-Cincinnati Public Schools email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct Cincinnati Public Schools business, thereby ensuring that official business is never confused with personal business.
5. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
6. All hosts that are connected to Cincinnati Public Schools internal networks via remote access technologies must use the most up-to-date anti-virus software. This includes personal computers.
7. Personal equipment that is used to connect to Cincinnati Public School's networks must meet the requirements of Cincinnati Public Schools-owned equipment for remote access available here: http://support.cps-k12.org/hardware software/index.html
8. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Cincinnati Public Schools production network must obtain prior written approval from Information Technology Management, Infrastructure Group.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and removal of remote access privileges.

I understand and agree to these terms.

Name of VPN User	
Signature of VPN User	
Date	

This page should accompany page 1 of the form.