UPWARD technology

Home User Support Policy

With todays distributed workforce, more and more of our customers are working from home and blurring the lines between their personal and professional digital devices. Not surprisingly, we are being asked more and more to help users connect their personal or home devices to work resources. As you might imagine, working on users unmanaged personal devices can open up quite a can of worms for us, and clear expectations are critical!

Here are our best practices and policies regarding this facet of supporting you:

Risk Management:

One of the three 'pillars' of our service is to ensure we help you manage your risk related to IT. You remember the old metaphor – "a chain is only as strong as it's weakest link." If you apply this to your business IT security, a home based computer can be a very 'weak link.'

In our research, approximately 80% of home PC's and devices do not have up to date security. If you allow access to your company's data from infected or compromised devices, your risk of loss goes up very quickly.

Home Users will be broken into two categories:

Remote Office User

For employees who regularly work from home to get their jobs done, we suggest the home environment gets set up as an extension of your primary business network. The computer in this Remote Office should be a company-owned asset. Additionally, this setup requires a SOHO (Small or Home Office) firewall provided by Upward that enforces the same security policies as your office. The device can be configured to operate all applications and with the same

The computer will be managed to the same standards as any other device in your environment, covered under our Emerging Plan. This means Anti-virus, Anti-Malware, updates, password policies, & company standards will be proactively managed and supported for $35/device/mo. All troubleshooting and break/fix work will be chargeable on these devices at a rate of $110/hour.

Home User

For users who occasionally log into the work network from a home device, Upward will support the user on a chargeable basis only. This includes the installation of VPN software, troubleshooting and any initial or future troubleshooting or break/fix support. This will be chargeable at $110/hour. We insist that any user connecting from a personal device to the work network utilize Remote Desktop Protocol (RDP) to access their designated work device. Upward will provide training on these best practices during setup and configuration of a VPN agent for the home user.

Companies should own their devices whenever possible.

The best practice for any company is to own the devices they intend their employees to use to get their jobs done. For a variety of reasons this avoids ambiguity about what is “theirs” and “ours” and allows for tighter controls of intellectual property and risk mitigation strategies.

Modern laptops are as powerful as desktops and can easily connect to desktop monitors and keyboards via a docking station, these are recommended in lieiu of personal devices whenever possible. Most companies should also budget for a spare machine.

As always, we will fully support a company-owned asset and all functionality related to using it.

Upward accepts no liability for any problems that occur. (we can’t say this)

Unlike your work network, we have very little control over your personal network (where you browse, what you store on the device, printers you use, etc.), so we accept no liability for anything that might happen to the data or performance of the device. All files stored on the machines should be backed up regularly. Backup and disaster recovery is not a service provided by Upward for home users (users can always save files to their work server via the VPN)

There are security risks with connecting unmanaged devices to the company network

There are some important risks for you to be aware of as a business owner:

- Malware or viruses on the home PC can be transmitted to your network.
- If the machine is lost or stolen, work data may be compromised. Once data begins transferring to and from outside networks, your liability as a business owner goes up.
- Upon termination, you may have no way of ascertaining what data the user has kept.

There are numerous security solutions to mitigate risk that concerned business owners can leverage to further protect their businesses:

1. Home network firewall- The personal or SOHO (small or home office) grade firewall will provide advanced filtering and malware protection for home users, as well as establish a permanent and secure, encrypted connection to the work network.
2. Cloud file management- For some companies, we can create a web-based file sharing site that can be used instead of a file-server.
3. Enterprise Mobility Suite- This is an advanced suite of services created by Microsoft that allows companies to clearly define what is work vs personal, then enact tight controls over their intellectual property.
4. BitLocker- This advanced encryption software will help protect the data on a PC if it is lost or stolen. It comes free with most PC’s, but there are implications for enabling it that should be discussed.

5. AuthAnvil- This is an advanced password vault application, that can allow companies to intelligently manage passwords across all users. It makes changing passwords easy if a user leaves.

After-Hours charges will apply to support needs outside of our regular business hours of 8-5 M-F.

Please let us know if there is anything we can do to support your business!