Working from Home Checklist

Firewall

Ensure that you have a firewall between any of your devices and the Internet. While your network router should include one, it is good practice to enable the firewall on your device, either the one supplied by Windows or your antivirus solution.

If you use a laptop computer and use it to connect to public networks, the firewall must be enabled. Hillsdale laptop computers all have the firewall enabled by default.

Antivirus

Having a good antivirus product installed is a policy requirement if you connect to the Hillsdale network and a good idea in general. Antivirus software isn't 100% foolproof – it's always one step behind the hackers attempting to break into your systems – so you will still need to be careful about any websites you browse or emails that you open.

Exercise caution and check the provenance before inserting an external input source, like a CD/DVD or a USB storage device. If you absolutely need to use external input sources, your antivirus software should be set up to scan these sources. Avoid connecting any external sources or devices as much as possible.

Connection Mechanism

When working from home, you will need to securely connect to the Hillsdale network; you can do so via a Virtual Private Network (VPN) or RDWeb. The procedure to set up access is available from the IT or Office Management Teams. Either method allows you to connect to the Hillsdale network via internet in a way that is safe and secure.

All remote access to the Hillsdale network requires two-factor authentication.

Two Factor Authentication

Regardless of how you connect to the Hillsdale network you have to confirm your connection with a second device in addition to entering your password. You must communicate with the IT Team to enable your device.

Wifi Or Wired Home Connections

If possible, it is best for both performance and security to have a wired connection between your home device and your Internet Service Provider (ISP)'s gateway. However, because of location or other factors that may not always be possible.

If you connect to the Internet via Wifi, then you must take steps to ensure that the connection is secure.

At a minimum, you must ensure that:

- The Wifi password used to secure your wireless network using the WPA2 or later protocol is a **strong password with 8 characters and including at least one number or symbol in it**. Do not use the WEP protocol or leave your Wifi access unsecured (without a password).
- You have changed your Wifi router's Administrator password and use a strong password (as described above).
- If your router allows remote management, disable it, i.e. do not allow it to be managed via Wifi.

You should avoid using personal information in your Wifi network name, also known as the SSID (Service Set Identifier).