TIP SHEET

Cybersecurity and remote work during the pandemic

COVID-19 forced millions of workers to shift to a remote environment — this could potentially introduce new risks to your system. While already working remotely, you can still take several steps to secure your network and business data.

Communicate a single source of truth

Cybersecurity is every one's responsibility. Distribute your remote work policy and cybersecurity best practices to encourage all employees to maintain the integrity of your network.

Secure WiFi connections

Ensure that everyone's wireless connection is properly encrypted: turn on full encryption from all wireless access points and set up strong passwords.

Secure cloud-based services

If your employees are taking advantage of cloud-based tools, such as Microsoft OneDrive or Dropbox, make sure to enable the paid versions — these have better protection than the free ones.

Set up two-factor authentication and encryption

One strong password isn't enough. Set up two-factor authentication methods (such as a secondary email or a cellphone) to verify your identity. Verify you're encrypting files and backing up data.

Ensure operating systems are fully patched

If you are notified of an update (i.e. Windows update), it's often because the provider has identified bugs or vulnerabilities. Upgrade to the latest version and enable automatic patching.

Reintegrating

Seize this opportunity to automate manual processes. You may find that critical processes which "worked just fine" manually suddenly become a lot more cumbersome when performed across a virtual workspace or between remote teammates.