REMOTE WORKING GUIDELINES FOR SMBs

IT admin's guide to securing remote workforce

As the COVID-19 pandemic forces many employees to work from home, can your organization stay productive — and safe? Many high-profile companies such as Google and Microsoft are encouraging this shift without any major setbacks. For many smaller companies and organizations, however, the situation is likely to be very different.

Remote working is probably limited to a few, and realistically mainly for email and other non-operational systems. How to make sure the infrastructure and policies are all in place to ensure business continuity?

Basic requirements

First of all, in order to stay productive, there are some common requirements that all remote workers need.

- A computer
- A good internet connection
- Chat and conferencing applications
- A dedicated workspace (preferred)
- Optionally, a phone
- Self-motivation and discipline
- A strict routine

Apart from the usual setup, companies and organizations also need to prepare themselves and their employees for the **increased cybersecurity risks** associated with remote working.

What are some of the challenges that need to be addressed?

1. Physical security of company devices
2. Company IT security when employees are home
3. What's in the home technology environment
4. Accessing the company network and systems
5. Collaborative tools and authorization processes
6. Cybersecurity training
7. Support and crisis management

1 Physical security of company devices

Employees will be exposing company devices to greater risk as they leave the safety and security of the workplace. Devices therefore need to be protected against loss and theft. Here are some key measures and tips on how to make sure all devices remain secured.

- **Log out when not in use** — both at home and in public places. An inquisitive child accidentally sending an email to the boss or a customer is easily prevented, as is limiting the opportunity for someone to access the machine while your back is turned in the local coffee shop.
- **Strong password policy** — set inactivity timeouts and ban sticky notes with passwords on them (yes, people still do this).
- **Never leave the device unattended** or on public display. If it's in the car, then it should be in the trunk.

PRO TIP

Full-disk encryption is a simple yet powerful solution ensuring that even if the device falls into the wrong hands, the company's data is not accessible.

2 Company IT security when employees are home

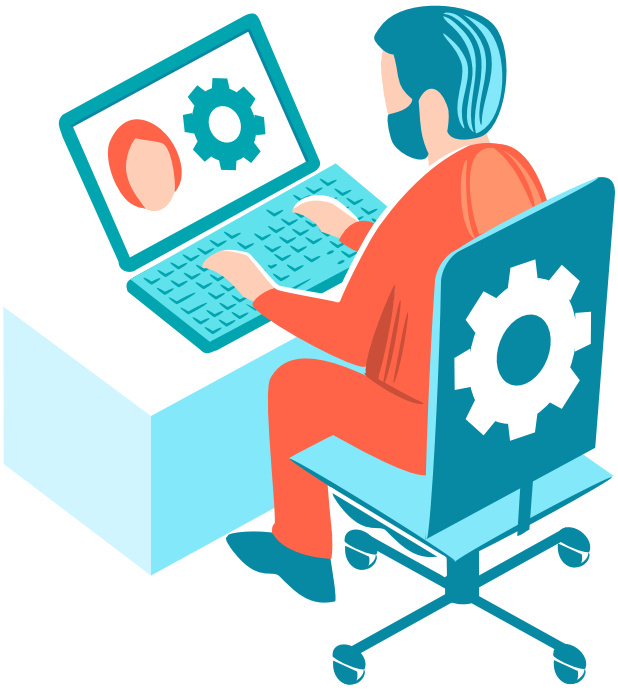
Now that employees are on their own in their homes, you have limited visibility to what is going on, especially if you are not used to manage and monitor devices remotely. Now is a good time to learn all the benefits of remote management and significantly lower the number of IT issues you will have to deal with anyway.

Using remote management will save your time:

- Easily configure and maintain all machines systems up to date. At once, without going from one to another.
- Schedule tasks, define policies and execute them by different groups of employees.
- Get notifications about incidents in real time so you can act immediately when incident occurs.

PRO TIP

If you're up to 250 devices, you can easily manage the network of computers via cloud-based console. Its activation takes only a few minutes.



3 What's in the home technology environment

Ask employees to audit their own home environment for vulnerabilities, before connecting work devices. There are continual disclosures regarding vulnerable Internet of Things (IoT) devices, and this is an excellent time for employees to take action on securing them with strong passwords and updating their firmware/software to the latest version.

Consider promoting, or even mandating, the use of a connected home monitoring app before allowing work devices to be connected to home networks. The scan or monitoring will highlight devices with known vulnerabilities, outdated software or firmware, or default passwords that need to be changed.

4 Accessing the company network and systems

Establish if the employee needs access to the organization's internal network or just access to cloud-based services and email. And take into consideration whether the same level of access to sensitive data enjoyed on-site should be granted when the employee is off-site.

If access to the organization's internal network is needed:

- It is strongly recommended to use only organization-owned devices so that full control of the connecting device is under the management of the technology security and IT team.
- Always **use a VPN to connect remote workers** to the organization's internal network. This prevents man-in-the-middle attacks from remote locations. Remember that since you're now working from home, the traffic is now flowing over public networks.
- **Control the use of external devices** such as USB storage and peripheral devices
- With many people working from home, they are becoming targets of scams or phishing emails. You can **keep suspicious emails off the limits** of employee machines with cloud-sandboxing solutions.
- Limit the ability to store, download or copy data. A data breach can happen from any device that contains sensitive company data.
- Consider the use of virtual machines to provide access. This may be more complex to set up but could be a superior longer-term solution.

In case some (or all) of your employees use BYOD (their personal) devices, make sure that if you allow them access to email and cloud services, you enforce the same endpoint security policy for antimalware, firewalls, etc. as with an organization-managed device. **If necessary, furnish the employee with a license for the same solutions used on the organization-owned devices**. If you need extra licenses, then contact the provider. They may have solutions to cover you through this unprecedented event.

PRO TIP

Multifactor authentication (MFA) ensures that access, whether to cloud-based services or full network access, is by authorized users only. Wherever possible, use an app-based system or physical hardware token to generate one-time codes that grant authenticated access.

5 Collaborative tools and authorization processes

It may seem strange to put these two items under the same heading, but one can help prevent issues with the other.

- Provide access to chat, video and conference systems so that employees can communicate with each other. This provides the productivity tools needed and helps employees to remain social with their colleagues.
- Use the collaborative tools to protect against unauthorized instructions or transactions. Cybercriminals will likely use the opportunity of remotely located workforces to launch Business Email Compromise (BEC) attacks. This is where a bogus urgent demand is sent by a bad actor, asking for the urgent transfer of funds, without the ability to validate the request in person.

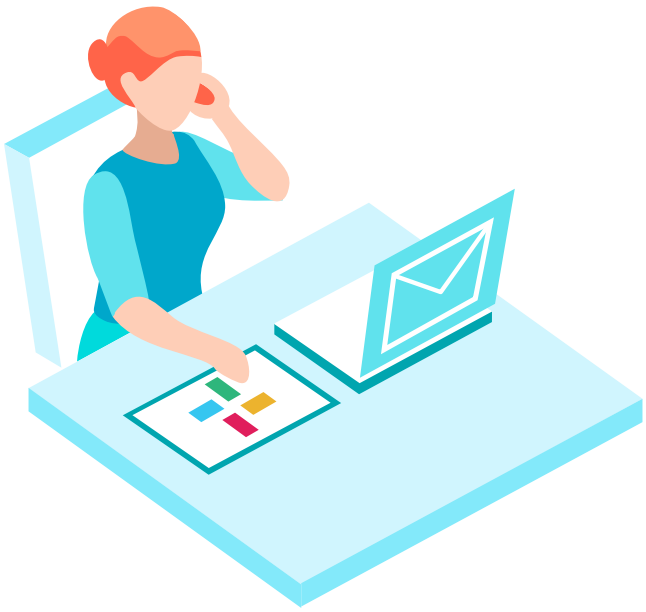
Be sure to use video conferencing/chat systems as a formal part of the approval system so that validation is made "in person", even when remote.

6 Cybersecurity training

We have already witnessed numerous COVID-19 scams in circulation, leading to face masks, vaccines, and disinformation. When employees are relocated out of the workplace and placed into the more casual atmosphere of working from home, they may consider clicking on links, as there are no colleagues who might see them watching that amusing video or visiting a webpage.

PRO TIP

Cybersecurity awareness training is typically an annual requirement for employees. Especially now, when working remotely, run an ad-hoc campaign and ask employees to go through such training.



7 Support and crisis management

In the rush to provide remote access, don't sacrifice cybersecurity or the ability to manage systems and devices. The ability to support users remotely is essential to ensure smooth operations, especially if users become quarantined due to health concerns. Remote workers need to have clear communication protocols for IT support and for crisis management if they encounter unusual or suspect issues that could be the result of a breach.

Don't assume that all employees can switch to remote working effectively and with little assistance or guidance. Home is not the office and they may need significant assistance to adapt.

How can ESET help?

When it comes to remote workplace security and its emerging challenges, you can rely on ESET. Here are some of our solutions that will help your company to stay safe and productive during these difficult times.

REMOTE MANAGEMENT

ESET Cloud Administrator

Cloud-managed security for up to 250 seats saving cost, time and simplifying the protection of your network.

- Setup and deployment within minutes
- No need for additional HW or software
- Single point of network security management
- Accessible safely via web browser from anywhere

Explore now

SECURED DEVICES

ESET Endpoint Protection

Multilayered technology, machine learning and human expertise combined with automated security management.

- Easy-to-run protection with cloud-based remote management
- Protects you from targeted attacks, ransomware and fileless attacks
- Full Disk Encryption add-on

Explore now

SECURE ACCESS

ESET Secure Authentication

A simple, effective way for businesses of all sizes to implement multi-factor authentication across commonly utilized systems. Enables your organization to:

- Prevent data breaches
- Meet compliance requirements
- Manage centrally from your browser
- Use your phone, or HW tokens

Explore now

For more information on Remote Working solutions, visit our dedicated **WEB PAGE**