Dr.WEB®
since 1992

DEFEND WHAT YOU CREATE

Task list

to ensure your information stays secure when your employees start working remotely

Give this document to your system administrator

A to-do list that ensures your information stays secure when your employees start working remotely

Before transitioning to remote work:

Action	Completed
Prepare the list of software recommended for installation on employee computers, and make the resulting regulations binding for all company employees. Notify all employees working remotely about this.	
Prepare distributions of the products that employees are recommended to use and place them in an accessible location, together with installation instructions, a list of recommended settings, and a list of plug-ins. Make sure that the programs are downloaded, installed, and configured properly.	
Recommend that employees use strong passwords; help them choose and change their password, if necessary.	
Recommend that employees install security updates for their operating system and the applications that they use; help them with this, if necessary. Verify that this task has been executed.	
Make sure that corporate services are available outside the office. Check your Internet channel and backup communication channel bandwidth — to see whether it is sufficient for your employees to be able to work outside the office.	
Minimise the number of corporate services available from the outside. Each of them is a probable target of attack. If possible, disable non-secure business processes that you can temporarily stop using. Scan your resources for vulnerabilities and be prepared for cybercriminals to launch DDoS attacks against you.	
If you doubt whether some employees are complying with the security measures, minimise risk by assigning them tasks that don't involve processing important data.	
To avoid receiving and sending infected email messages, employees should handle email via the company's mail server — ensure that they can do this.	
Ensure that the anti-virus scans email messages on the server end to detect any malicious programs and spam.	
Install security solutions on the devices that your employees will be using to work remotely — the anti-virus, anti-spam, firewall, tools to restrict access to non-secure resources. If it is impossible to remotely install and configure the security tools, provide the employees with anti-virus distributions, license keys, and instructions on how to install and properly configure them.	
Advise employees to update their home-router firmware.	
The anti-virus settings must prevent anyone from deliberately making changes to them (for example, an employee's family members). Tell employees how to configure and control whether a task is complete.	
Recommend that employees work only with user privileges — not administrator ones. Tell them why it is risky to work as an administrator. Recommend that they use a separate account for working with corporate documents.	
Configure Office Control restrictions for the account used by employees for work in order to prevent them from accessing malicious resources.	

When installing anti-virus protection on employee devices

You can use both single-user (non-centrally managed) Dr.Web anti-virus products and the centralised corporate anti-virus protection system to provide anti-virus protection to computers and devices that are used for remote work and are accessible to third parties (family members, and so on).

Using centrally managed protection implies less risk to the company because an employee and a person who has access to their PC or mobile, by default, do not have the right to disable anti-viruses and change their settings. This shields the company's network from hackings and data theft.

- If non-centrally managed anti-virus solutions are used to protect remote workers:

Action	Completed
Give employees the needed number of licenses or key files. Provide them with access to the necessary distributions if they will be carrying out the installation themselves.	
Before installing the anti-virus protection, it is recommended that you scan the system using the current version of Dr.Web CureIt!	
Check whether administrator privileges to install an anti-virus are present.	
Before installing corporate anti-virus protection, remove any other manufacturer solutions that may have been installed previously.	
Deploy the protection system.	
In case software that is not compatible with the Dr.Web Enterprise Security Suite anti-virus agent or potentially dangerous software is detected — remove it.	
Check the results of deploying the protection and the current settings.	
Scan employee stations with the anti-virus.	

- If employee devices and computers are included in the centrally managed security system:

Action	Completed
Check whether administrator privileges to install an anti-virus are present.	
Install security updates on the devices and computers.	
Prior to installing the Dr.Web Enterprise Security Suite anti-virus agent, it is recommended that you scan devices using the current version of Dr.Web CureIt!	
Before installing corporate anti-virus protection, remove any other manufacturer solutions that may have been installed previously.	
Configure the Dr.Web anti-virus server if employees are connected directly to it, or install an anti-virus proxy server.	
In the Dr.Web SCC's Anti-virus network, create separate groups for the employees' protected stations.	
Take the necessary steps to configure the created groups. If, during the installation process, it becomes necessary to specify parameters for accessing the anti-virus server or anti-virus proxy, allow the corresponding actions in the Control Center.	

Add to the Dr.Web Control Center the key file or files that are protecting the needed number of employees.	
Create the required number of new stations and give anti-virus agent distributions to your employees according to the deployment scheme you selected.	
Check the results of the protection deployment process and the current settings.	
In case software that is not compatible with the Dr.Web Enterprise Security Suite anti-virus agent or potentially dangerous software is detected — remove it.	
Scan employee stations with the anti-virus.	
Use the Dr.Web Control Center features to monitor the list of installed updates and employee-installed software. If potentially dangerous software is detected, create rules to block it using the Dr.Web Application Control module.	

Detailed instructions on using Dr.Web Enterprise Security Suite to protect employees working remotely

About Doctor Web

Doctor Web is the Russian developer of Dr.Web anti-virus software. Dr.Web anti-virus software has been developed since 1992. The company is a key player on the Russian market for software that meets the fundamental need of any business — information security.

Doctor Web was the first company on the Russian market to offer an anti-virus as a service and, to this day, is still the undisputed Russian market leader in Internet security services for ISPs.

Customers trust Dr.Web

Doctor Web's IT security experts possess a wide range of capabilities, which allows the company to thoroughly understand the operational nuances of all kinds of businesses and offer its customers the best selection of quality products at minimal TCO.
The fact that Doctor Web has satisfied customers—home users, major corporations, and small businesses—all over the world is clear evidence that the quality of its products, created by a talented team of Russian programmers, is undisputed.

Here are just some Dr.Web customers: https://customers.drweb.com.

Why Dr.Web?

All rights to Dr.Web technologies are reserved by Doctor Web. The company is one of the few anti-virus vendors in the world to have its own technologies for detecting and curing malware. Doctor Web has its own anti-virus laboratory, global virus-monitoring service, and technical support service.

3rd street Yamskogo polya 2-12A, Moscow, Russia, 125040
Phone: +7 (495) 789-45-87 (multichannel)
Fax: +7 (495) 789-45-97
https://www.drweb.com