A reference for employees

who use their personal
handhelds/computers
for work (BYOD)

#1

Learn and follow your company's policy on using personal devices for work.

#2

If your device's operating system allows, create two administrator accounts—one for personal use and one for business use—and disable the Guest account and the autorun function.

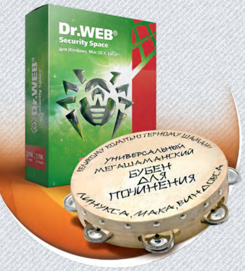
#3

Use strong passwords.

#4

Install in a timely manner all updates and new versions of ALL the programs (all obtained from official sources) installed on your device. In a corporate environment, use a system that centrally distributes software updates.

#5



Leave it to your company's system administrator to choose the anti-virus that is to protect your PC/laptop or smart phone.

#6

The anti-virus used must be able to be incorporated into the corporate security system, so that it can be controlled centrally.

#7

The application must provide comprehensive protection; an anti-virus alone is no longer enough.

Protection components for PCs

Protection components for mobile devices

On smart phones and tablets using SIM cards, the Anti-theft allows devices to be locked remotely and data to be deleted from them to prevent them from falling into criminals' hands.

These protection components should not be disabled under any circumstances (if administered centrally, the anti-virus makes it impossible to disable them)!

#8

Use special software to **wipe corporate information** from the device **permanently**, if:

- The device requires repairs or reflashing via a third party (for example, at a service center);
- You leave the company;
- Someone else will be using your device;

It is recommended that you entrust your company's system administrator with this task and document it so that if a data leak occurs, you won't be held responsible even after you leave the company.

#9

Write down the device's serial number and keep it in a safe place—it may come in handy if the device is lost.

Never!

- Use a device with modified firmware or an OS image created by a third party.
- Use inexpensive smart phones and tablets of dubious origin that do not guarantee top quality, security, and reliability.
- Download and install Android software from sources other than Google Play or the official sites of software developers.
- Allow other people to use your device.
- Use your corporate account to browse the Internet for your personal needs.
- Disable automatic updating for the anti-virus.
- Demand that the company's system administrator disable updating and regular scanning (if a corporate security system is in use).
- If you use your handheld for remote banking, **do not use it to perform any other tasks!**

Doctor Web is the Russian developer of Dr.Web anti-virus software. We have been developing our products since 1992.

3d street Yamskogo polya 2-12A, Moscow, Russia, 125124

Tel: +7 (495) 789-45-87
Fax: +7 (495) 789-45-97

www.drweb.com | www.drweb-curenet.com | www.av-desk.com
http://freedrweb.com | http://mobi.drweb.com