Dr.WEB®
с 1992 года

Памятка ответственного сотрудника

при использовании личного мобильного устройства/компьютера для работы (BYOD)

#1

Изучите и соблюдайте установленные вашей компанией правила использования личных устройств для работы.

#2

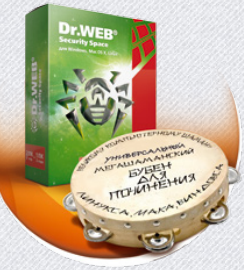
Если функционал ОС позволяет, заведите на устройстве 2 администраторские учетные записи: для личных и рабочих нужд; отключите учетную запись Гость и возможность автозапуска программ.

#3

Используйте сложные пароли для входа в учетные записи.

#4

Своевременно устанавливайте все обновления и новые версии ВСЕГО установленного ПО (которое должно быть только лицензионным) из официальных источников. При использовании корпоративной системы безопасности должна действовать централизованная установка обновлений установленного ПО.



#5

Доверьте выбор антивируса для защиты вашего ПК/ноутбука или смартфона системному администратору вашей компании.

#6

Используемый антивирус должен обладать возможностью включения в корпоративную систему безопасности для централизованного управления.

#7

Антивирусная защита должна быть комплексной, только антивируса уже недостаточно.

На смартфонах и планшетах с SIM-картами Антивор позволит удаленно заблокировать устройство и стереть на нем всю информацию, чтобы она не попала в руки злоумышленников.

Эти компоненты защиты нельзя отключать ни при каких условиях (а при централизованном управлении защитой это сделать невозможно)!

#8

Безвозвратно удаляйте корпоративную информацию с помощью специальных средств, если:

- устройству требуется перепрошивка или ремонт силами сторонних специалистов (например, в сервисном центре);
- вы увольняетесь;
- ваше устройство меняет владельца.

Рекомендуем доверить это системному администратору вашей компании и задокументировать этот факт – если произойдет утечка данных, вас не смогут обвинить в ней даже после вашего увольнения.

#9

Запишите и храните в надежном месте серийный номер устройства – это необходимо на случай его пропажи.

Нельзя!

- Использовать устройства с модифицированной заводской прошивкой или версией ОС, созданной третьими лицами.
- Использовать подозрительно дешевые смартфоны и планшеты, происхождение которых не гарантирует 100% качества, надежности и защищенности.
- Для Android-устройств — скачивать и устанавливать программы из других источников, кроме каталога Google Play или официальных сайтов разработчиков.
- Разрешать другим пользоваться вашим устройством.
- Заходить в Интернет по личным делам с рабочего аккаунта.
- Отключать автоматические обновления антивируса.
- Требовать от системного администратора компании отключать обновления и регулярные сканирования (если используется корпоративная система безопасности).
- Если вы используете устройство для проведения платежей через систему дистанционного банковского обслуживания — на нем нельзя проводить никакие другие операции.

«Доктор Веб» — российский разработчик средств информационной безопасности. Антивирусные продукты Dr.Web разрабатываются с 1992 года.

125124, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а

Телефон: +7 (495) 789-45-87 (многоканальный)
Факс: +7 (495) 789-45-97

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