Mobile Device Requirements for Employees

In 2020, we're all working remotely in some capacity. Our phones, tablets, and laptops were already well on their way to being data goldmines full of sensitive company data, but that process has been kicked into high gear thanks to the "new normal."

BYOD (Bring-Your-Own-Device) policies have become absolutely mandatory for any business trying to survive the COVID-19 work-from-home mandate. They provide clear guidelines on how companies should manage the devices being used by employees to remotely access an organization's files and data.

"EMPLOYEES NEED A CLEAR LIST OF PROCESSES AND GUIDELINES THEY CAN FOLLOW"

But these policies can be large and wide-sweeping, covering things from IT department policies to detailed patch processes for back-end hardware such as servers.

Employees need a clear list of processes and guidelines they can follow. This guide will show exactly what should be expected of end users, and how they can be responsible with the devices they use every day.

EMPLOYEE CHECKLIST!

General Rules

- No single copy of company data is be stored on any mobile device - secondary copies must be kept on an internal server.
- Do not "jailbreak" or "root" devices.
- Do not leave devices visible in unattended vehicles or hotel rooms.
- Do not use unsecured networks (wired or wireless) if at all possible.
- Devices should remain with you, and not be shipped or checked for transport.

Installations, Backups, Downloads, & Updates

- Download files only from known good sources for business purposes.
- Allow the immediate installation of any updates, patches, or other fixes.
- Users are responsible for backing up their own personal data.
- Do not install unauthorized or pirated applications.

Passwords

- Passwords must be changed immediately if suspected of theft.
- Never share passwords with those who are not authorized to have them.
- Store all shared passwords in a centralized password database.
- Notify IT department of passwords that should be transferred upon termination.

Phones & Tablets

- Become familiar with services like Find My iPhone in case of lost/stolen devices.
- Lock devices when not in use.
- Do not share devices with non-company personnel.
- Report any theft or potential data compromise to IT department immediately.

Laptops & PCs

- Never access, insert, or connect to any disks or drives of unknown origin.
- All systems handling company data must have anti-malware programs.
- Do not uninstall or tamper with any security software installed by IT department.
- If applicable, run a virus scan on any executable file received via the internet.