EMPLOYEE SATISFACTION WITH MDM

MOBIVISOR

ABOUT US

IOTIQ GmbH has been providing innovative software solutions for various application areas since 2017. Our mission is to support companies of all industries and sizes in taking the path towards digitalization with the right tools at hand and the right partner at their side.
In a world that is mobile and constantly becoming more so, security remains the top priority. To ensure this, we have developed MobiVisor - the mobile device management system that is just right for you.

IOTIQ

Smartly Done.

BRING YOUR OWN DEVICE TO WORK

Mobile devices such as laptops and smartphones are widely used for personal and business purposes. Especially with the COVID-19 pandemic, as working from home has increased, the importance attributed to the usage of mobile devices has also grown. Employees started to use their own devices, but connected them to the company network or accessed company data remotely. This situation then kept its effect when work-life returned to the “new normal”. Most companies found it beneficial for their employees to bring in and work with their own devices, both from a practical and economic standpoint. Of course, as in every technological development, employees' use of their own devices carries risks as well as advantages.

Bring Your Own Device (BYOD), for example, is a policy that allows company employees to use their personally owned devices. Companies define a set of policies to allow their employees to use their own devices for accessing emails, corporate apps and data as well as connecting to corporate networks.

There are alternatives to BYOD models such as company-owned/business-only (COBO) devices, or company-owned/personally-enabled (COPE) devices. These two options mean that the company purchases and owns the mobile devices and grants employees the ability to access company information and applications. However, the main focus of this infopaper is the BYOD model, which is commonly linked to IT consumerization.

As BYOD models offer employees access to company information, it is crucial for companies to have a well defined BYOD policy to avoid the danger of cyber threats such as ransomware, hacking and data breaches.

IMPLEMENTING A BYOD POLICY

A BYOD policy is generally created in a document with some requirements that employees agree on implementing. These requirements can be:

- Types of mobile devices approved for use by IT department
- A clear definition of the termination policy
- Security measures such as password requirements
- User responsibilities around the device and its access to the network
- Any incentives or cost reimbursement for using personal data plans for work-related activities
- Software that must be installed to help secure a device, like an MDM tool
- An exit plan when employees no longer wish to use their personal devices

WHY BYOD?

Employee Satisfaction

The BYOD model has become increasingly popular in recent years, especially during the COVID-19 pandemic, since it enables employees to work remotely, accessing their company's network and data from home or on the go. With the help of the BYOD model, people can choose where they want to work or move independently as they have the opportunity to bring their own devices wherever they go. Young people especially like to choose where they want to live and do not want to be held by a job in a particular location, making a BYOD model more attractive for this workforce.

The spread of the BYOD model, above all, has increased employee satisfaction. With the adoption of the BYOD model by companies, employees have achieved the welfare of being able to work anywhere without having to carry additional devices.

Why should employees use their own devices at work?

- Higher employee productivity: Employees find it easier to work from home or other locations when they do not have to switch devices
- More comfort: Employees are more comfortable when using their own devices as opposed to learning how to use new equipment
- Upgraded technologies are integrated into the workplace: Without IT spent on hardware, software licencing or device maintenance
- Increased employee satisfaction through supporting flexible work arrangements
- Better overall user experience as employees know how to use their own devices
- Reduced amount of devices employees need to carry

Why should companies adopt the BYOD model?

- Simplified onboarding and offboarding: With the usage of MDM and the BYOD model, company network access can be enabled/disabled
- Device cost savings: The usage of the BYOD model decreases the company assets that need to be tracked, issued, managed or upgraded
- 59% of organizations have adopted BYOD
- 67% of employees use their own devices at work
- 87% of businesses are dependent on their employee's ability to access mobile business apps from their smartphone

Company Security

As the use of the BYOD model becomes more widespread, ensuring its security becomes crucial. In this case, the IT departments of the companies can use a mobile device management system (MDM) to be aware of the dangers and risks in the devices in advance and provide permission and access accordingly.

Furthermore, companies adopting BYOD models can also ensure certain security policies for every device. The policy should include:

- Security controls including data encryption and password strength
- Which mobile device management (MDM) software must be installed on BYOD devices
- Whether the company is authorized to remotely control, access or intervene when a policy breach is detected
- Which websites are off-limits while connected to enterprise resources, corporate network or VPN.
- Which enterprise applications and data can be accessed from user devices, i.e. email, calendar, messaging, contacts, etc.

Employee Security

The **Bring Your Own Device (BYOD)** model on the one hand provides access to company information, while employees are worried that their private information will also be revealed. Mobile Device Management (MDM), which is integrated for the security of the BYOD model, provides both company security and employee security.

With MDM, companies do not access, control or monitor the personal data of the device owner while granting access to various company data and applications. MDM is used only for the security of company information and company-related transactions. Therefore, it requests access to information that will provide this security. This information is technical and device specific information such as the serial number, device model name. It does not have such a feature as tracking search history or access to personal notes. Above all, MDM is not for control, but for management.

In this context, the first and most important precaution to be taken to ensure employee safety in the BYOD model is to use an MDM

Social Media Usage

Another issue that has become controversial with the adoption of the Bring Your Own Device model is that security and employee productivity are affected by employees' social media use. The BYOD model offers various opportunities to employees such as defining policies which apply to security vulnerabilities. Of course, since this situation and the implementation of the policies are made from the perspective of the company, the existence of any security policy for the social media that employees use daily on their own devices is a matter of debate. Therefore, companies that adopt the BYOD model should also adopt a social media policy.

Security Issues:
Employees' use of social media in the BYOD model may pose a danger to confidential business information, as well as revealing information about employees' private lives. Therefore, while adopting BYOD policies, companies should take security measures, including their employees' use of social media, and train their employees on the implementation of policies and access to information. In addition, they should use a Mobile Device Management (MDM) to ensure the separation between personal and company data and to access information within the context of this separation.

What MobiVisor MDM offers:
By setting up a secondary profile that is used for work, data is separated by private and work data being backed up in different containers. Apps that are only used in the work profile, for example, are marked accordingly on Android. This means that two versions of the same app exist that are not connected to each other and thus divide private and work data. Regardless of your chosen usage scenario, your data and apps are neatly separated thanks to MobiVisor, which ensures security for the company and privacy for your employees.

Employee Productivity

Does using one's own devices in the BYOD model increase employees' social media usage? How does this affect their productivity? The answers to these questions vary according to the purpose for which employees use social media. If we evaluate the social media usage of the employees in terms of their productivity, we need to be aware of two distinctions. According to a study, if employees use social media to socialize between work, this increases their job satisfaction. But if they use social media with work-related motivation, then this increases their productivity.

The BYOD model provides space for both. Employees can both socialize with their own devices on social media without any privacy violations, increase their productivity by making promotions and follow developments related to their work. Especially in areas of work where problem solving skills, creativity and awareness of developments and trends are important, such as marketing, business development or sales, social media usage can help to evolve the company's activities by taking inspiration from competitors.

The study also shows that:

- Social-oriented usage of social media enables maintaining contact with existing friends and customers.
- Social media has significant impacts on communication and management in workplaces and businesses.
- Social media in organizations could facilitate internal knowledge management and increased communication efficiency, and even enhance work performance.

Although the **increased use of social media among employees**, especially with the **transition to the BYOD model**, seems to be a risk for productivity, it is a fact that it **increases employee motivation.**

This increase in motivation also **affects productivity**. As a result, **both company and employee satisfaction** is achieved.

DO YOU WANT TO KNOW MORE?

Do you have questions about how MobiVisor and our extensions work, or are you unsure whether MobiVisor MDM fits your company and its challenges?

We are happy to assist you with advice and support! Just contact us by phone or e-mail.
We would also be happy to arrange a personal presentation appointment with you and provide you with a test environment of MobiVisor without obligation.

Toni Voß
toni@iotiq.de
+49 1578 3020995

Saskia Riechers
saskia@iotiq.de
+49 176 1500 6080