Mobile Device Management Policy

Sydney Meadows

East Carolina University

**Abstract**

The use of mobile devices in the workplace has grown significantly over the years. Most adults do not leave home without their phones, laptops, tablets, or other portable media devices. With this expansion, there needed to be a policy put in place to protect those devices from cybersecurity threats and threats that can occur. This is how the Mobile Device Management (MDM) Policy was created and has been implemented and most companies throughout the world. In this paper, I will go into depth about the MDM policy and why it is important in today's world of technology, especially within the workplace.

**Introduction**

Mobile device management (MDM) is defined as the method and toolset used to “provide a workforce mobile productivity tools and applications while keeping corporate data secure” (IBM, n.d.). Mobile devices have become normal within the workplace today and rely on them for various tasks. Having a policy in place that addresses this is a vital part of the productivity and efficiency of these technologies. As technology grows so will the need for new policies like MDM so that a company and its employees can be secure and productive.

Mobile device management (MDM) allows IT admin to manage mobile devices that access business data securely. Essential information is stored on these mobile devices so if the device is stolen or lost there are solutions in place to prevent theft (ManageEngine, 2022). This policy uses tools like device tracking, mobile management, application security, and identity and access management to keep this safe environment. These are only a few tools that can be used to ensure MDM is being used to its full potential (IBM,n.d.).

An MDM policy is very customizable to whatever the company's needs may be at the time of making it. Some common policy controls that are added by companies are requiring a passcode, enforcing OS updates, allowing only approved applications, controlling usage, and forcing regular backups or files (Haviland, 2021). The policy controls help an organization regulate and stay on top of anything and everything that is happening on their mobile devices. It also helps ensure that employees stay on top of important security tasks. These additions to the MDM policy must be written out and communicated clearly to properly be able to monitor and enforce the policy correctly (Haviland, 2021).

**Background of the Policy or Policy Need**

This policy was first introduced in the early 2000s as the use of mobile devices in the workplace started to increase. It made the need for this policy essential because now mobile devices are normal in the modern-day workplace (Keinänen, 2022). Statistics show that within the next few years, 4 in 10 people say their smartphone “will replace the need for a traditional computer” (ManageEngine, 2022). The need for this policy is to ensure that a company’s data remains confidential, and its resources are being used productively.

**Stakeholders and Impacts in relation to the Policy**

Based on my research the main stakeholders for this policy have been big businesses and corporations including Apple. Companies want to make sure their data stays secure but also realize how mobile devices like laptops and smartphones have made it easier for work to get done. With the MDM policy, IT workers can easily manage all the devices used by employees on their systems (Keinänen, 2022). Organizations rely heavily on the MDM tools, because of that, making them strong advocates for the policy.

The impacts of this policy for corporations are that they can control all corporate mobile devices, protect data and device security, and increase productivity while lowering costs. Many companies give out their own mobile devices to employees, so this allows them to keep track of those devices and establish a unified device management process (Keinänen, 2022). MDM also offers data protection regulations for tablets and mobile phones because, compared to PCs and laptops, these devices are more susceptible to cyber-attacks. By giving organizations this control, it helps to decrease human error and it makes an easier setup for these devices (Keinänen, 2022).

**Various Viewpoints of the Policy**

Many of the things that make mobile device management (MDM) a good policy can also be the same reason why people may be skeptical about it. For example, having full control over devices using the network could call some employees to question their privacy. This makes it important for some organizations to give their own mobile devices to employees working for them. Most of the tools used in MDM can easily be adjusted to fit the company’s needs, making some companies’ weaknesses easily solvable.

MDM does not have many known disadvantages or reasons why people may not use this policy however three setbacks of the policy are required security audit reports, system integration, and defining company policies. With security audit reports, a company must perform them regularly and these audits are very time-consuming and require a lot of resources (Nash, 2021). System integration is also another setback due to the number of mobile devices that must be managed through the organization. It increases the traffic on the network usually requiring a company to customize or replace the current system. Lastly, defining company policies is another time-consuming task where the company must customize the MDM policies with the current company policies (Nash, 2021).

**Why this Policy is Important in IT and to others**

This policy is important in IT because mobile devices are becoming a huge part of society and how companies operate. This policy not only affects the workplace but also things we do not think about simply because it has become normal in society. Most organizations including schools and your favorite clothing brands use mobile device management. If you've ever worked in these places a point-of-sale (POS) terminal is an example of MDM being used (Keinänen, 2022).

MDM has been important in many cases including healthcare, transportation, and education just to name three. Within healthcare, most health organizations are moving towards electronic health records (EHRs) making mobile device usage more popular than ever (ManageEngine, 2022). Most people also keep their personal health information on their mobile devices, so it is important to make sure their devices are secure and meet HIPAA regulations. The mobile device management policy has given solutions to meet these standards and keep health information from unauthorized access (ManageEngine, 2022).

Transportation is a case that involves MDM because many organizations use it to securely track shipments and vehicle locations. With corporate devices being locked down for specific applications, it helps prevent misuse of the device and makes sure it is being used productively (ManageEngine, 2022). We often use this ourselves when we are tracking shipments for our packages. Education is also one of the most influenced cases of mobile devices being used and needing more protection. With MDM, schools can configure secure and essential applications on the tablets and laptops that they allow their students to use (Keinänen, 2022). The MDM policy is important in the IT world, but it is also important for many other companies and organizations.

**Ideal Outcome Regarding the Policy**

The ideal outcome for this policy is that it remains prevalent in companies but there could also be a tighter leash on the use of personal devices in the workplace. As previously stated, many companies give out work phones and work laptops that their employees are obligated to work on. My mom works for a company that does that, and it makes it easier for her to separate her work-related content from her personal content. This also helps the company have full control over those devices and what happens on them.

MDM helps protect these companies and the mobile devices used within the workplace. If their companies do not abuse the power given by the policy, it is being used for the benefit of the employer and employee. Technology will continue to grow and as this happens, this policy is subject to make updates and changes that go along with the times.

**Conclusion**

Mobile device management is an important policy that helps protect businesses and employees and makes them feel secure while using mobile devices in the workplace. While there may be opposing sides to the use and personal privacy within this policy, it has many more pros than cons. Technology is a rapidly growing industry and over the past 20 years, the MDM policy has become one of the most important policies regarding the use of mobile devices in organizations today. This has helped many employers to maintain a healthy workplace that properly uses mobile devices to get work done.

**References**

Haviland, J. (2021, December 14). *Essential Mobile device policy considerations for growing*

*businesses*. Samsung Business Insights. Retrieved April 8, 2022, from

<https://insights.samsung.com/2021/12/14/essential-mobile-device-policy->

considerations-for-growing-businesses-3/

Keinänen, K. (2022, March 28). What is MDM? A complete guide to mobile device

management. Miradore. Retrieved April 6, 2022, from

https://www.miradore.com/blog/mdm-mobile-device-management/

ManageEngine. (2022). *What is MDM?* What is MDM? | MDM Software - Solutions - Benefits.

Retrieved April 6, 2022, from <https://www.manageengine.com/mobile-device->

management/what-is-mdm.html

Nash, A. (2021). *7 advantages and disadvantages of Mobile Device Management [2022]*. 7

Advantages and Disadvantages of Mobile Device Management [2022]. Retrieved

April 8, 2022, from <https://mobiletrans.wondershare.com/mobile-device->

management/advantages-and-disadvantages-of-mdm.html

IBM. (n.d.). *What is Mobile Device Management (MDM)?* IBM. Retrieved April 6, 2022, from

https://www.ibm.com/topics/mobile-device-management