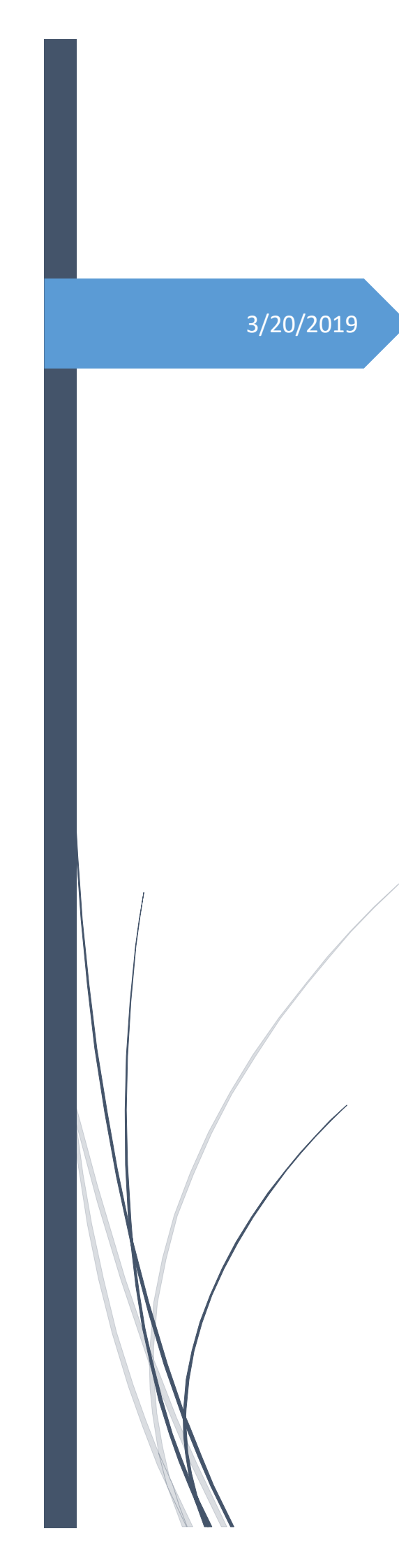




3/20/2019

Internet Technology & Security

Report

ACCA4018

Cameron Anthony Dallimore
DAL14815894

Report

Contents

Contents	1
Introduction.....	1
Security Policies.....	2
Password Policy	2
Remote Access Policy.....	2
Acceptable Use Policy	2
Email/Communication Policy	Error! Bookmark not defined.
Access Control Policy.....	Error! Bookmark not defined.
Device Management Policy	3
BYOD Policy	3
Mobile Device Management Software	3
Rationale of My Choice	4
Advantages of BYOD.....	4
Disadvantages of BYOD.....	4
References.....	5

Introduction

First I will be discussing various policies not limiting myself as a certain user, this is so I can cover a wider range of which the policies are most efficient and beneficial. Then I will select a Mobile Device Management Software (MDMS) for “Bring Your Own Device” (BYOD) and explain in depth why I have chosen the certain software, and go on to discuss why I believe this is the more efficient software to choose. Then I shall go on to the advantages and disadvantages of bringing your own devices, with a concluded opinion, I will also be including a diagram to show the efficiency of BYOD and how it’s used.

DAL14815894

ACCA4018

Security Policies

Security policies are terms in which a company has stated their intentions of safe and secure guidelines they have set to abide by, the *mustn't* break these as it's a breach of their own security and can cause serious consequences. All employees of the company must read the policies to make it a safe and secure place of work, these are in place to ensure no breaches of outside or inside threats will gain access or to help protect private or valuable data/information.

Password Policy

Password policies is to help protect personal information/data, it's important to follow the recommended requirements for creating passwords these include, mixture of numbers, upper and lower case letters as well as having it reasonably long, you want it unique and less likely for someone to guess it., also memorable to you, because you don't want a password that's easy to forget, also you should use a different password for each of your accounts/ logins, just to ensure you protect all of your accounts instead of having one password for everything then if someone does get into one of your accounts then, they'll be able to access everything. This is especially dangerous if you have a comprising workplace where someone would be able to access important and valuable information as well as your bank details, if you have online banking.

Password policy will also state how to deal with a breach of this policy, if your device has been stolen or someone's accessing your accounts and how to file a report for security breach.

Remote Access Policy

Remote access policy is where an employee can work from home or work outside of a workplace using their own devices, although there have been an increase of more employee working from outside their workplace, they are vulnerable to outside attacks, within the policy it'll be stated how make the experience a more safer and secure way of work, to prevent these outside attacks. This does its benefits of using devices you'd be more familiar with.

Acceptable Use Policy

This this where the company is monitoring your activity on the company device/computer, all data and information that has been created on the company's systems belong to them. It' also where the company's able to block access to certain websites and pages, although this doesn't prohibit an employee finding loop-holes to access unauthorised website/pages, a policy should be included to block these accesses, with any attempts made will involve some form of punishment. This is to protect the company's systems from malicious attacks attached to certain websites.

DAL14815894

ACCA4018

Device Management Policy

Device Management policy is a policy that all those that are part of the company, must abide by protecting private information, of the staff, and in some case the customers information.

BYOD Policy

This is the use of your own personal devices, devices that someone would understand fully and know how it works as well as what to use it for, the certain aspects of their job, whether it be your phones, tablets or even in some cases computers or laptops. This allows the user using their own devices to access to the company's networks. There are security terms the user must abide by and carry out, some of these would be as follows, to have a secure password that even their family can't access in case there's confidential information on the device, up to date software and operating system and avoid downloading certain sensitive information, which should stay in the company's system and not taken out.

Mobile Device Management Software

My MDMS of choice is Cisco Meraki MDM, this can be used for both PC's and Macs, including mobile devices, as well as the whole network. Cisco Meraki has a vast array of features and uses, and personally I believe it to be one of the best MDMS's to date, it helps and matches a lot of the policies I have already mentioned and even extra features that help with efficiency and many automated features. Cisco Meraki allows management to monitor all company devices and their information, including recent locations, administrators are also able to lock any device and even erase them, if needed. It helps to enforce the organisations policies, for all the organisations devices, this can help to protect all the devices and data if, some individual users have not taken it upon themselves to protect the devices, this way management can be certain that all the devices are protect and secure. Management can also control the usage on the devices, using and enforcing a password policy to devices to block or stop access for a period of time if an individual has been using unauthorised means, wasting time when they should have been working or simply doing something productive, Cisco Meraki has a feature that allows management to block and restrict access to the app store, or even apps and games themselves. Another feature is that management can check or set/change the network settings on all networks, including wireless connections, remote VPN access and the security of all devices at the same time, this is time efficiency and nothing needs to be changed or sorted out manually. Cisco Meraki has another built-in feature, but this feature called ' Backpack' allows android users to send and even manage their file packages, documents, images, anything and this feature can be sent to a vast multicity of devices/departments or even globally. It can help to enforce protection for BYOD with an array of built-in features, all in one product, this defeats the need of having multiple product and licenses, and it also has, automated summarised reports of the network and shows the total percentage of their entire traffic.

DAL14815894

ACCA4018

Rationale of My Choice

I chose to write and discuss about Cisco Meraki because as I previously mentioned, it is firstly ranked one of the best Mobile Device Management Software's to this date, it has a vast multitude of features that assists in enforcing and protecting all devices of an organisation. It is very time efficient when dealing with the company's policies, it's automated so there's no need for as much manual input as it would normally require, and it

I believe that with Cisco Meraki, the brand name also makes it more reliable, as Cisco have a number of software products.

Advantages of BYOD

There are a number of advantages for BYOD, they are as follows; cost effectivity, no need for any extra or unneeded costs, for your device(s) as you are using your own, another advantage is familiarity, where because you are using a device you already own and are familiar with how it works, how it runs. Employees in the IT industry constantly want/need the most up to date device and/or software going, this can then rule out the slowness and insufficient productivity that would usually occur on older device/software, this also gives employee's their freedom. When using their own devices employees will have greater care and protection with and when using their own device, they won't have any, "it's only a company device, they pay for it", kind of attitude. They will have the latest protection and updates and careful not to break or damage the device, as it'll be them who pays for it. Anyone, let alone an employee in the IT industry will always have a personal preference of what device they would, rather be working with or on, this then can improve productivity as well as, their wellbeing. In some cases, where employees are working from their own devices, they are then granted an increase of flexibility, they don't to stay in an office constantly, they can go to hotspots or even their own home, as long as they do the work.

Disadvantages of BYOD

Just like there being an array of different advantages for BYOD, there are various disadvantages too. A potential risk is having no policy for BYOD, meaning employees can freely roam with their possibly unprotected devices, all through the company's systems. Another potential downfall is the cost, employee's may not have a vast range of affordable options when it comes to these devices, they may have higher priorities in their lives than the latest up to date device, the device they have could therefore be slower, effecting the rate of their work.

There are greater security risks with BYOD than without, so ensuring that a policy for a well-protected device is enforced, is a priority, without it then the company is opening up their systems out to all kinds of threats, including if an employee has children or is just living with someone, or just someone knowing their passcode, they too can gain access to the company's information, so ensuring that the device has a passcode and not to share it with anyone, otherwise disciplinary actions should be taken.

References

- [1] CPCSTech, "Password Policy," [Online]. Available: http://www.cpcstech.com/pdf/password_policy.pdf. [Accessed 20 March 2019].
- [2] CPCSTech, "Remote Access Policy," [Online]. Available: http://www.cpcstech.com/pdf/remote_access_policy.pdf. [Accessed 20 March 2019].
- [3] CPCSTech, "InfoSec Acceptable Use Policy," [Online]. Available: http://www.cpcstech.com/pdf/acceptable_use_policy.pdf. [Accessed 20 March 2019].
- [4] L. Irwin, "5 information security policies your organisation must have," IT Governance, 15 January 2019. [Online]. Available: <https://www.itgovernance.co.uk/blog/5-information-security-policies-your-organisation-must-have>. [Accessed 20 March 2019].
- [5] Finances Online, "20 Best Mobile Device Management Software in 2019," Finances Online, 2019. [Online]. Available: <https://financesonline.com/mobile-device-management/>. [Accessed 27 March 2019].
- [6] Cisco, "Solutions: Mobile device management," 2019. [Online]. Available: <https://meraki.cisco.com/solutions/mobile-device-management>. [Accessed 27 March 2019].
- [7] B. Chignell, "The Advantages Of BYOD," Ciphir, 28 Febuary 2013. [Online]. Available: <https://www.ciphir.com/advice/the-advantages-of-byod/>. [Accessed 1 April 2019].
- [8] Optimus Learning Services, "The Advantages and Disadvantages of BYOD," Optimus Learning Services, 4 September 2013. [Online]. Available: <https://www.optimuslearningservices.com/practical-ld/advantages-disadvantages-byod-in-learning/>. [Accessed 1 April 2019].
- [9] Your IT Department Ltd, "The Advantages and Disadvantages of BYOD," Your IT Department Ltd, 1 June 2017. [Online]. Available: <https://www.your-itdepartment.co.uk/news/advantages-disadvantages-byod/>. [Accessed 8 April 2018].