SEMARAK ILMU PUBLISHING

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Implementation of BYOD Security Policy in Malaysia Institutions of Higher Learning (MIHL): An Overview

Izzah Inani Abdul Halim[1,*], Alya Geogiana Buja[2], Mohd Shah Shafie Idris[1], Nurul Jannah Mahat[1]

[1] Department of Computer Science, Faculty Computer, Media and Technology Management, Universiti College TATI, Jalan Panchor Teluk Kalong 24000 Kemaman, Terengganu, Malaysia
[2] Computing Science Studies, College of Computing Studies, Informatics and Media, Universiti Teknologi MARA (UiTM) Melaka Branch, Jasin Campus, 77300 Merlimau, Melaka, Malaysia

ARTICLE INFO

Article history:
Received 20 June 2023
Received in revised form 3 October 2023
Accepted 11 October 2023
Available online 31 October 2023

Keywords:
Bring Your Own Devices (BYOD); BYOD Security Policy; information security; Malaysia

ABSTRACT

The BYOD Security Policy (BYOD-SP) constitutes formal documentation protecting sensitive data and information during BYOD implementation in an organization. The BYOD environment in an organization might face threats if information assets security is not prioritized before initializing BYOD. Releasing BYOD-SP is one of the key strategies to safeguard safety in BYOD implementation and to ensure users adhere to the BYOD-SP. It can also increase the understanding of ways to protect the BYOD environment from any risk. Hence, this study explores the current situation of BYOD, specifically in Malaysian tertiary education institutions, and the compulsory components that should be highlighted in the BYOD-SP. The implementation of (BYOD-SP) in Malaysian Institutions of Higher Learning (IHL) has led to a sense of discouragement, with only a few institutions being able to clearly outline their implementation strategy, in contrast to what has been done by foreign universities. This has resulted in a lack of information and understanding about the components of BYOD-SP in the Malaysian environment, making it difficult to make deeper comparisons. Understanding the current practice of BYOD can provide a more comprehensive study of a suitable model, cybersecurity framework, or other features to prepare a comprehensive BYOD-SP documentation on campus. As the BYOD implementation is underway, this study could increase awareness of all aspects of BYOD to aid organizations in formulating the BYOD-SP document. This could encourage BYOD players to achieve maximum information security protection.

1. Introduction

Bring Your Own Device (BYOD) Security Policy (BYOD-SP) was initiated following the initiation of BYOD to avoid possible attacks on information security within organizations. It was designed to safeguard confidential data and private information circulated within the BYOD environment in any sector. The security policy was established to emphasize the protection of information security in an organization to ensure BYOD is practiced safely. In this light, security policy acts as a defense to protect mobile systems, networks, and data by Scott *et al.,* [1]. Furthermore, BYOD security policy

* *Corresponding author.*
E-mail address: izzahinani.ah@gmail.com

https://doi.org/10.37934/araset.33.2.114

must strike a balance between access, security, and privacy, given the personal device use in company security architecture as stated in Anderson *et al.,* [2]. As the trend of BYOD gains traction and becomes preferable in the corporate world, many studies have focused on BYOD implementation from the perspective of employees in different sectors. Studies have claimed that organizations should design a suitable security policy that meets BYOD requirements in their respective sector. This is a critical move as the existing security policy does not consider BYOD as the main ICT component. Several studies found that the current security policy is weak. Yeop *et al.,* [3] reiterated that it lacks technical experts, support, and enforcement mechanisms. In the meantime, the top management has started to allow employees to engage in BYOD since there is an urge from the employee side that BYOD promotes their massive benefits.

BYOD was introduced in early 2009 when Intel found that most employees bring their devices to the workplace to finish work. This move was followed by other companies and gained popularity as it lowered the expenses to purchase office equipment, specifically technological devices, reduced maintenance costs, and improved operational efficiency. On the employees' side, it increased their flexibility, productivity, satisfaction, and mobility. Various studies have reported BYOD as an extra perk. Employees working on their personal devices can accomplish the given tasks well. Cisco found that BYOD puts employees in more comfortable and homely environments as they utilize personal devices at the workplace reported by Rajapaksha [4]. Furthermore, it benefits younger employees like Millennials, who currently form a large part of the workplace in an organization claimed by Palanisamy *et al.*, Almarhabi *et al.*, [5,6]. BYOD makes employees feel proactive, balanced, empowered, and confident at work as they can work with familiar devices.

The high acceptance of BYOD drives the researchers to discuss BYOD trends and demand in each sector, its benefit, and the consequences of BYOD practice. After being implemented in the corporate world for a few years, researchers have emphasized the risks that could occur in the BYOD environment. Information security contributed to the top consideration in BYOD; therefore, the management should have come out with how BYOD can be practiced safely. As reiterated in Bello *et al.,* [7], organizations face difficulties, and inherent security issues must be addressed to protect their private information. Researchers then shifted the trend of the investigation from the BYOD demands to the BYOD consideration of establishing a policy to safeguard confidential data from being stolen by a third party. It is also applied to the network so each connected BYOD device would not be attacked. Studies on BYOD safety have described the method and solution to overcome this problem either on the employee side or in the context of the top management. In this light, there are several options to reduce the risks, from analysis to the technical part.

The existing BYOD-SPs are not focused on BYOD implementation in educational organizations. There is still limited research on this matter, and there is a need for more intensive study as BYOD is being practiced in education premises. BYOD in academics refers to Kebande *et al.,* [8], the simple idea that young people and school staff are permitted to bring their Internet-enabled device into school and use it to help them work, learn, and (if appropriate) socialize. This new approach, known as the mobile learning paradigm, urges the students to use devices they already own. Mobile learning reached momentum during the COVID-19 pandemic as teaching and learning had shifted to more online mode due to the lockdown, and schools were closed during that time [9-10]. Subsequently, as Covid restrictions ease, educational institutions have started to reopen, and students can stay on campus although online classes are still conducted. In this scenario, students do not have alternatives other than using their personal devices and the campus wireless service to access the university system.

In Malaysia, BYOD-SP has only been introduced in several Institutions of Higher Learning (IHL) as stand-alone documents and included in the general Information and Communication Technology

(ICT) security policy. The policy can be accessed online, where it can be downloadable by everyone. However, the policy of several private IHLs indicates the lack of any security policy. Furthermore, most statements in the existing BYOD-SP are too general, with no elaboration of how it can be practiced safely, and there is a slightly different concept of BYOD in a few institutions. The scenario becomes more complicated when the BYOD is not defined well for its implementation in Malaysia IHL, which is; (i) Allowing an individual to bring personal devices and use them on the campus and (ii) A grant called 'BYOD Grant' was allocated to buy the devices (mainly for permanent staffs) and utilize them for work purposes.

This study investigated how the security policy of BYOD implementation in education sectors focuses on Malaysia IHL. For this study, quantitative methods were chosen to understand the current situation on how it is being practiced; and the level of users' compliance with the BYOD security policy. This study aims to develop a cybersecurity framework (CSF) approach to ensure BYOD-SP encompasses standard security policy adhering to BYOD requirements in education premises. This study explains the current practice of BYOD security policy in MIHL and how the BYOD players in the education sector comply with this security policy. Therefore, this study can fulfil the requirement for BYOD implementation in education sectors, specifically tertiary institutions. This study is novel as it examines implementing a manageable BYOD security policy based on CSF-related BYOD features that can be implemented in Malaysian IHLs. This study will fill the research gap in practicing the standard security policy of BYOD implementation in Malaysian IHLs

1.1 Problem Background

As BYOD is becoming preferable in education sectors, thus it is required to prepare an appropriate and effective policy to eliminate the risks of cyber threats in the BYOD environment, suggested by Aguboshim [11]. A survey conducted in South Korean educational institutions by Tinmaz and Lee [12] found that BYOD is much supported in educational institutions. However, some participants have raised their concerns over security matters, but a few ignored them. In the meantime, most studies on BYOD focused on the challenges of handling device and network compatibility, individual behavior, security, and acceptance of BYOD. With the lack of resources in the Asian region, specifically in Malaysia, more research is necessary to find the solution in establishing a Cybersecurity framework model that suits the HLIs environment so that it can have big impact and positive effects, as about more research done not focused on the HLIs sector. Below are the research objective and research question that this study seeks to answer;

RO1: To evaluate the information security awareness on the implementation of BYOD in Malaysia Higher Learning Institutions (MIHL)

RQ1a: Do all MIHL practice standard BYOD-SP?

RQ1b: What components in BYOD-SP influence the awareness of BYOD implementation?

1.2 Theoretical Background (Overview of BYOD Security Policy (BYOD-SP)

The provision of Bring Your Own Device (BYOD) has offered many benefits, including productivity, flexibility, satisfaction, mobility, and convenience claimed by Scott *et al.,* [1], Rajapaksha [4], French [13], Cho and Ip [14] to the BYOD users. This triggered the change toward the use of technology in life, apart from additional issues such as the ease of getting the latest technology devices and the

ability to understand the features available on the device and use the app in completing some of the day-to-day tasks. Despite it's a bit many benefits, the issue of information security of an organization cannot be removed from the use of BYOD simply because of issues arising, such as a lack of awareness from the users themselves and the weakness of the organization's management in regulating information security. Chen *et al.,* [15] reiterate the issue of BYOD in confidentiality, integrity, and authenticity in the organization's data discussed in Disterer *et al.,* [16].

In the education sector, BYOD users are students and the younger generations susceptible to malware threats but have little awareness of potential attacks. Pittayachawan *et al.,* [17] also claimed that they make up the majority of users of online social networks. The popularity of social media has been exploited by scammers targeting use based on algorithms and social media engagements. They typically use seemingly fun activities; for example, offering fake prizes and gift cards or games like predicting the real age, your life in 2030, to lure people to click malware-embedded links. According to statistics from the Australian Communication and Media Authority (ACMA) report in 2013-2014, the younger generation is s the majority group using the Internet for leisure. As a result, students are highly exposed to the malware threats behind these non-academic activities. Similarly, BYOD users, including university employees, spend much of their time on social media applications and online storage such as iCloud and Google Drive to store documents related to the organizations stated in Musarurwa *et al.,* [18].

Institutions of Higher Learning (IHL) are responsible for preparing students to become a future workforce. Hence, they should be prepared for the BYOD scenario as soon as they enter the job market. BYOD practice has been accepted in every sector and used in schools (French 2014). Hence, IHL should encourage students to adhere to the BYOD security policy and be aware of threats to information security. Considering that the younger generations have grown up with different technology devices, it is worth considering. Therefore, the education environment should empower the knowledge about BYOD among the students (including staff who are not in the IT field) and strengthen their awareness and training to identify the risks of BYOD. Again in [18], they found that employees implementing BYOD do not comply with their organization's security policy.

The research trend for the first five years after BYOD was introduced showed that most studies had reported increased BYOD practices in all sectors. Intel was the first to introduce this over in 2009, followed by various organizations across all sectors. BYOD has become the preferred choice for many organizations. Nonetheless, experts warn there are risks in BYOD implementation in 2013. Researchers then continued to emphasize BYOD's threats, issues, and challenges that could bring loss and cause critical breaches, especially in corporate security. As we know, accessing websites, downloading apps embedded with malicious codes, and connecting to an unsecured network using BYOD devices could being risks of exposure to illegal activities. Along the years, research trend has shifted to find the solutions to overcome risks in response to the growing interest on BYOD, causes of threats to BYOD and security technical configurations. Figures 1 and 2 show the timeline of BYOD research outside and inside Malaysia.

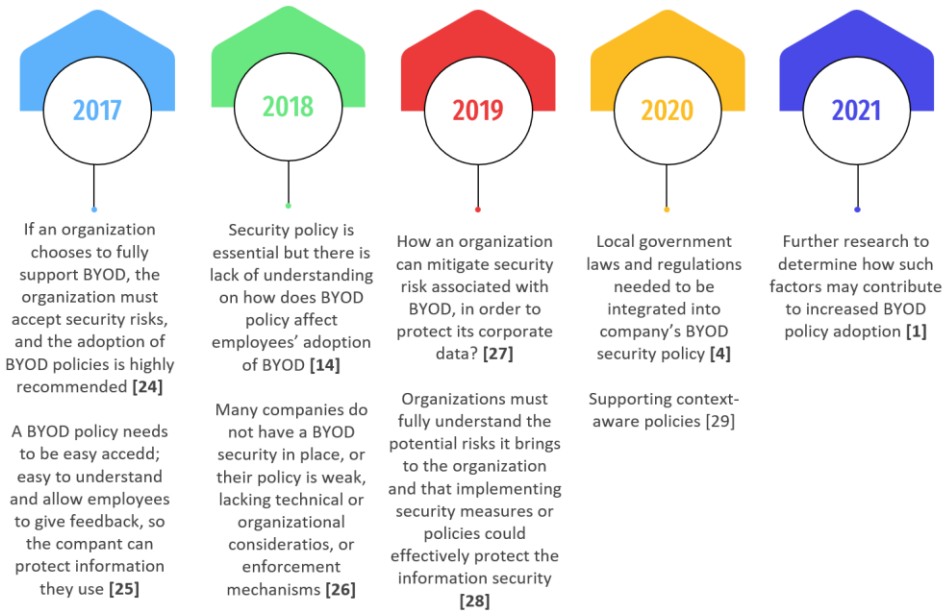

Fig. 1. BYOD Research Timeline (2017-2021)

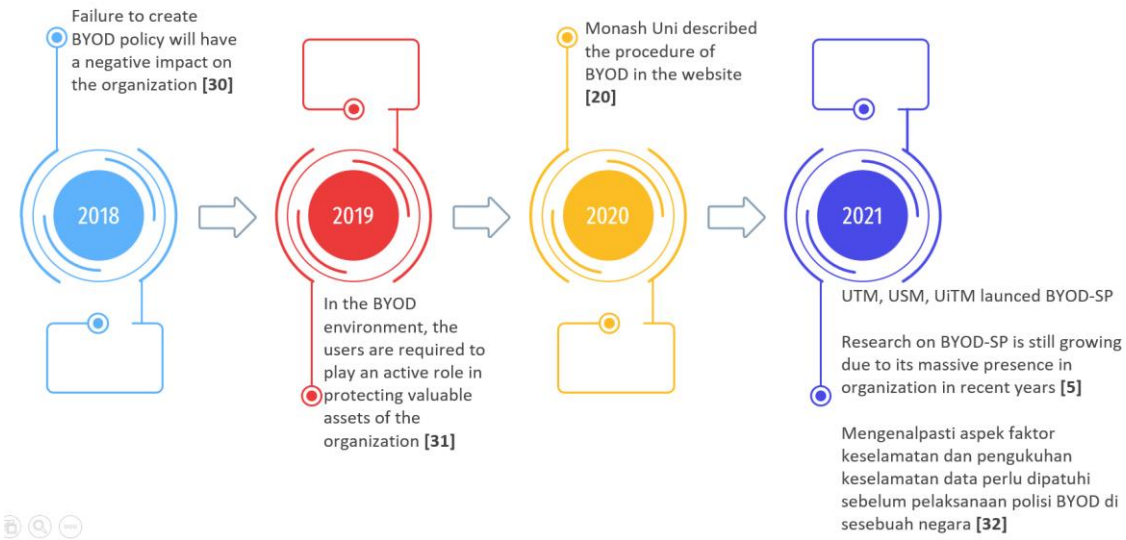

Fig. 2. BYOD Research in Malaysia (2018 – 2020)

This paper is divided into four main sections. Section 2 elaborated on how this research was tailored on the methodology to meet the objectives. In this paper, methodology stops at phase 3 as we want to do the investigation on BYOD-SP implemented in available documents released via online searching or official documentation on the institution's official website and the comparison components in BYOD-SP between Malaysia IHL and foreign universities. In Section 3, the results were presented which elaborating the BYOD-SP concept in each Malaysia IHL, the established of BYOD-SP in few Malaysia IHL, the list of foreign universities in certain regions that published their own BYOD-SP. The discussion then furthered to identify the trend of each component listed in both Malaysia IHL and foreign universities which were summarized into a table. It then concluded the most similarities of components being featured in official BYOD-SP. The significant of this study is to enrich the literature in BYOD field, narrowing down to the security policy in BYOD implementation. It offers a future reference for formulating BYOD-SP that meet and match the education policies.

2. Methodology – Proposed Research Design

This study will apply the quantitative research approach. Table 1 shows the proposed design to answer the research questions and achieve the research objectives. We are now in final step in third phase, preparing the data collection of BYOD-SP documents in local and foreign universities before moving to the final phase of conducting the quantitative methods for data analysis of BYOD-SP awareness among BYOD users in education premises. This research design is proposed to which intends to tailoring the development of cybersecurity framework in Security Policy for BYOD awareness.

Table 1
Research Design

Phases	Research Process	Method	Deliverables	Expected Outcome
Phase 1 Feasibility study – RQ1a	Knowledge acquisition via online databases like Scopus, IEEE, and Google Scholar	Literature Review	• Explore the BYOD current research trend • Understand the situation	BYOD-SP implementation in MIHL.
Phase 2 Empirical Study (RQ1a)	Data Collection Data Analysis	Secondary data (offline/online), accessible and downloadable and accessible form Google or Univeristi online site.	Find the BYOD-SP documents in MIHL and foreign university.	Identify the local and foreign universities that have implemented BYOD-SP on the campuses.
Phase 3 Empirical Study (RQ1b)	Data Collection Data Analysis	Secondary data (offline/online) Comparing the components, and remark the similarities and differentiation into Microsoft Excel.	Find out the components in the BYOD-SP.	Retrieve the components in BYOD-SP in local and foreign universities.
Phase 4 Development of cybersecurity framework (CSF) for Bring Your Device (BYOD) Awareness	Data Collection Data Analysis	Survey	To identify suitable CSF or other components in BYOD-SP To improve BYOD-SP documentation by matching the suitable CSF.	Proposed cybersecurity framework to promote the awareness of security in BYOD implementation in MIHL

In the first phase, the study explored current research on BYOD topics, focused on the BYOD Security Policy and BYOD Policy Model. The knowledge acquisition phase involved retrieving relevant articles from online databases such as Scopus, Science Direct, Emerald Insight, and Google Scholar. As illustrated in Figure 1, although BYOD has been widely accepted in the industry today, this study has examined latest research on BYOD to analyze the current trend of BYOD research. After identifying the latest issue, we narrowed our search down to the latest 5 years back, starting in 2017 until early 2022. The scope is to determine the most suitable approach for the BYOD Security Policy.

We expanded this study to identify how organizations conduct the release of the BYOD Security Policy documentation. Since the target is institutions of higher learning in Malaysia, this study sought the official document of the BYOD Security Policy in each institution. We visited each public IHL website, which directed us to find the available BYOD-SP under the IT/ICT Unit/Department links. As a result, only a few documents are accessible and can be downloaded by the public. Some of the public IHL cannot be downloadable which required the visitor to have the id and password to retrieve the private documents (see Figure 3). The documents on the BYOD Security Policy highlight the definition, scope, purposes, and other components. The search for the BYOD Security Policy document was extendee to foreign universities, and the components in these documents were compared to see the similarities and differences between Malaysian and foreign universities (see more Section 3).

3. Results

3.1 BYOD Security Policy

The first three phases are crucial to ensure this study could identify the gap in current BYOD Security Policy research. This study found that scholars had actively discussed BYOD security risks after 3 to 4 years as BYOD became more preferred in 2011. Researchers have discussed the potential attacks from any sources, such as unauthorized software, malicious application embedded in media social apps, games or joy quizzes, and the lack of network and system protection in organizations.

3.1.1 Public MIHL

There are 20 Public Malaysian Institutions of Higher Learning (MIHL) across Malaysia. These MIHLs can be divided into Research Universities (RUs) and others. On average, there are 1-3 public universities in each state. Based on the online search for the security policy of each MIHL, it was found that each university had prepared its security policy and frameworks for safeguarding information security in Information and Communication Technology (ICT). However, before going deeper to discuss the BYOD security policy in MIHL, the study had examined the concept of BYOD in Malaysia environment. In general, we have our stand that BYOD is defined as allowing employees/user to bring their devices to the workplace. In the meantime, in the context of education, BYOD means that lecturers and students can bring and use technology for in-class activities. In MIHLs, the BYOD grant concept is linked to the BYOD Grant.

The BYOD Grant refers to university management's allocation of funding money to eligible staff to buy technology devices, including personal laptops, tablets, or other related technology equipment for working purposes. This highlights the issue of information security and how to tighten the practice of securing any private data and confidential information of that organization if the terms do not explain any risks from the BYOD practice. Moreover, less information has been described on the BYOD technical mechanisms and protection. Although the registration of devices after purchasing is done at an earlier stage to monitor device activities, it should not be limited to just 'registration', the staff should also be trained in BYOD to increase their understanding of technical aspects and identifying threats.

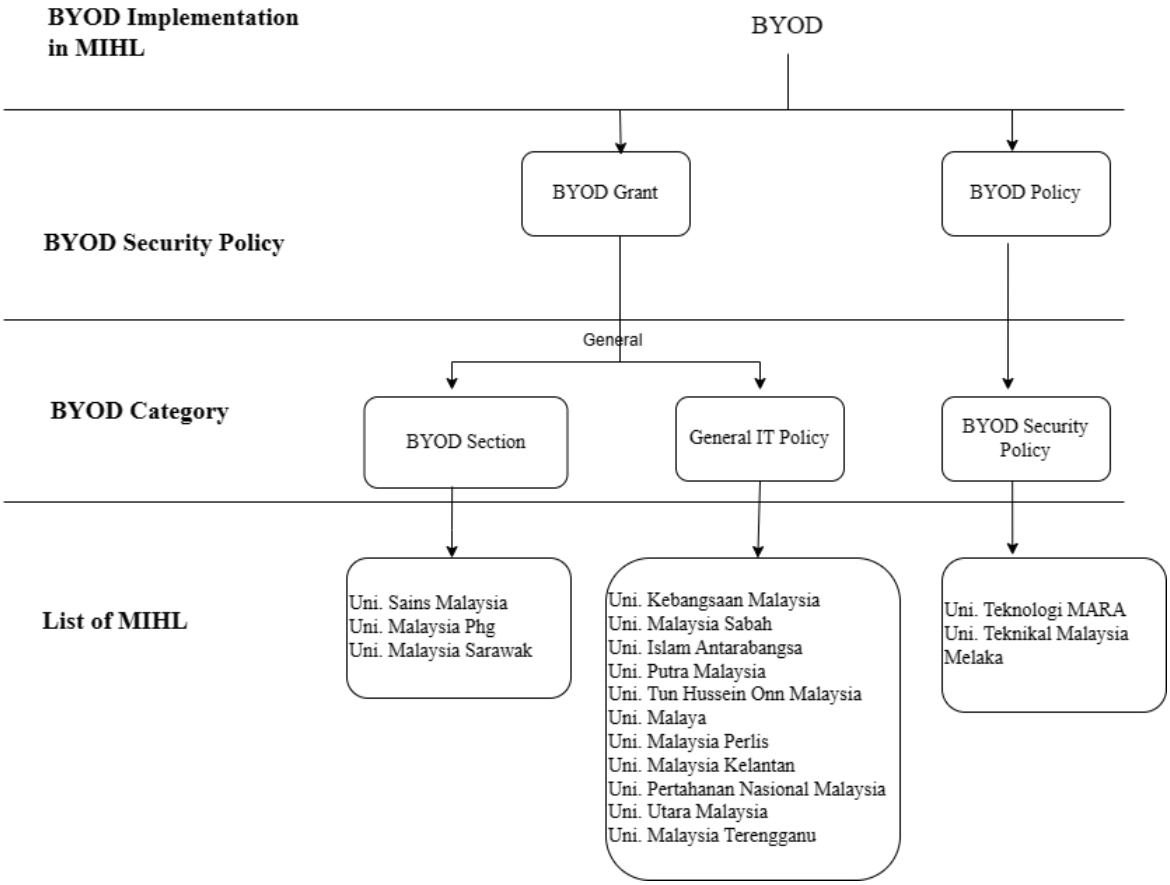

Fig. 3. BYOD Security in Public MIHL

3.1.2 Private MIHL

Tertiary institutions in Malaysia comprises public and private institutions. There are 50 private universities, 34 university colleges, and 10 foreign university branch campuses summarized in [19]. Subsequently, the scope for the search for BYOD security policies in Malaysia Institution of Higher Learning (MIHL) has been extended to private institutions to investigate the extend of BYOD implementation in the education sector. For instance, how far has BYOD security policies of foreign universities been implemented in their branch campuses in Malaysia. For example, the University of Reading in Reading, Berkshire, England, published their Bring Your Device (BYOD) policy in May 2017. The document briefly describes the purpose, definitions, rules, responsibilities, requirements, consequences of non-compliance to this policy, guidance, and key principles and related policies applied.

However, the search for BYOD security policy for the rest of private institutions found discouraging results. Some institutions have explained their policy in a short description displayed on their website, like Monash University [20] (accessed via *BYOD Guidelines - IT Services (monash.edu.my)*. The situation worsens when the BYOD security policy documents for established universities or private college are unavailable or missing. These unwanted conditions could confuse BYOD players who have no idea what to do when they detect BYOD risks. Indirectly, if the BYOD policy is not established, it will be hard to train users about BYOD security and become aware of threats in BYOD implementation. Throughout this search, it was observed that several schools have established their BYOD security policies. This brought questions on how tertiary institutions can guide students on the BYOD concept and implementation. In this light, it is their responsibility to educate younger generations and prepare them for the reality of the workplace.

Answering RQ1a, it can be early summarized from the finding, not all MIHLs established the BYOD-SP. Still, a result in minor IHL released the BYOD-SP earlier in 2020. This condition worsens as for the private IHL, what are the status of BYOD implementation and the result of its security on campuses network, system or confidential staff and students' data if BYOD practice is not in university control that led to the serious case of data loss, data breach etc. As BYOD is one of the mobile computing trends that demand its popularity it contributes to innumerable benefits for all parties in universities, further exploration of how aware people towards the risks in BYOD playground. In addition, the extra approach of BYOD-SP needs to be spread so that users understand to adhere to each component contains in BYOD-SP as suggested by Galego *et al.,* [21], employees should be invited in the tailoring process of BYOD policies to obtain user buy-in and compliance and is an effective strategy for converting a weak link to a strong security control.

3.1.3 Foreign universities

The study extended its search to the BYOD security policy of education institutions outside Malaysia (see Table 2). The study found that in terms of online documents and files regarding BYOD or BYOD security policy, several higher education institutions had published stand-alone guidelines for BYOD security policy. Furthermore, we discovered that starting in 2015, they had started BYOD security policy in organizations. Compared with Malaysia's situation, most universities established stand-alone documents that only focus on BYOD security. It can also be seen from the surveillance that the documentation of the BYOD security policy has been separated from the general information technology policy.

After reviewing this BYOD security policy, it could be observed that BYOD players are aware of how BYOD can be practiced in one organization and serious matters related to information security, such as data leakage, cyber threat, and attack or risks, can be addressed earlier in the implementation of BYOD as precaution towards any cyber security threats and to mitigate risks of misuse by irresponsible individuals. In addition, some BYOD security policy documents were reviewed after a few years of being published. The auditing and review process of the documents can be seen as a good practice for the top management to see any flawed information and necessary actions for strengthening BYOD implementation in institutions. Such information can also encourage them to plan necessary actions to update information security components, and increase understanding of BYOD practice.

Table 2
List of foreign universities

Region	Country	University
Europe	United Kingdom	Buckinghamshire New University
		Sheffield Hallam University
		University of Hull
		University of Reading
		The University of Edinburgh
		University of Dundee
North America	United States of America	Northampton Community College
		Centenary University
		Clayton State University
		West Virginia University
		Mansfield University of Pennsylvania
Oceania	Australia	University of Newcastle

3.2 BYOD Security Policy Component

After analyzing each component in the BYOD Security Policy for these educational institutions, it was found that most documentation comprises standard 5-10 pages documents. The earliest version was published in 2017 by Clayton State University. In terms of online accessibility, these documents can be downloaded by the public, and the policies contain several components to be comprehended and accepted by BYOD practitioners. Table 3 shows the components found in the BYOD Security Policy document in Local (Malaysia Universities) and Foreign Universities. The accessible documents were downloaded and analysed during the comparison stage, where the components in all the BYOD security policies were identified to see the similarities. We compared the most frequent components retrieved in both Malaysia local and foreign universities regarding on their similarities and difference of the components contained in the BYOD-SP document. This was done to investigate what are the top consideration of components that should be highlighted for BYOD-SP to have a comprehensive approach tailored in the future. Figure 4 illustrates the most common components listed in the BYOD Security Policy of local and foreign universities. The Venn diagram showed that few components such as Scope, Procedure, Associated Policy and Act found in both based on the comparison of BYOD Security Policy. Nonetheless, there are still exist few different components

Table 3
BYOD components in local MIHL and foreign universities

UNI	DEP	DOC	ISS	REV	PRIN	PUR	DEF	SCO	PRO	ASS POL	ACT	SUP
LOCAL MIHL												
UTEM	Pusat Perkhidmatan Pengetahuan Dan Komunikasi	Peraturan Bring Your Own Device	-NA-	-NA-		/	/	/	/	/	/	/
UiTM	Jbtn Infostruktur PPII UiTM	Garis Panduan Pelaksanaan Bring Your Own Device (BYOD)	Aug 2021	-NA-		/	/	/	/			
FOREIGN UNIVERSITIES												
Northampton Community College	ICT Services	BYOD (Bring Your Own Device) Policy	Mar 2021	Mar 2022	/		/	/	/	/		
Buckinghamshire New University	IS&T Directorate	BRING YOUR OWN DEVICE (BYOD) POLICY	Apr 2019	Oct 2021					/	/	/	
Centenary University	Office of Information Technology	Bring Your Own Device (BYOD) Policy	10/2019	-NA-					/	/		/
Clayton State University	-NA-	BYOD Bring Your Own Device Policy	July 2017	-NA-				/	/	/		
University of Newcastle	-NA-	Information Security BYOD Procedure	Mar 31, 2017	Jul 1, 2017					/	/	/	/
Mansfield University	Campus Technology	-NA-	Mar 17, 2020	-NA-					/	/		/
Sheffield Hallam University	-NA-	Bring Your Own Device (BYOD) Policy for University and Staff	Feb 2022	Feb 2023				/		/		/
University of Hull	Security and Architecture Manager, ICT (Steph Jones)	Managed Device and BYOD Policy	Nov 9, 2021	-NA-	/		/	/		/	/	
University of Reading	Information Management and Policy Services (IMPS) and Information Technology (IT)	Bring Your Own Device (BYOD) Policy	May 17	July 18	/	/	/			/	/	
University of Edinburgh	David Williamson, Anne Grzybowski, and Susan Graham	BYOD Policy: Use of Personally Owned Devices for University Work	Feb 2015	-NA-		/					/	
University of Dundee	University's Help4U service	Mobile and bring your own device (BYOD) policy	-NA-	Apr 29, 2020		/	/	/		/	/	
West Virginia University	Information Security Services	Bring Your Own Device (BYOD) Standard	Dec 31, 2019	Dec 30, 2022		/	/	/	/			

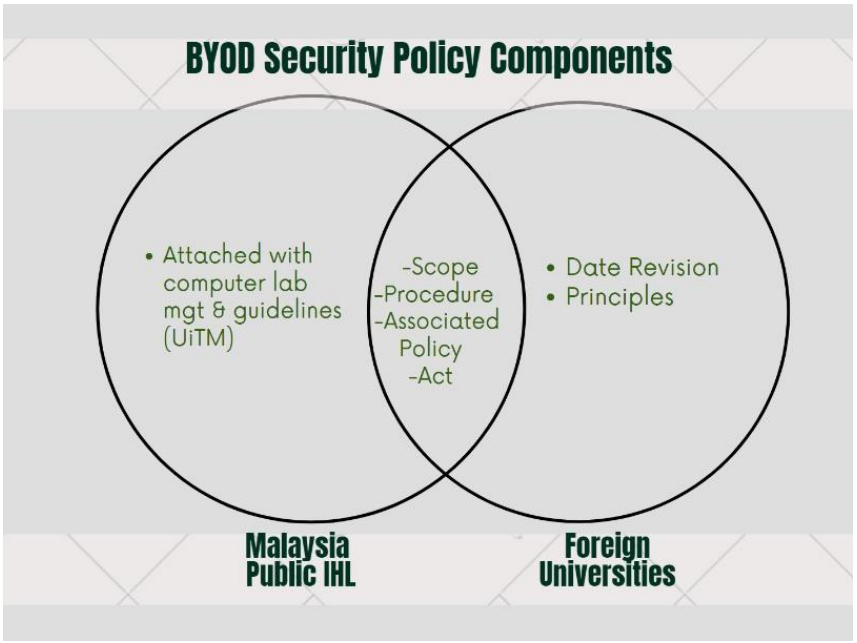

Fig. 4. Venn Diagram of Comparison BYOD Security Policy components

4. Conclusions

In conclusion, this study has shown the opportunity for diverse research on BYOD implementation, emphasizing security and the development of the security policy itself. In addition, it may drive BYOD implementation in the future, especially in the education sector, to create more opportunities and ways to strengthen the BYOD agenda on campus, such as awareness and security practices. It is clearly stated to use BYOD, the availability of legislation and policies must be emphasized suggested in Almarhabi *et al.,* [22] in the organization and applied in the campuses. Government's law and related education agenda and the latest innovation in mobile devices and other devices may help identify suitable components and compatible guidances for BYOD security policy. The findings will be beneficial in BYOD practices and aid several parties, including the top management, policy maker, or ICT Department, to better understand the BYOD environment. In addition to policy formulation, it delegates the responsibility to the BYOD practitioners recommended by Weeger *et al.,* [23] and at the same time the policy should be readable, accessible, and user-friendly to guarantee better protection of an organization's security information Scott *et al.,* [1].

While the implementation of BYOD is expected to continue growing in various sectors in the future, it is essential to establish a comprehensive BYOD-SP to ensure maximum protection in all aspects of risk management. This study focuses on BYOD implementation in tertiary education and provides several suggestions to university top management on how to create an official BYOD-SP documentation for the campus area:

i. This study provides guidance for creating a stable BYOD-SP that meets the needs of educational learning and teaching activities
ii. The BYOD-SP should take into account all aspects of the BYOD environment, including the latest devices, software, applications, and users, with the aim of ensuring all parties have a good understanding and adhere to each component in the BYOD-SP.
iii. The BYOD-SP should consider yearly revisions to identify the latest changes in technology and recognize the newest techniques of cyberattacks in BYOD practices.

The mission of achieving a comprehensive BYOD policy cannot be accomplished solely by the organization; it also requires BYOD users to stay up-to-date with the latest technological changes. As users are most familiar with their own devices, they play a significant role in ensuring compliance with the BYOD-SP. In the academic community, BYOD users should be familiar with the components listed in the BYOD-SP and understand their descriptions to comply with the policy's requirements. Furthermore, users should be aware of their accountability and integrity in every action they take to prevent any loss to the company through the BYOD practice. The future research of this project will concentrate on implementing strategies and developing a BYOD framework that aligns with the education agenda to spread information security protection and reduce BYOD risks in campus areas.

Acknowledgement
This research was funded by a grant from University College TATI under Short Term Grant No. GPJP2022 / 9001-2202. We would like to express gratitude to University College TATI for the grant of this study. We also sincerely appreciated the reviewers' valuable and constructive comments in helping us to produce this paper.

References

[1] Scott, Ben, Raina Mason, and Patryk Szewczyk. "A snapshot analysis of publicly available BYOD policies." In *Proceedings of the 2021 Australasian Computer Science Week Multiconference*, pp. 1-6. 2021. https://doi.org/10.1145/3437378.3437394

[2] Anderson, John, Qiqing Huang, Long Cheng, and Hongxin Hu. "BYOZ: Protecting BYOD Through Zero Trust Network Security." In *2022 IEEE International Conference on Networking, Architecture and Storage (NAS)*, pp. 1-8. IEEE, 2022. https://doi.org/10.1109/nas55553.2022.9925513.

[3] bin Yeop, Yusri Hakim, Zulaiha Ali Othman, Siti Norul Huda Sheikh Abdullah, Umi Asma'Mokhtar, and Wan Fariza Paizi Fauzi. "BYOD implementation factors in schools: A case study in Malaysia." *International Journal of Advanced Computer Science and Applications* 9, no. 12 (2018). https://doi.org/10.14569/IJACSA.2018.091245

[4] Rajapaksha, Nirusha. "Bring Your Own Device (BYOD): Existent State, Issues, and solutions." https://doi.org/10.13140/RG.2.2.16340.83849.

[5] Palanisamy, Rathika, Azah Anir Norman, and Miss Laiha Mat Kiah. "Compliance with Bring Your Own Device security policies in organizations: A systematic literature review." *Computers & Security* 98 (2020): 101998. https://doi.org/10.1016/j.cose.2020.101998

[6] Almarhabi, Khalid, Kamal Jambi, Fathy Eassa, and Omar Batarfi. "Survey on access control and management issues in cloud and BYOD environment." *International Journal of Computer Science and Mobile Computing* 6, no. 12 (2017): 44-54.

[7] Bello, A. G., Murray, D., & Armarego, J. 2015. "Information & Computer Security Article Information :" *Information & Computer Security* 23 (2): 145–60.

[8] Kebande, Victor R., Nickson M. Karie, and H. S. Venter. "A generic Digital Forensic Readiness model for BYOD using honeypot technology." In *2016 IST-Africa Week Conference*, pp. 1-12. IEEE, 2016. https://doi.org/10.1109/ISTAFRICA.2016.7530590.

[9] Jie, C. Y., and N. Mat Ali. "COVID-19: What are the challenges of online learning? A literature review." *International Journal of Advanced Research in Future Ready Learning and Education* 23, no. 1 (2021): 23-29.

[10] Masrom, Maslin, Mohd Nazry Ali, Wahyunah Ghani, and Amirul Haiman Abdul Rahman. "The ICT implementation in the TVET teaching and learning environment during the COVID-19 pandemic." *International Journal of Advanced Research in Future Ready Learning and Education* 28, no. 1 (2022): 43-49.

[11] Aguboshim, Felix C., and Joy I. Udobi. "Security issues with mobile IT: A narrative review of Bring Your Own Device (BYOD)." *Information Technology (IT)* 8, no. 1 (2019). https://doi.org/10.7176/jiea/8-1-07.

[12] Lee, Jin Hwa, and Hasan Tinmaz. "A perceptional analysis of BYOD (bring your own device) for educational or workplace implementations in a South Korean case." *Participatory Educational Research* 6, no. 2 (2019): 51-64. https://doi.org/10.17275/per.19.12.6.2.

[13] French, Aaron M., Chengqi Guo, and Jung P. Shim. "Current status, issues, and future of bring your own device (BYOD)." *Communications of the Association for Information Systems* 35, no. 1 (2014): 10. https://doi.org/10.17705/1CAIS.03510.

[14] Cho, Vincent, and W. H. Ip. "A study of BYOD adoption from the lens of threat and coping appraisal of its security policy." *Enterprise Information Systems* 12, no. 6 (2018): 659-673. https://doi.org/10.1080/17517575.2017.1404132
[15] Chen, Hao, Ying Li, Lirong Chen, and Jin Yin. "Understanding employees' adoption of the Bring-Your-Own-Device (BYOD): the roles of information security-related conflict and fatigue." *Journal of Enterprise Information Management* 34, no. 3 (2021): 770-792. https://doi.org/10.1108/JEIM-10-2019-0318.
[16] Disterer, Georg, and Carsten Kleiner. "BYOD bring your own device." *Procedia Technology* 9 (2013): 43-53. https://doi.org/10.1016/j.protcy.2013.12.005
[17] Dang-Pham, Duy, and Siddhi Pittayachawan. "Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach." *Computers & Security* 48 (2015): 281-297. https://doi.org/10.1016/j.cose.2014.11.002
[18] Musarurwa, Alfred, Stephen Flowerday, and Liezel Cilliers. "An information security behavioural model for the bring-your-own-device trend." *South African Journal of Information Management* 20, no. 1 (2018): 1-9. https://doi.org/10.4102/sajim.v20i1.980.
[19] "List of Universities in Malaysia." Retrieved from List of Universities in Malaysia - StudyMalaysia.com.
[20] Campus, Monash University Malaysia. "BYOD Guidelines." https://www.monash.edu.my/its/our-services/students/byod-guidelines.
[21] Galego, Nuno Miguel Carvalho, Rui Miguel Pascoal, and Pedro Ramos Brandão. "BYOD: Impact in Architecture and Information Security Corporate Policy." In *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1-2. IEEE, 2022. https://doi.org/10.23919/CISTI54924.2022.9820043.
[22] Almarhabi, Khalid A., Ahmed M. Alghamdi, and Adel A. Bahaddad. "Adoption of the Bring Your Own Device (BYOD) Approach in the Health Sector in Saudi Arabia." *IJCSNS Int. J. Comput. Sci. Netw. Secur* 6 (2022): 371-382.
[23] Weeger, Andy, Xuequn Wang, Heiko Gewald, Mahesh Raisinghani, Otavio Sanchez, Gerald Grant, and Siddhi Pittayachawan. "Determinants of intention to participate in corporate BYOD-programs: The case of digital natives." *Information Systems Frontiers* 22 (2020): 203-219. https://doi.org/10.1007/s10796-018-9857-4.
[24] Vorakulpipat, Chalee, Soontorn Sirapaisan, Ekkachan Rattanalerdnusorn, and Visut Savangsuk. "A policy-based framework for preserving confidentiality in BYOD environments: A review of information security perspectives." *Security and Communication Networks* 2017 (2017). https://doi.org/10.1155/2017/2057260.
[25] Herrera, Andrea Vaca, Mario Ron, and Carlos Rabadão. "National cyber-security policies oriented to BYOD (bring your own device): Systematic review." In *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1-4. IEEE, 2017. https://doi.org/10.23919/CISTI.2017.7975953
[26] Ratchford, Melva M. "BYOD: a security policy evaluation model." In *Information Technology-New Generations: 14th International Conference on Information Technology*, pp. 215-220. Springer International Publishing, 2018. https://doi.org/10.1007/978-3-319-54978-1.
[27] Ratchford, Melva M., and Yong Wang. "Byod-insure: A security assessment model for enterprise byod." In *2019 Fifth Conference on Mobile and Secure Services (MobiSecServ)*, pp. 1-10. IEEE, 2019. https://doi.org/10.1109/MOBISECSERV.2019.8686551.
[28] Tu, Cindy Zhiling, Joni Adkins, and Gary Yu Zhao. "Complying with BYOD security policies: A moderation model based on protection motivation theory." *Journal of the Midwest Association for Information Systems (JMWAIS)* 2019, no. 1 (2019): 2. https://doi.org/10.17705/3jmwa.000045.
[29] Kang, Qiao, Lei Xue, Adam Morrison, Yuxin Tang, Ang Chen, and Xiapu Luo. "Programmable {In-Network} security for context-aware {BYOD} policies." In *29th USENIX Security Symposium (USENIX Security 20)*, pp. 595-612. 2020.
[30] Mahat, Norhazilah Binti, and Nor'Ashikin Ali. "Empowering employees through BYOD: Benefits and challenges in Malaysian Public Sector." *International Journal of Engineering and Technology (UAE)* 7, no. 4 (2018): 643-649. https://doi.org/10.14419/ijet.v7i4.35.23077
[31] Palanisamy, Rathika, Azah Anir Norman, and Miss Laiha Mat Kiah. "BYOD Security Policy Compliance Framework." (2019).
[32] Mohamed, Ibrahim. 2020. "Model Tahap Kesedaran Pekerja Terhadap Penggunaan BYOD."